UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	10/11/2016	9465104		7721

23497 7590 09/21/2016

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 596 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Jed Margolin, VC Highlands, NV;

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number — Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US- 2013/0176163	07-11-2013	Margolin	
	4	US- 5,153,836	10-06-1992	Fraughton, et al.	Abstract
	6	US- 7,414,567	08-19-2008	Zhang, et al.	Cols 3, 6, 7, 8
	8	US- 2011/0140950	~~09-16-2011~~ 06/2011	~~Anderson~~ Andersson	Abstract
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

Change(s) applied to document, /M.H.E./ 6/29/2016

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document — Country Code[3] -Number[4] -Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
	7	EP 2136222 A1	12-23-2009	Persson, et al.	Page 3	

Examiner Signature	/TIMOTHY A BRAINARD/	Date Considered	01/06/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.A.B/

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23497 7590 06/20/2016

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

TITLE OF INVENTION: ADS-B Radar

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	09/20/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
BRAINARD, TIMOTHY A	3648	342-029000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1 ______
   2 ______
   3 ______

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☒ Advance Order - # of Copies 5

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☒ Payment by credit card. ~~Form PTO-2038 is attached~~. **Paid through EFS**
- ☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number ______ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature Jed Margolin Date 09/06/2016

Typed or printed name Jed Margolin Registration No. ______

Electronic Patent Application Fee Transmittal

Application Number:	14146202
Filing Date:	02-Jan-2014
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Filer:	Jed Margolin
Attorney Docket Number:	

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
Printed Copy of Patent - No Color	8001	5	3	15
		Total in USD ($)		**495**

Electronic Acknowledgement Receipt

EFS ID:	26848754
Application Number:	14146202
International Application Number:	
Confirmation Number:	7721
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Customer Number:	23497
Filer:	Jed Margolin
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-SEP-2016
Filing Date:	02-JAN-2014
Time Stamp:	22:49:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$495
RAM confirmation Number	7881
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	adsb2_fee_partb.pdf	241318 6d64fcbc58ae9fe0ef60e3783b203461dda9a375	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31498 dbad58e3c2f7b678071c915dc47a2bcb8b8daf9a	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	272816	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23497 7590 06/20/2016
JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

EXAMINER	
BRAINARD, TIMOTHY A	
ART UNIT	PAPER NUMBER
3648	

DATE MAILED: 06/20/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

TITLE OF INVENTION: ADS-B Radar

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	09/20/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23497 7590 06/20/2016
JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

TITLE OF INVENTION: ADS-B Radar

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	09/20/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
BRAINARD, TIMOTHY A	3648	342-029000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1 ________________
   2 ________________
   3 ________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies ________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number __________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ______________________ Date ______________________

Typed or printed name ______________________ Registration No. ______________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

23497 7590 06/20/2016

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

EXAMINER
BRAINARD, TIMOTHY A

ART UNIT	PAPER NUMBER
3648	

DATE MAILED: 06/20/2016

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/146,202	Applicant(s) MARGOLIN, JED	
	Examiner TIMOTHY A. BRAINARD	Art Unit 3648	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/9/2016*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *2,6 and 14*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

2. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

Allowable Subject Matter

3. Claims 2, 6, and 14 are allowed.

4. The following is an examiner's statement of reasons for allowance: Margolin (US 20110169684) and Wu et al (US 20110156878) do not teach nor make obvious (claim 2, 6, and 14) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target and said radar processor is configured to note said discrepancy on said display as a second attention item, and a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TIMOTHY A. BRAINARD whose telephone number is (571)272-2132. The examiner can normally be reached on Monday - Friday 9:00 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tashiana Adams can be reached on (571) 270-5228. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/TIMOTHY A BRAINARD/
Primary Examiner, Art Unit 3648

Notice of References Cited	Application/Control No. 14/146,202	Applicant(s)/Patent Under Reexamination MARGOLIN, JED	
	Examiner TIMOTHY A. BRAINARD	Art Unit 3648	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2011/0169684 A1	07-2011	Margolin; Jed	G01S5/12	342/30
*	B	US-2011/0156878 A1	06-2011	Wu; Ryan Haoyun	G01S5/0081	340/10.1
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14146202	MARGOLIN, JED
	Examiner	Art Unit
	TIMOTHY A BRAINARD	3648

CPC- SEARCHED

Symbol	Date	Examiner
G01S13/9303; G01S11/02; G01S13/003; G01S5/12; G01S13/42	1/6/2015	TAB

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
342	29, 30, 118	1/6/2016	TAB

SEARCH NOTES

Search Notes	Date	Examiner
updated east search -- see attached	1/6/2015	TAB
updated east search -- see attached	6/1/2016	TAB
updated east search -- see attached	6/13/2016	TAB

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
G01S	13/9303; 11/02; 13/003; 5/12; 13/42	6/13/2016	TAB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Jed Margolin
Serial No.: 14/146,202
Filed: 01/02/2014
For: ADS-B RADAR

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir: OK TO ENTER: /TB/

This is in response to the Office Action mailed 6/6/2016 in which, in a Final Rejection, the Examiner:

A. Rejected Claims 1, 3-5, 7-8, 13, and 15-16 under 35 U.S.C. 103 as being unpatentable over Margolin (US 20110169684) in view of Wu et al (US 20110156878). (Examiner's Sections 2 and 3.)

B. Rejected Claims 9-12 and 17-20 under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu and further in view of Donovan (US 20100090882). (Examiner's Section 4.)

C. Advised Applicant in Examiner's Section 5 that:

> 7. Claims 2, 6, and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Amendments to Claims begin on page 2.

Remarks begin on page 10.

OK TO ENTER: /TB/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S30	5	((ads-b automatic near3 dependent near3 broadcast$4) and velocit$4 near14 error$2).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/13 13:01
S29	110	((ads-b automatic near3 dependent near3 broadcast$4) and radar$2).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/13 12:37
S28	39116	((G01S13/9303 OR G01S11/02 OR G01S13/003 OR G01S5/12 OR G01S13/42).CPC. OR (342/118 OR 342/29 OR 342/30).CCLS. OR (G01S13/93 OR G01S13/00 OR G01S13/75).IPCR.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/13 12:37

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S31	110	((ads-b automatic near3 dependent near3 broadcast$4) and radar$2).clm.	US-PGPUB; USPAT	OR	ON	2016/06/13 12:37

6/14/2016 1:40:45 PM
C:\Users\tbrainard\Documents\EAST\Workspaces\14146202.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14146202	MARGOLIN, JED
	Examiner	**Art Unit**
	TIMOTHY A BRAINARD	3648

CPC

Symbol				Type	Version
G01S	13	/	9303	F	2013-01-01
G01S	13	/	42	I	2013-01-01
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			

CPC Combination Sets

Symbol				Type	Set	Ranking	Version
		/					
		/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 3	
/TIMOTHY A BRAINARD/ Primary Examiner.Art Unit 3648 (Primary Examiner)	06/13/2016 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14146202	MARGOLIN, JED
	Examiner	**Art Unit**
	TIMOTHY A BRAINARD	3648

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION					
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED
342	29	G	0	1	S	13 / 00 (2006.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 3	
/TIMOTHY A BRAINARD/ Primary Examiner.Art Unit 3648 06/13/2016 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14146202	MARGOLIN, JED
	Examiner	**Art Unit**
	TIMOTHY A BRAINARD	3648

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☒ **T.D.** ☐ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 3
/TIMOTHY A BRAINARD/ Primary Examiner.Art Unit 3648 06/13/2016 (Primary Examiner) (Date)	O.G. Print Claim(s): 1 — O.G. Print Figure: 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Jed Margolin
Serial No.: 14/146,202
Filed: 01/02/2014
For: ADS-B RADAR

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is in response to the Office Action mailed 6/6/2016 in which, in a Final Rejection, the Examiner:

A. Rejected Claims 1, 3-5, 7-8, 13, and 15-16 under 35 U.S.C. 103 as being unpatentable over Margolin (US 20110169684) in view of Wu et al (US 20110156878). (Examiner's Sections 2 and 3.)

B. Rejected Claims 9-12 and 17-20 under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu and further in view of Donovan (US 20100090882). (Examiner's Section 4.)

C. Advised Applicant in Examiner's Section 5 that:

> 7. Claims 2, 6, and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Amendments to Claims begin on page 2.

Remarks begin on page 10.

Amendments to Claims

Please amend the claims as follows.

1. (Canceled)

2. (Currently amended) A system for sensing aircraft and other objects comprising:

(a) an ADS-B transmitter;

(b) an ADS-B receiver;

(c) an ADS-B antenna;

(d) an ADS-B antenna multiplexer;

(e) an ADS-B processor;

(f) a radar processor;

(g) a datastream comparator;

(h) a display;

whereby

(i) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B multiplexer is configured to allow either said ADS-B transmitter or said ADS-B receiver to use said ADS-B antenna,

(j) said ADS-B processor and said radar processor are configured to work together,

(k) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through said ADS-B antenna multiplexer to said ADS-B antenna,

(l) said transmitted signal is reflected by a target producing a reflected signal,

(m) said reflected signal is received by said ADS-B antenna, and said ADS-B antenna multiplexer is configured to send said reflected signal to said ADS-B receiver,

(n) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target,

(o) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal,

(p) said radar processor is configured to display said range on said display, [[.]]

and whereby

(a) (q) if said range to said target does not match a possible position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item,

(b) (r) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target,

(c) (s) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target,

(d) (t) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target and said radar processor is configured to note said discrepancy on said display as a second attention item, and

(e) (u) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

3. (Canceled)

4. (Canceled).

5. (Canceled)

6. (Currently amended) A system for sensing aircraft and other objects comprising:

(a) an ADS-B transmitter;

(b) an ADS-B receiver;

(c) a first ADS-B antenna;

(d) a second ADS-B antenna;

(e) an antenna controller;

(f) an ADS-B antenna multiplexer;

(g) an ADS-B processor;

(h) a radar processor;

(i) a datastream comparator;

(j) a display;

whereby

(k) said second ADS-B antenna is directional, and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna,

(l) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna,

(m) said ADS-B processor and said radar processor are configured to work together,

(n) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer,

(o) said transmitted signal is reflected by a target producing a reflected signal,

(p) said reflected signal is received by either or both said first ADS-B antenna and said second ADS-B antenna, and said ADS-B antenna multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said ADS-B receiver,

(q) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target,

(r) said radar processor is configured to use the direction of said second ADS-B antenna to determine a bearing to said target,

(s) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal,

(t) said radar processor is configured to display said range and said bearing on said display, [[.]]

and whereby

~~(a)~~ (u) if said range and said bearing to said target do not match the position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item,

~~(b)~~ (v) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target,

~~(c)~~ (w) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target,

~~(d)~~ (x) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the

ADS-B system on said target, or deliberate misreporting by said target, and said radar processor is configured to note said discrepancy on said display as a second attention item, and

~~(e)~~ (y) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Canceled)

13. (Canceled)

14. (Currently amended) A system for sensing aircraft and other objects comprising:

(a) an ADS-B transmitter;

(b) a first ADS-B receiver;

(c) a first ADS-B antenna;

(d) a second ADS-B receiver;

(e) a second ADS-B antenna;

(f) an antenna controller;

(g) an ADS-B antenna multiplexer;

(h) an ADS-B processor;

(i) a radar processor;

(j) a datastream comparator;

(k) a display;

whereby

(l) said second ADS-B antenna is directional and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna,

(m) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said first ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said second ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna,

(n) said ADS-B processor and said radar processor work together,

(o) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer,

(p) said transmitted signal is reflected by a target producing a reflected signal,

(q) said reflected signal is received by either or both said first ADS-B antenna or said second ADS-B antenna, and said ADS-B multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said second ADS-B receiver,

(r) said radar processor is configured to process said reflected signal from said second ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target,

(s) said radar processor is configured to use the direction of said second antenna to determine a bearing to said target,

(t) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal,

(u) said radar processor is configured to display said range and said bearing on said display, [[.]]

and whereby

~~(a)~~ (v) if said range and said bearing to said target do not match the position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item,

~~(b)~~ (w) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target,

~~(c)~~ (x) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target,

~~(d)~~ (y) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target, and said radar processor is configured to note said discrepancy on said display as a second attention item, and

~~(e)~~ (z) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

REMARKS

Applicant has:

1. Amended Claims 2, 6, and 14, making them independent claims that include all of the limitations of their respective base claims and any intervening claims;

2. Canceled claims 1, 3-5, 7-13, and 15-20.

These actions by the Applicant should not be interpreted to mean that Applicant agrees with the Examiner's Final Rejection dated 6/6/2016. Applicant reserves the right to file RCEs, Continuations, and Whatever.

CONCLUSION

Having relied on the Examiner's promise that Claims 2, 6, and 14 would be allowed if rewritten in independent form including all of the limitations of the base claim and any intervening claims and amended the claims accordingly, this application is now in condition for allowance and notice of same is requested.

Respectfully submitted,

/Jed Margolin/ Date: June 9, 2016

Jed Margolin

Jed Margolin
1981 Empire Rd.
Reno, NV 89521-7430
775-847-7845

Electronic Acknowledgement Receipt

EFS ID:	26015547
Application Number:	14146202
International Application Number:	
Confirmation Number:	7721
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Customer Number:	23497
Filer:	Jed Margolin
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	09-JUN-2016
Filing Date:	02-JAN-2014
Time Stamp:	12:58:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	jm_adsb2_soa_response.pdf	47035 2a7d14fa2604b098ad39f78ec412fbf7028e5fad	no	10

Warnings:

Information:

Total Files Size (in bytes):	47035

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD
Substitute for Form PTO-875

Application or Docket Number	Filing Date	
14/146,202	01/02/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT

06/09/2016	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 3	Minus	** 20	= 0	x $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	**0**

AMENDMENT

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/DIANA BATES/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

23497 7590 06/06/2016

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

EXAMINER	
BRAINARD, TIMOTHY A	

ART UNIT	PAPER NUMBER
3648	

MAIL DATE	DELIVERY MODE
06/06/2016	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 14/146,202	Applicant(s) MARGOLIN, JED	
	Examiner TIMOTHY A. BRAINARD	Art Unit 3648	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _4/4/2016_.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) _1-20_ is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.
6)☐ Claim(s) _____ is/are allowed.
7)☒ Claim(s) _1,3-5,7-13 and 15-20_ is/are rejected.
8)☒ Claim(s) _2,6 and 14_ is/are objected to.
9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.
11)☒ The drawing(s) filed on _1/2/2014_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a)☐ All b)☐ Some** c)☐ None of the:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.
3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
4) ☐ Other: _____.

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 3-5, 7-8, 13, and 15-16 are rejected under 35 U.S.C. 103 as being unpatentable over Margolin (US 20110169684) in view of Wu et al (US 20110156878). Margolin teaches (claim 1) a system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) an ADS-B receiver; (c) an ADS-B antenna; (d) an ADS-B antenna multiplexer; (e) an ADS-B processor; (f) a radar processor; (g) a datastream comparator; (h) a display; whereby (i) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B multiplexer is configured to allow either said ADS-B transmitter or said ADS-B receiver to use said ADS-B antenna, (j) said ADS-B processor and said radar processor are configured to work together, (k) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through said ADS-B antenna multiplexer to said ADS-B antenna, (1) said transmitted signal is reflected by a target producing a reflected signal, (m) said reflected signal is received by said ADS-B antenna, and said ADS-B antenna multiplexer is configured to send said reflected signal to said ADS-B receiver, (n) said

radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (o) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and (p) said radar processor is configured to display said range on said display (claim 1) (claim 4) said radar processor is incorporated into said ADS-B processor (claim 2), (claim 5) a system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) an ADS-B receiver; (c) a first ADS-B antenna; (d) a second ADS-B antenna; (e) an antenna controller; (f) an ADS-B antenna multiplexer; (g) an ADS-B processor; (h) a radar processor; (i) a datastream comparator; (j) a display; whereby (k) said second ADS-B antenna is directional, and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna, (1) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, (m) said ADS-B processor and said radar processor are configured to work together, (n) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer, (o) said transmitted signal is reflected by a target producing a reflected signal, (p) said reflected signal is received by either or both said first ADS-B antenna and said second ADS-B antenna, and said ADS-B antenna multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said ADS-B receiver, (q) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (r) said radar processor is configured to use the direction of said second ADS-B antenna to determine a bearing to said target, (s) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and (t) said radar processor is configured to display said range and said bearing on said display (claim 3), (claim 8) said radar processor is incorporated into said ADS-B processor (claim 4), (claim 13) system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) a first ADS-B receiver; (c) a first ADS-B antenna; (d) a second ADS-B receiver; (e) a second ADS-B antenna; (0 an antenna controller; (g) an ADS-B antenna multiplexer; (h) an ADS-B processor; (i) a radar processor; (j) a datastream comparator; (k) a display; whereby (1) said second ADS-B antenna is directional and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna, (m) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said first ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said second ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, (n) said ADS-B processor and said radar processor work together, (o) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer, (p) said transmitted signal is reflected by a target producing a reflected signal, (q) said reflected signal is received by either or both said first ADS-B antenna or said second ADS-B antenna, and said ADS-B multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said second ADS-B receiver, (r) said radar processor is configured to process said reflected signal from said second ADS- B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (s) said radar processor is configured to use the direction of said second antenna to determine a bearing to said target, (t) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and (u) said radar processor is configured to display said range and said bearing on said display (claim 3), (claim 16) said radar processor is incorporated into said ADS-B processor (claim 4). **Margolin** does not teach said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal and said datastream comparator is incorporated into said radar processor. **Wu** teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify **Margolin** to include said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new or unexpected results. It would have been obvious to modify Margolin to include said datastream comparator is incorporated into said radar processor because it is merely one method to apply to using multiple processors in a radar device.

4. Claims 9-12 and 17-20 are rejected under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu as applied to claim 5 and 13 above, and further in view of Donovan (US 20100090882). Donovan teaches (claim 9, 11, 17, and 19) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and (claim 10, 12, 18, and 20) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (para 29). It would have been obvious to modify Donovan to include said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array because it is merely an implementation to control the ADS-B antenna with no new or unexpected results.

Allowable Subject Matter

5. Claims 2, 6, and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

6. Applicant's arguments filed 4/4/2016 have been fully considered but they are not persuasive. Applicant argues

7. 1) Wu does not use a data stream.

8. Response: Margolin teaches in paragraph 123 “The time delay between when the TCAS Interrogation signal is sent out by TCAS Interrogation Transmitter 105 and when a transponder signal from other aircraft is received by TCA Transponder Receiver 108 is used to determine the range to the responding aircraft.” The interrogation signal is a data stream because it is communication a request for information. Furthermore, Margolin teaches in paragraphs 129-131“FIG. 3 is a general illustration showing an ADS-B system used as a radar, using omni-directional antennas”, “ADS-B operation is improved by using the signal produced by ADS-B Transmitter 303 as a radar with reflected signals received by ADS-B Receiver 304 under the control of ADS-B Processor 305 and Radar Processor 308.”, and “If the number and range of targets reported by radar do not match the number and range of aircraft reported by ADS-B then there is an aircraft out there that does not have ADS-B or it is broken or has been disabled”. Since Margolin teaches an ADS-B transmitter and receiver and applicant claims the data stream of an ADS-B transmitter. It is inherent that Margolin transmits an ADS-B data stream. Applicant does not describe any further types of data need to be transmitted to be the data stream.

9. 2) Wu’s signal contains no data so it is not a data stream.

10. Response: The data in Wu is the unique delay in the signal that indicates that it is the specific signal transmitted by Wu. Also Wu is merely cited to teach how to determine distance using a transmitted signal and received signal.

11. 3) Wu’s signal is not reflected from a DME transponder, it is rebroadcast by the DME transponder on a different frequency.

12. Response: Wu is merely cited to teach how a correlation is used between a transmitted signal and received signal to determine distance to an object.

13. 4) Wu's invention is very different from applicants and has a different purpose.

14. Response: Wu may have a different invention than the applicant's but the method used to determine distance is the only part of Wu needed to help determine the distance of Margolin.

15. 5) If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

16. Response: Margolin is not being significantly modify by Wu. It is merely using the method of Wu to determine the distance. If the delay of the object is a reflection of the radar signal the calculation used to determine distance is set with the known delay being zero. The motivation for the combination is needing a calculation to determine distance.

17. 6) Donovan teaches away from applicant’s ADS-B radar.

18. Response: Donovan merely teaches the detail of the ADS-B radar and is merely modifying the antenna types of Margolin.

19. 7) This Office Action does not contain any rejections under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre- AIA), 2nd paragraph. Applicant cannot respond to rejections that have not been made.

20. Response: Claims would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TIMOTHY A. BRAINARD whose telephone number is (571)272-2132. The examiner can normally be reached on Monday - Friday 9:00 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tashiana Adams can be reached on (571) 270-5228. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/TIMOTHY A BRAINARD/
Primary Examiner, Art Unit 3648

Notice of References Cited	Application/Control No. 14/146,202	Applicant(s)/Patent Under Reexamination MARGOLIN, JED	
	Examiner TIMOTHY A. BRAINARD	Art Unit 3648	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2011/0156878 A1	06-2011	Wu; Ryan Haoyun	G01S5/0081	340/10.1
*	B	US-2010/0090882 A1	04-2010	Donovan; Timothy P.	G01S13/781	342/32
*	C	US-2011/0169684 A1	07-2011	Margolin; Jed	G01S5/12	342/30
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14146202	MARGOLIN, JED
	Examiner	**Art Unit**
	TIMOTHY A BRAINARD	3648

CPC- SEARCHED

Symbol	Date	Examiner
G01S13/9303; G01S11/02; G01S13/003; G01S5/12; G01S13/42	1/6/2015	TAB

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
342	29, 30, 118	1/6/2016	TAB

SEARCH NOTES

Search Notes	Date	Examiner
updated east search -- see attached	1/6/2015	TAB
updated east search -- see attached	6/1/2016	TAB

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	0	("20100090882" | "20110156878" | "20110169684").PN.	USPAT	OR	OFF	2016/06/01 12:29

EAST Search History (Interference)

<This search history is empty>

6/1/2016 12:29:59 PM
H:\ east workspaces\ 14146202.wsp

Index of Claims	Application/Control No. 14146202	Applicant(s)/Patent Under Reexamination MARGOLIN, JED
	Examiner TIMOTHY A BRAINARD	Art Unit 3648

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/06/2016	06/01/2016							
	1	✓	✓							
	2	✓	O							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	O							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	O							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14146202
Filing Date	02-Jan-2014
First Named Inventor	Jed Margolin
Attorney Docket Number	
Title of Invention	ADS-B Radar

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Jed Margolin	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8643534

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

◉ Small Entity

○ Micro Entity

○ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

○ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number ____________

◉ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Jed Margolin/
Name	Jed Margolin

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14146202
Filing Date:	02-Jan-2014
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Filer:	Jed Margolin
Attorney Docket Number:	

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or Terminal Disclaimer	2814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14146202

Filing Date: 02-Jan-2014

Applicant/Patent under Reexamination: Margolin et al.

Electronic Terminal Disclaimer filed on April 4, 2016

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	25381721
Application Number:	14146202
International Application Number:	
Confirmation Number:	7721
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Customer Number:	23497
Filer:	Jed Margolin
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	04-APR-2016
Filing Date:	02-JAN-2014
Time Stamp:	03:29:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$160
RAM confirmation Number	7724
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33087 cf76b919610eb44e7aa583f03d576f123e1d2697	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29319 28740f8da8456a8af7b9b17b91d2a0ee67b1273b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	62406		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Jed Margolin
Serial No.: 14/146,202
Filed: 01/02/2014
For: ADS-B RADAR

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is in response to the Office Action mailed 1/21/2016 in which the Examiner:

A. Rejected Claims 1-20 on the ground of nonstatutory double patenting as being unpatentable over claims 1-14 of U.S. Patent No. 8,643,534 in view of Wu et al (US 20110156878). (Examiner's Sections 2 and 3.)

B. Rejected Claims 1, 3-5, 7-8, 13, and 15-16 under 35 U.S.C. 103 as being unpatentable over Margolin (US 20110169684) in view of Wu et al (US 20110156878). (Examiner's Sections 4 and 5.)

C. Rejected Claims 9-12 and 17-20 under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu and further in view of Donovan (US 20100090882). (Examiner's Section 6.)

D. Advised Applicant in Examiner's Section 7 that:

> 7. Claims 2, 6, and 14 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

REMARKS

Since Wu is cited in all of the rejections, in order to save unnecessary duplication Wu will be discussed first and referred to in Applicant's responses to the specific rejections.

Applicant will show that Wu teaches away from Applicant's invention and that the use of Wu's DME Interrogator signal as a radar, instead of Applicant's ADS-B Radar, would cripple Applicant's invention.

It will first be noted that:

1. Wu et al (US 20110156878) was issued as U.S. Patent 8,063,744 **System and method for providing timing services and DME aided multilateration for ground surveillance** on November 22, 2011. Since the Examiner references Wu (US 20110156878) Applicant will do the same.

2. Rejection A refers to Margolin (U.S. Patent 8,643,534). Rejections B and C refer to Margolin (US 20110169684). Margolin (US 20110169684) is the published patent application that as a result of a Divisional requirement resulted in U.S. Patent 8,373,591 (issued Feb. 12, 2013) and U.S. Patent 8,643,534 (issued 2/4/2014). U.S. Patent 8,643,534 also had its own Publication Number: US 20130176163 (July 11, 2013). The disclosures in Margolin (US 20110169684) and Margolin (U.S. Patent 8,643,534) are identical.

3. The Examiner's rejections use similar language in citing Wu:

Rejection A:

> Wu teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify U.S. Patent No. 8643534 to include said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new or unexpected results.

Rejection B:

> Wu teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify Margolin to include said datastream comparator is configured to

compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new or unexpected results. It would have been obvious to modify Margolin to include said datastream comparator is incorporated into said radar processor because it is merely one method to apply to using multiple processors in a radar device.

Rejection C references Rejection B regarding Wu:

6. Claims 9-12 and 17-20 are rejected under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu as applied to claim 5 and 13 above, and further in view of Donovan (US 20100090882). Donovan teaches (claim 9, 11, 17, and 19) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and (claim 10, 12, 18, and 20) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (para 29). It would have been obvious to modify Donovan to include said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array because it is merely an implementation to control the ADS-B antenna with no new or unexpected results.

The Examiner cites Wu Paragraphs 7 and 39.

[0007] An interrogation signal containing pseudo-randomly spaced DME pulse pairs is transmitted by the DME interrogator on a DME downlink frequency to the DME transponder, as shown in FIG. 1. Upon receiving the interrogation signal, the DME transponder determines whether the pulse pair of the interrogation signal is valid and when the received interrogation signal is valid the DME transponder replies with a reply signal containing an identical DME pulse pair to the interrogator on a DME uplink frequency after a fixed transponder delay. The DME interrogator receives the reply signal and correlates the received pulse pair in the reply signal with the known pulse pair transmitted in the interrogation signal to determine the total delay time. By subtracting the known transponder delay time (t_d) from the total delay time, dividing the resulting time delay by two, and then multiplying the result by the speed of light, the DME interrogator determines the range from the DME interrogator to the DME transponder.

[0039] A first embodiment of the present invention uses a DME listener to receive interrogation signals transmitted by DME interrogators and reply signals transmitted by DME transponders. The DME listener is a multi-channel DME receiver that includes a processor, a time reference, such as a GPS time receiver, atomic clock or timing reference containing a high precision oscillator, and a transmitter, such as an RF transmitter. The DME listener receives both the interrogation signals transmitted by DME interrogators and the reply signals transmitted by DME transponders within reception range of the DME listener, and then it correlates the two signals to determine a time difference between the time of receiving an interrogation signal from a DME interrogator and the time of receiving the reply signal from the DME transponder that corresponds to the interrogation signal. The present invention then uses the MLAT technique, generally known as the time difference of arrival (TDOA) MLAT technique, to determine the position of the DME interrogator. One embodiment of the present invention also uses data from SSR (Mode A/C/S) transponder systems for retrieving aircraft identity and other SSR transponder information.

Applicant will show that:

1. Wu does not use a datastream. A DME Interrogator in his aircraft transmits DME pulse pair signals with a pseudorandom delay between the pulse pairs. This signal is received by a DME Transponder (on the ground) which retransmits Wu's signal on a different frequency. Wu's Interrogator receives the transmission from the DME Transponder, determines if the delay between the pulse pairs is the same as in the signal he sent, and measures the time delay between transmission and reception. This gives a distance (a slant distance) to the DME Transponder on the ground. Wu's signal contains no data so it is not a datastream.

2. Wu's signal is not reflected from the DME Transponder, it is rebroadcast by the DME Transponder on a different frequency.

<u>Wu's Invention</u>

Wu's invention is very different from Applicant's and has a different purpose.

From Applicant's Paragraph 15:

> **[015]** Therefore, an objective of the present invention is to improve the ADS-B system by using ADS-B as a radar system for sensing aircraft and other objects so that aircraft equipped with ADS-B can detect target aircraft not equipped with ADS-B, or the target aircraft's ADS-B is broken or has been deliberately turned off, or a false ADS-B signal is being emitted.

From Wu's Abstract:

> The present invention utilizes the existing DME transponder system infrastructure to augment existing ground surveillance multilateration (MLAT) capabilities by providing additional measurements for determining the position of an aircraft equipped with a DME transponder. DME listeners receive DME interrogation signals and DME reply signals, determine TDOA between the DME transponder and each DME listener, and transmit data to a central computer that clusters TDOAs between the DME transponder and the DME listeners and computes the aircraft position using the clustered TDOAs. The DME-aided MLAT can be used as a backup surveillance system when GNSS-based systems are unavailable. The DME-aided MLAT can be integrated with SSR receive units (RUs) performing multilateration (MLAT) calculations.

Wu explains DME in Paragraphs 2 - 7:

> **[0002]** DME is a ground-based navigation system which consists of a network of ground transponders and airborne interrogating units (interrogators). The main purpose of DME transponder operations is to allow aircraft to identify and obtain a range to a DME transponder. In operation, an interrogator transmits DME pulse pair signals to be received by an intended ground transponder on a predetermined downlink frequency within the DME frequency band of 962 MHz to 1150 MHz. Upon receiving an interrogation pulse pair signal the ground

transponder determines whether the received signal is a valid interrogation signal by checking the spacing between the two pulses in the DME pulse pair signal. If a valid interrogation is detected, ground transponder transmits a reply signal on a predetermined uplink frequency after a preset delay of approximately 50 us. The reply signal consists of a pulse pair with a fixed spacing that is transmitted on a different predetermined uplink frequency within the DME frequency band. The specific pairing of interrogation and replying frequencies and the spacing between the pulses in the interrogation and replying pulse pair signals defines the DME channel/mode of the DME operation.

[0003] The interrogation and replying operation between an interrogator (e.g., aircraft) and a ground transponder enables the aircraft to determine a range to the transponder based on the observed round-trip delay between the transmission of the interrogation signal and receipt of the reply signal. FIGS. 1 and 2 illustrate the operating principles of legacy DME equipment using the interrogation and reply method of operation.

[0004] There are 126 frequency pairings (Channel #001 ~ #126) and four spacing pairings (Mode X W Y Z) allocated for DME operation within the DME frequency band. Each channel consists of an interrogation frequency band and a replying frequency band that are separated from adjacent bands by 1 MHz. The purpose of defining DME channels and modes is to minimize the co-channel interference between adjacent DME transponders. It is important that adjacent DME transponders operate either on a different frequency or use different modes when operating on the same uplink or down link frequency.

[0005] Since the DME frequency range includes the uplink and downlink Secondary Surveillance Radar (SSR) frequency bands, the DME channels that are within these SSR frequency bands need to be reserved from usage for sites whose operating coverage area (including both interrogation and replying) overlaps with the coverage area of an operating SSR. The FAA Next Generation (NextGen) Automatic Dependent Surveillance--Broadcast (ADS-B) surveillance system, which is largely built upon SSR links, includes DME channels that overlap the SSR frequencies and these overlapping DME channels cannot be assigned to any DME operations.

[0006] Interrogation signals consist of pseudo-randomly spaced DME pulse pairs. The interrogation and reply pulses are modulated at different frequencies to minimize interference.

[0007] An interrogation signal containing pseudo-randomly spaced DME pulse pairs is transmitted by the DME interrogator on a DME downlink frequency to the DME transponder, as shown in FIG. 1. Upon receiving the interrogation signal, the DME transponder determines whether the pulse pair of the interrogation signal is valid and when the received interrogation signal is valid the DME transponder replies with a reply signal containing an identical DME pulse pair to the interrogator on a DME uplink frequency after a fixed transponder delay. The DME interrogator receives the reply signal and correlates the received pulse pair in the reply signal with the known pulse pair transmitted in the interrogation signal to determine the total delay time. By subtracting the known transponder delay time (t_d) from the total delay time, dividing the resulting time delay by two, and then multiplying the result by the speed of light, the DME interrogator determines the range from the DME interrogator to the DME transponder.

Wu has described the DME system that has existed for several decades. He does not claim to have invented it. See Appendix A - **Distance Measuring Equipment** from Wikipedia.

Thus:

1. DME is a ground-based navigation system which consists of a network of ground transponders and airborne interrogating units (interrogators). The main purpose of DME transponder operations is to allow aircraft to identify and obtain a range to a DME transponder.

2. In operation, an interrogator (on an aircraft) transmits DME pulse pair signals to be received by an intended ground transponder on a predetermined downlink frequency within the DME frequency band of 962 MHz to 1150 MHz.

3. Upon receiving an interrogation pulse pair signal the ground transponder determines whether the received signal is a valid interrogation signal by checking the spacing between the two pulses in the DME pulse pair signal. If a valid interrogation is detected, ground transponder transmits a reply signal on a predetermined uplink frequency after a preset delay of approximately 50 us. The reply signal consists of a pulse pair with a fixed spacing that is transmitted on a different predetermined uplink frequency within the DME frequency band.

4. The interrogation and replying operation between an interrogator (e.g., aircraft) and a ground transponder enables the aircraft to determine a range to the transponder based on the observed round-trip delay between the transmission of the interrogation signal and receipt of the reply signal.

5. There are 126 frequency pairings (Channel #001 ~ #126) and four spacing pairings (Mode X W Y Z) allocated for DME operation within the DME frequency band. Each channel consists of an interrogation frequency band and a replying frequency band that are separated from adjacent bands by 1 MHz.

6. From Paragraph 6: Interrogation signals consist of pseudo-randomly spaced DME pulse pairs. The interrogation and reply pulses are modulated at different frequencies to minimize interference.

7. From Paragraph 8: The DME interrogation signals containing pseudo-randomly spaced DME pulse pairs do not carry any information other than the unique randomness that is only meaningful to the DME interrogator. Later, discussing the embodiment that provides time synchronization (Paragraph 85) Wu mentions:

> [0085] Since the conventional DME signal does not encode any information, the time synchronization must be operated on the pulse positions when using DME signals for reference transmitter purposes. The DME pulse timestamps produced by different ground stations provide the basis of time corrections of the WAM measurement timestamps among different ground stations.

Wu uses the conventional DME signal which does not encode any information. It carries only the unique randomness between the two pulse pairs that it sends out.

8. From Paragraph 9: While the main purpose of the DME Transponder is to reply to the interrogation signals from aircraft, the DME Transponder also broadcasts its identity periodically. In accordance with international standards, approximately every 40 seconds, each transponder broadcasts its station ID using International Morse code in a time period not exceeding 10 seconds.

9. Therefore, as long as there is a DME Transponder (a ground installation) within range (preferably at least three DME Transponders within range) an aircraft can determine its location.

Wu alludes to ADS-B in Paragraph 5. In Paragraph 12 Wu observes:

> [0012] The next generation (NextGen) national airspace system (NAS) relies on GNSS-based surveillance systems (i.e., GPS) to provide aircraft position information both on the ground and airborne to the ground for surveillance and control purposes. However, existing GNSS-based surveillance systems can be disrupted by solar storms that cause severe ionosphere delay variations that degrade both GPS and WAAS and affect L1 and L5. Current correction broadcasting cannot keep up with the rapid variations in times of solar storms. In addition, there are practical concerns regarding intentional and unintentional interference, regional and temporal unavailability of GPS services, thereby causing a severe degradation or loss of GNSS-based surveillance capability.

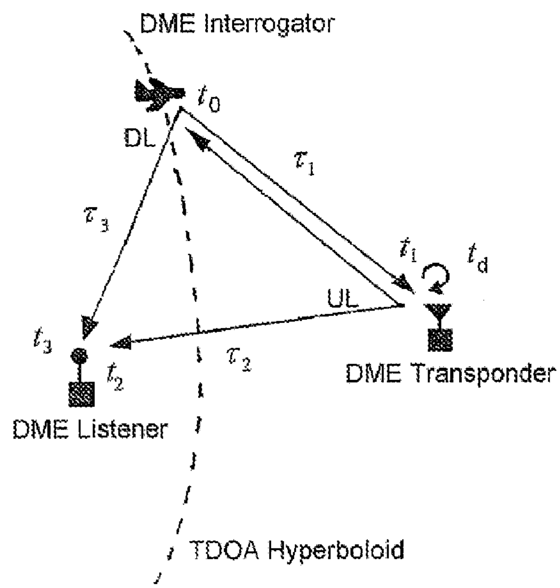
ADS-B uses GPS (Global Positioning System) which is a specific type of GNSS (Global Navigation Satellite System). GPS is not the only GNSS system. The other types are not relevant here.

Wu then noted in Paragraph 13:

> [0013] What is needed is a system and method that provides a ground surveillance capability for determining aircraft position in the NAS (National Airspace System) as a backup to or to augment the existing GNSS-based surveillance systems.

Wu's Figure 3 will help in understanding his invention.

FIG. 3



The Examiner cites Wu's first embodiment (Paragraph 39).

> **[0039]** A first embodiment of the present invention uses a DME listener to receive interrogation signals transmitted by DME interrogators and reply signals transmitted by DME transponders. The DME listener is a multi-channel DME receiver that includes a processor, a time reference, such as a GPS time receiver, atomic clock or timing reference containing a high precision oscillator, and a transmitter, such as an RF transmitter. The DME listener receives both the interrogation signals transmitted by DME interrogators and the reply signals transmitted by DME transponders within reception range of the DME listener, and then it correlates the two signals to determine a time difference between the time of receiving an interrogation signal from a DME interrogator and the time of receiving the reply signal from the DME transponder that corresponds to the interrogation signal. The present invention then uses the MLAT technique, generally known as the time difference of arrival (TDOA) MLAT technique, to determine the position of the DME interrogator. One embodiment of the present invention also uses data from SSR (Mode A/C/S) transponder systems for retrieving aircraft identity and other SSR transponder information.

Wu introduces a DME Listener which listens to the conversation between the DME Interrogator (aircraft) and at least one DME Transponder (on the ground). The DME Listener gathers this information and sends it to a central computer.

From Paragraph 19:

> The central computer receives at least the determined TDOA interrogation pattern information, and DME listener ID from the at least one DME listener, associates the determined TDOA to a specific transmission of interrogation pulses from the at least one DME interrogator using the interrogation pattern information to form a TDOA cluster, and determines a position for the at least one DME interrogator when three or more TDOAs are clustered.

Difference Between Wu's Invention and Applicant's Invention

1. Wu's invention is for the purpose of determining an aircraft's location for ground surveillance. It is the central computer that performs the calculations needed to determine the aircraft's location and Wu does not make it clear what the central computer does with this information. Presumably, the central computer reports this information to ATC. The aircraft is identified by using data from SSR (Mode A/C/S) transponder systems. Unless Wu's data is reported to the aircraft this does not help the pilot determine his/her location or the location of aircraft or other objects in his/her vicinity.

Wu's invention is for aircraft that want to be located. If an aircraft does not want to be located it can simply turn off its DME transmitter and Mode A/C/S transponder.

Applicant's invention is for improving the ADS-B system by using ADS-B as a radar system for sensing **other** aircraft and objects so that aircraft equipped with ADS-B can detect target aircraft not equipped with ADS-B, or the target aircraft's ADS-B is broken or has been deliberately turned off, or a false ADS-B signal is being emitted.

Note that Applicant's invention performs its intended function even if GPS is malfunctioning since only the first 40us of the ADS-B message is needed to identify a reflected signal. Referring to Figure 4 of the current Application, the first 8us of the ADS-B message is the Preamble, followed by the DF (Downlink Format) of 5 bits (5us), and then the CA (which indicates information about the capabilities of employed transponder) of 3 bits (3us). Then comes the AA field which carries the unique ICAO aircraft address which identifies the aircraft. The AA field is 24 bits (24us). Then comes the ME field which contains positional and other data. The ME field is 56 bits (56us). The ADS-B message ends with the 24-bit CRC field (24us) which allows recipients to detect and correct up to 5 bit errors in the transmission. The aircraft's ADS-B signal being used as a radar is completely identified by the AA data which identifies the aircraft. The data in the ME field does not have to be accurate. Indeed, the signal can be identified without the entire AA data although having less AA data makes identification less reliable.

2. Wu's DME Interrogator signal (transmitted by the aircraft) is received by a DME Transponder station (on the ground) which retransmits the received signal on another frequency. This is the signal that Wu receives. Wu does not receive a radar reflection which would be at the same frequency that he transmits (except for a possible Doppler shift).

Applicant's invention uses the ADS-B signal transmitted by the aircraft as a radar.

a. The signal is reflected by other aircraft and other objects. This reflected signal is then received by the originating aircraft which uses it to determine the range and direction to these other aircraft and other objects. These other aircraft and other objects do not participate in this process other than by physically being there. They are detected whether they want to be detected or not.

b. No ground installations are used.

c. Since a reflected signal is detected, it is on the same frequency (other than a possible Doppler shift) as the signal transmitted by the originating aircraft.

3. Applicant uses a datastream comprising the standard ADS-B message. Wu does not use a datastream. Wu uses the standard DME interrogation signal containing pseudo-randomly spaced DME pulse pairs. As Wu states, these pulse pairs do not encode any information. (Wu Paragraphs 8 and 85.)

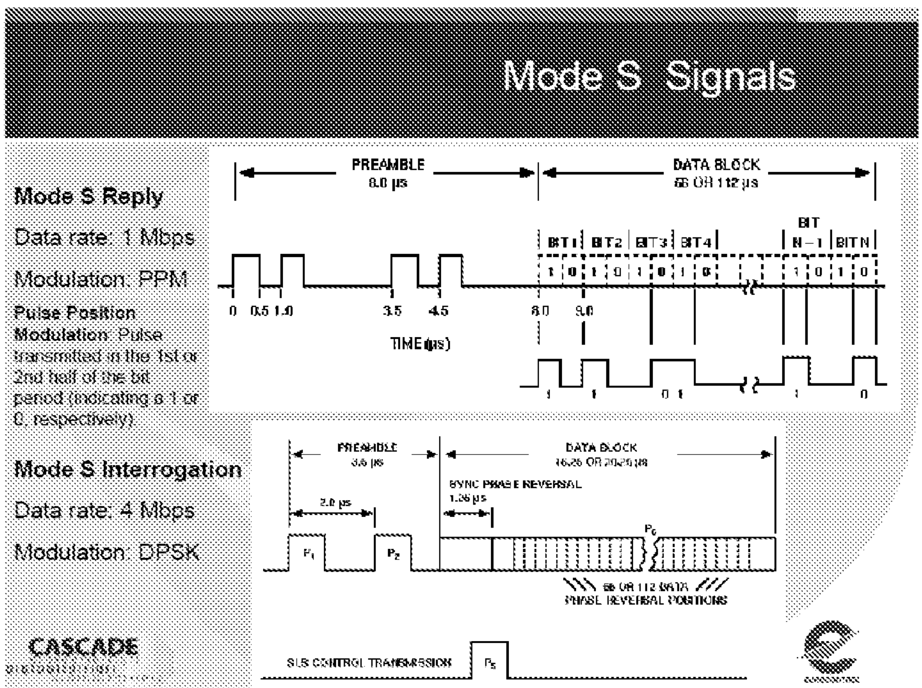
Using Wu's DME signal as a radar, while perhaps feasible, would change Applicant's ADS-B Radar into a less useful DME Radar, which is a different invention. It would be less useful because:

a. The DME signal is identified only by the time between the pulse pairs. During the time between the pulse pairs there is no signal, meaning no carrier, no data. DME is a component of TACAN, a tactical air navigation system used by military aircraft. (See Appendix B - **Tactical Air Navigation System** from Wikipedia.). The TACAN specification calls for essentially no signal during the period between pulse pairs. (The specification says 20 dB below the pulse pair amplitudes. See

Appendix C - **MIL-STD-291C STANDARD TACTICAL AIR NAVIGATION (TACAN) SIGNAL.** Section 5.1.3.)

<u>**b.**</u> A DME Interrogator sends out pulse pairs at a rate of 150 pulse pairs/sec in Search Mode and 30 pulse pairs/sec in Track Mode. (See Appendix A - **Distance Measuring Equipment** from Wikipedia.) As a result, the DME Interrogator signal is much more likely to be interfered with by the DME Interrogator signals from other aircraft. While the DME Interrogator could change channels and try again it might take some time to find an unused channel. (DME has a range of 200nmi.)

<u>**c.**</u> ADS-B broadcasts its message using the Mode S protocol shown below. (The graphic comes from a good article with the unfortunate title of **ADS-B For Dummies**. See Appendix D.)



The protocol uses Pulse Position Modulation: A pulse transmitted in the first half of the bit period indicates a "1" while a pulse transmitted in the second half of the bit period indicates a "0". The pulses are produced using Differential Phase Shift Keying (DPSK) of a carrier. For an explanation of DPSK see Appendix E **Mode S - Differential Phase shift Keying (DPSK).**

The point is that the ADS-B message is a stream of data, i.e. a datastream, while Wu's DME transmission is not a stream of data. It is not a datastream.

The chances of a signal collision between two aircraft broadcasting their ADS-B messages can be reduced simply by following the dictum, "Listen before talking."

In addition, Applicant's ADS-B Radar detects when a target with ADS-B is misreporting its position or if an ADS-B transmission is being spoofed. These situations are brought to the pilot's attention as attention items.

Therefore, as shown above, Wu teaches away from Applicant's invention and the use of Wu's DME Interrogator signal as a radar would cripple Applicant's invention.

4. Case law that applies here is *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. (Claimed device was a blood filter assembly for use during medical procedures wherein both the inlet and outlet for the blood were located at the bottom end of the filter assembly, and wherein a gas vent was present at the top of the filter assembly. The prior art reference taught a liquid strainer for removing dirt and water from gasoline and other light oils wherein the inlet and outlet were at the top of the device, and wherein a pet-cock (stopcock) was located at the bottom of the device for periodically removing the collected dirt and water. The reference further taught that the separation is assisted by gravity. The Board concluded the claims were prima facie obvious, reasoning that it would have been obvious to turn the reference device upside down. The court reversed, finding that if the prior art device was turned upside down it would be inoperable for its intended purpose because the gasoline to be filtered would be trapped at the top, the water and heavier oils sought to be separated would flow out of the outlet instead of the purified gasoline, and the screen would become clogged.).

Moreover, Applicant respectfully submits that this is an improper combination of references, in that, when taken as a whole, there is no motivation or suggestion to combine the references to achieve the Applicant's claimed invention. Section 2143.01 of the MPEP states: "The mere fact that references can be combined or modified is not sufficient to establish prima facie obviousness."

In Applicant's invention the Person having Ordinary Skill In The Art (POSITA) would be a person who is familiar with and understands the details of the different avionics systems involved: ADS-B, TACAN, DME, Mode A/C/S transponders, etc. A POSITA would understand that the DME

Interrogator and DME Transponder signals do not constitute a datastream and that substituting Wu's DME Interrogator or DME Transponder signals for Applicant's ADS-B signals would cripple Applicant's invention.

Applicant's Response to the Specific Rejections

A. The Examiner rejected Claims 1-20 on the ground of nonstatutory double patenting as being unpatentable over claims 1-14 of U.S. Patent No. 8,643,534 in view of Wu et al (US 20110156878). (Examiner's Sections 2 and 3.) The Examiner further stated:

> Wu teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify U.S. Patent No. 8643534 to include said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new or unexpected results.

Applicant's Response

Applicant has shown in the above section **Wu's Invention** that:

1. Wu does not use a datastream. A DME Interrogator in his aircraft transmits DME pulse pair signals with a pseudorandom delay between the pulse pairs. This signal is received by a DME Transponder (on the ground) which retransmits Wu's signal on a different frequency. Wu's Interrogator receives the transmission from the DME Transponder, determines if the delay between the pulse pairs is the same as in the signal he sent, and measures the time delay between transmission and reception. This gives a distance (a slant distance) to the DME Transponder on the ground. Wu's signal contains no data so it is not a datastream.

2. Wu's signal is not reflected from the DME Transponder, it is rebroadcast by the DME Transponder on a different frequency.

3. Wu teaches away from Applicant's invention and the use of Wu's DME Interrogator signal as a radar, instead of Applicant's ADS-B Radar, would cripple Applicant's invention.

4. Case law that applies here is *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

Moreover, Applicant respectfully submits that this is an improper combination of references, in that, when taken as a whole, there is no motivation or suggestion to combine the references to achieve the Applicant's claimed invention. Section 2143.01 of the MPEP states: "The mere fact that references can be combined or modified is not sufficient to establish prima facie obviousness."

In Applicant's invention a POSITA would understand that the DME Interrogator and DME Transponder signals do not constitute a datastream and that substituting Wu's DME Interrogator or DME Transponder signals for Applicant's ADS-B signals would cripple Applicant's invention.

As a result Claims 1 - 20 stand as filed.

Nonetheless, in order to move the case forward Applicant has filed an eTerminal Disclaimer.

However, it should be understood the filing of the terminal disclaimer to obviate the rejection based on nonstatutory double patenting is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991). The court indicated that the "filing of a terminal disclaimer simply serves the statutory function of removing the rejection of double patenting, and raises neither a presumption nor estoppel on the merits of the rejection."

B. Claims 1, 3-5, 7-8, 13, and 15-16 were rejected under 35 U.S.C. 103 as being unpatentable over Margolin (US 20110169684) in view of Wu et al (US 20110156878). (Examiner's Sections 4 and 5.)

The Examiner again cites Wu Paragraphs 7 and 39.

> Wu teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify Margolin to include said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new

or unexpected results. It would have been obvious to modify Margolin to include said datastream comparator is incorporated into said radar processor because it is merely one method to apply to using multiple processors in a radar device.

Applicant's Response

Applicant has shown in the above section **Wu's Invention** that:

1. Wu does not use a datastream. A DME Interrogator in his aircraft transmits DME pulse pair signals with a pseudorandom delay between the pulse pairs. This signal is received by a DME Transponder (on the ground) which retransmits Wu's signal on a different frequency. Wu's Interrogator receives the transmission from the DME Transponder, determines if the delay between the pulse pairs is the same as in the signal he sent, and measures the time delay between transmission and reception. This gives a distance (a slant distance) to the DME Transponder on the ground. Wu's signal contains no data so it is not a datastream.

2. Wu's signal is not reflected from the DME Transponder, it is rebroadcast by the DME Transponder on a different frequency.

3. Wu teaches away from Applicant's invention and the use of Wu's DME Interrogator signal as a radar, instead of Applicant's ADS-B Radar, would cripple Applicant's invention.

4. Case law that applies here is *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

Moreover, the Applicant respectfully submits that this is an improper combination of references, in that, when taken as a whole, there is no motivation or suggestion to combine the references to achieve the Applicant's claimed invention. Section 2143.01 of the MPEP states: "The mere fact that references can be combined or modified is not sufficient to establish prima facie obviousness."

In Applicant's invention a POSITA would understand that the DME Interrogator and DME Transponder signals do not constitute a datastream and that substituting Wu's DME Interrogator or DME Transponder signals for Applicant's ADS-B signals would cripple Applicant's invention.

Applicant has traversed the rejection of Independent Claims 1, 5, and 13. Dependant Claims 2, 3, and 4 are based on and limited by Independent Claim 1. Dependant Claims 6 - 12 are based on and limited by Independent Claim 5. Dependent Claims 14 - 20 are based on and limited by Independent Claim 13,

Having traversed the rejection of Independent Claims 1, 5, and 13 Claims 1 - 20 stand as filed.

____

C. Claims 9-12 and 17-20 were rejected under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu and further in view of Donovan (US 20100090882). (Examiner's Section 6.) The Examiner stated:

> 6. Claims 9-12 and 17-20 are rejected under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu as applied to claim 5 and 13 above, and further in view of Donovan (US 20100090882). Donovan teaches (claim 9, 11, 17, and 19) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and (claim 10, 12, 18, and 20) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (para 29). It would have been obvious to modify Donovan to include said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array because it is merely an implementation to control the ADS-B antenna with no new or unexpected results.

Applicant's Response:

Applicant has shown in the above section **Wu's Invention** that:

1. Wu does not use a datastream. A DME Interrogator in his aircraft transmits DME pulse pair signals with a pseudorandom delay between the pulse pairs. This signal is received by a DME Transponder (on the ground) which retransmits Wu's signal on a different frequency. Wu's Interrogator receives the transmission from the DME Transponder, determines if the delay between the pulse pairs is the same as in the signal he sent, and measures the time delay between transmission and reception. This gives a distance (a slant distance) to the DME Transponder on the ground. Wu's signal contains no data so it is not a datastream.

2. Wu's signal is not reflected from the DME Transponder, it is rebroadcast by the DME Transponder on a different frequency.

3. Wu teaches away from Applicant's invention and the use of Wu's DME Interrogator signal as a radar, instead of Applicant's ADS-B Radar, would cripple Applicant's invention.

4. Case law that applies here is *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

Moreover, the Applicant respectfully submits that this is an improper combination of references, in that, when taken as a whole, there is no motivation or suggestion to combine the references to achieve the Applicant's claimed invention. Section 2143.01 of the MPEP states: "The mere fact that references can be combined or modified is not sufficient to establish prima facie obviousness."

In Applicant's invention a POSITA would understand that the DME Interrogator and DME Transponder signals do not constitute a datastream and that substituting Wu's DME Interrogator or DME Transponder signals for Applicant's ADS-B signals would cripple Applicant's invention.

Having traversed the rejection of Independent Claims 1, 5, and 13 over Wu they stand as filed. Regarding the part of the rejection directed to Donovan (claim 9, 11, 17, and 19).

Referring to Donovan Figure 1, Donovan has:

1. A Secondary Surveillance Radar (SSR);
2. A first aircraft, which is equipped with an ADS-B system and a Mode A/C/S Transponder;
3. A second aircraft, which is not equipped with ADS-B but which has a Mode A/C/S Transponder;
4. A Bi-Static Receiver.

The SSR interrogates the Mode A/C/S Transponder in the first aircraft (which has a Mode A/C/S Transponder as well as ADS-B). The SSR also interrogates the Mode A/C/S Transponder in the second aircraft (which has a Mode A/C/S Transponder but no ADS-B). By doing this, the SSR has the range, altitude, and bearing for both aircraft.

The first aircraft (which has ADS-B) broadcasts its position.

The Bi-Static Receiver is listening to the SSR interrogations, the Mode A/C/S replies from both aircraft, and the ADS-B position of the first aircraft. (If it were to communicate with SSR it would also have the range and bearing from SSR to the two aircraft.) The Bi-Static Receiver applies bi-static methods to determine the position of the second aircraft (the one without ADS-B).

Presumably, Donovan's system produces a more accurate position for the second aircraft (the one without ADS-B) than just using SSR. For an explanation of SSR see Appendix F **Secondary Surveillance Radar** from Wikipedia.

But there are some questions begging to be to be asked.

1. What if there is no first aircraft (the one with ADS-B) in the vicinity?

2. Is Donovan's system more accurate than just using SSR?

Donovan's invention is very different from Applicant's. Applicant does not require Donovan's SSR or Bi-Static Receiver. Moreover, Donovan requires the cooperation of the second aircraft (the one without ADS-B). The second aircraft needs to have a Mode A/C/S Transponder and have it turned on. It has to want to be found. Therefore, Donovan teaches away from Applicant's ADS-B Radar.

Applicant's Claims 9 and 11 are Dependent Claims based on and limited by Independent Claim 5. The Examiner does not allege that Donovan teaches the combination of the elements in Claims 5 and 9 or Claims 5 and 11.

Claims 17 and 19 are Dependent Claims based on and limited by Independent Claim 13. The Examiner does not allege that Donovan teaches the combination of the elements in Claims 13 and 17 or Claims 13 and 19.

Therefore, Claims 1 - 20 stand as filed.

D. Advised Applicant that (Examiner's Section 7):

> 7. Claims 2, 6, and 14 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Applicant's Response:

This Office Action does not contain any rejections under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), 2nd paragraph. Applicant cannot respond to rejections that have not been made.

If the Examiner meant the rejections made under 35 U.S.C. 103, Applicant believes he has traversed the rejections and no amendments are necessary.

CONCLUSION

For the above reasons Claims 1 - 20 stand as filed and it is respectfully submitted that this application is now in condition for allowance and notice of same is requested.

Respectfully submitted,

/Jed Margolin/ Date: April 4, 2016

Jed Margolin

Jed Margolin
1981 Empire Rd.
Reno, NV 89521-7430
775-847-7845

Appendices

Appendix A

Distance Measuring Equipment

Downloaded from Wikipedia 4/1/2016

https://en.wikipedia.org/wiki/Distance_measuring_equipment

Appendix B

Tactical Air Navigation System

Downloaded from Wikipedia 4/1/2016

https://en.wikipedia.org/wiki/Tactical_air_navigation_system

Appendix C

MIL-STD-291C STANDARD TACTICAL AIR NAVIGATION (TACAN) SIGNAL

http://everyspec.com/MIL-STD/MIL-STD-0100-0299/download.php?spec=MIL-STD-291C.011561.pdf

Appendix D

ADS-B For Dummies

www.ssd.dhmi.gov.tr/getBinaryFile.aspx?Type=3&dosyaID=195

Appendix E

Mode S - Differential Phase shift Keying (DPSK)

http://www.radartutorial.eu/13.ssr/sr23.en.html

Appendix F

Secondary Surveillance Radar

Downloaded from Wikipedia 4/2/2016

https://en.wikipedia.org/wiki/Secondary_surveillance_radar

Appendix A

Distance Measuring Equipment (DME)

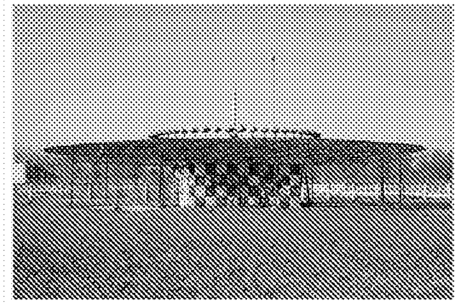
Downloaded from Wikipedia 4/1/2016

https://en.wikipedia.org/wiki/Distance_measuring_equipment

Distance measuring equipment

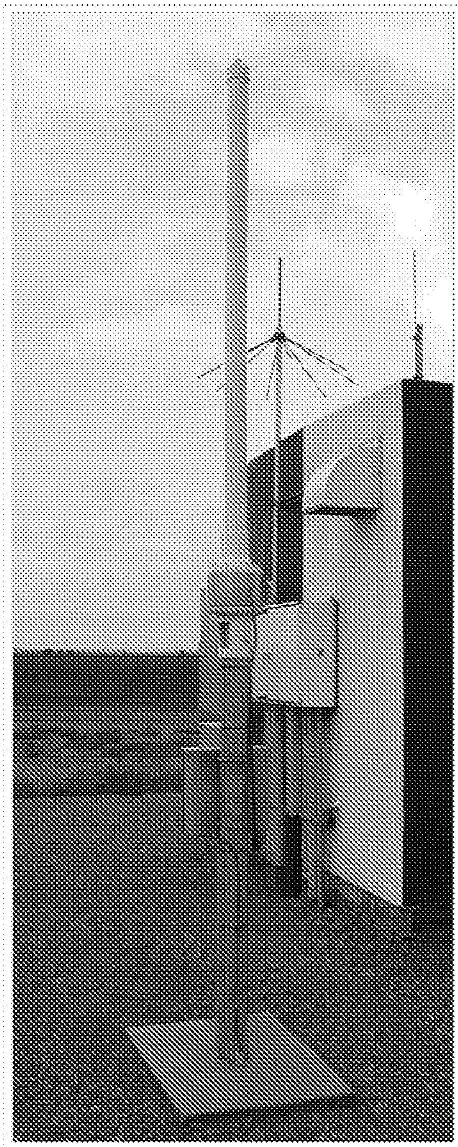
From Wikipedia, the free encyclopedia

Distance measuring equipment (DME) is a transponder-based radio navigation technology that measures slant range distance by timing the propagation delay of VHF or UHF radio signals.


D-VOR/DME ground station

Developed in Australia, it was invented by James *Gerry* Gerrand [1] under the supervision of Edward George "Taffy" Bowen while employed as Chief of the Division of Radiophysics of the Commonwealth Scientific and Industrial Research Organisation (CSIRO). Another engineered version of the system was deployed by Amalgamated Wireless Australasia Limited in the early 1950s operating in the 200 MHz VHF band. This Australian domestic version was referred to by the Federal Department of Civil Aviation as DME(D) (or DME Domestic), and the later international version adopted by ICAO as DME(I).

DME is similar to secondary radar, except in reverse. The system was a post-war development of the IFF (identification friend or foe) systems of World War II. To maintain compatibility, DME is functionally identical to the distance measuring component of TACAN.


DME antenna beside the DME Transponder shelter

Contents

Operation

Aircraft use DME to determine their distance from a land-based transponder by sending and receiving pulse pairs – two pulses of fixed duration and separation. The ground stations are typically collocated with VORs. A typical DME ground transponder system for en-route or terminal navigation will have a 1 kW peak pulse output on the assigned UHF channel.

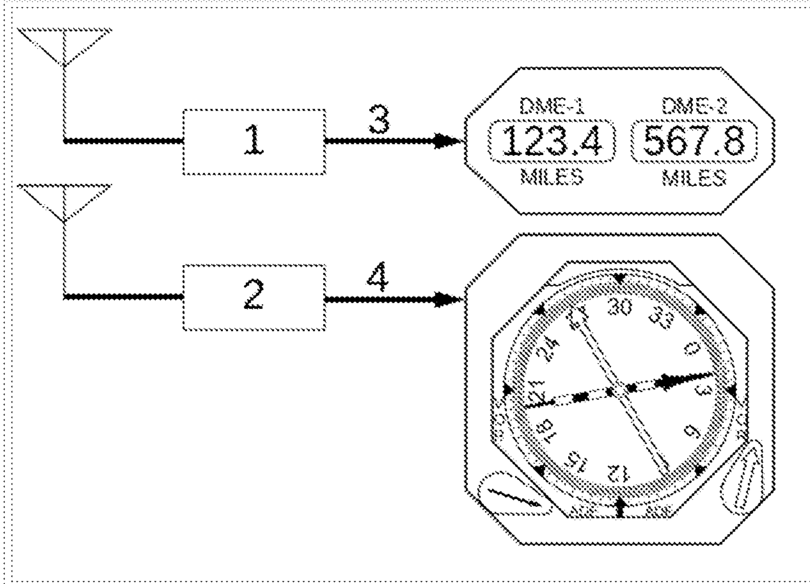
Appendix - 3

A low-power DME can be collocated with an ILS glide slope antenna installation where it provides an accurate distance to touchdown function, similar to that otherwise provided by ILS marker beacons.

Hardware

The DME system comprises a UHF transmitter/receiver (interrogator) in the aircraft and a UHF receiver/transmitter (transponder) on the ground.

Timing



DME distance and VOR/ADF cockpit display instruments

SEARCH MODE: 150 interrogation pulse-pairs per second.

The aircraft interrogates the ground transponder with a series of pulse-pairs (interrogations) and, after a precise time delay (typically 50 microseconds), the ground station replies with an identical sequence of pulse-pairs. The DME receiver in the aircraft searches for reply pulse-pairs (X-mode= 12 microsecond spacing) with the correct interval and reply pattern to its original interrogation pattern. (Pulses-pairs that are not coincident with the individual aircraft's interrogation pattern e.g. not synchronous, are referred to as filler pulse-pairs, or Squitter. Also, replies to other aircraft that are therefore non-synchronous also appear as squitter).

TRACK MODE: less than 30 interrogation Pulse-pairs per second, as the average amount of pulses in SEARCH and TRACK is limited to max 30 Pulse Pairs per second.

The aircraft interrogator locks on to the DME ground station once it recognizes a particular reply pulse sequence has the same spacing as the original interrogation sequence. Once the receiver is locked on, it has a narrower window in which to look for the echoes and can retain lock.

Distance calculation

A radio signal takes approximately 12.36 microseconds to travel 1 nautical mile (1,852 m) to the target and back—also referred to as a radar-mile. The time difference between interrogation and reply, minus the 50 microsecond ground transponder delay, is measured by the interrogator's timing circuitry and converted to a distance measurement (slant range), in nautical miles, then displayed on the cockpit DME display.

The distance formula, *distance = rate * time*, is used by the DME receiver to calculate its distance from the DME ground station. The rate in the calculation is the velocity of the radio pulse, which is the speed of light (roughly 300,000,000 m/s or 186,000 mi/s). The time in the calculation is *(total time – 50μs)/2*.

Accuracy

The accuracy of DME ground stations is 185 m (±0.1 nmi).[2] It's important to understand that DME provides the physical distance from the aircraft to the DME transponder. This distance is often referred to as 'slant range' and depends trigonometrically upon both the altitude above the transponder and the ground distance from it.

For example, an aircraft directly above the DME station at 6,076 ft (1 nmi) altitude would still show 1.0 nmi (1.9 km) on the DME readout. The aircraft is technically a mile away, just a mile straight up. Slant range error is most pronounced at high altitudes when close to the DME station.

Radio-navigation aids must keep a certain degree of accuracy, given by international standards, FAA,[3] EASA, ICAO, etc. To assure this is the case, flight inspection organizations check periodically critical parameters with properly equipped aircraft to calibrate and certify DME precision.

ICAO recommends accuracy of less than the sum of 0.25 nmi plus 1.25% of the distance measured.

Specification

A typical DME transponder can provide distance information to 100 to 200 aircraft at a time. Above this limit the transponder avoids overload by limiting the sensitivity of the receiver. Replies to weaker more distant interrogations are ignored to lower the transponder load.

Radio frequency and modulation data

DME frequencies are paired to VHF omnidirectional range (VOR) frequencies and a DME interrogator is designed to automatically tune to the corresponding DME frequency when the associated VOR frequency is selected. An airplane's DME interrogator uses frequencies from 1025 to 1150 MHz. DME transponders transmit on a channel in the 962 to 1213 MHz range and receive on a corresponding channel between 1025 to 1150 MHz. The band is divided into 126 channels for interrogation and 126 channels for reply. The interrogation and reply frequencies always differ by 63 MHz. The spacing of all channels is 1 MHz with a signal spectrum width of 100 kHz.

Technical references to X and Y channels relate only to the spacing of the individual pulses in the DME pulse pair, 12 microsecond spacing for X channels and 30 microsecond spacing for Y channels.

DME facilities identify themselves with a 1,350 Hz morse code three letter identity. If collocated with a VOR or ILS, it will have the same identity code as the parent facility. Additionally, the DME will identify itself between those of the parent facility. The DME identity is 1,350 Hz to differentiate itself from the 1,020 Hz tone of the VOR or the ILS localizer.

Terminal DME

A terminal DME, referred to as a TDME in navigational charts, is a DME that is designed to provide a 0 reading at the threshold point of the runway, regardless of the physical location of the equipment. It is typically associated with ILS or other instrument approach.

Future

DME operation will continue and possibly expand as an alternate navigation source to space-based navigational systems such as GPS and Galileo.[4]

See also

- Global Positioning Satellite (GPS)
- Instrument flight rules (IFR)
- Transponder Landing System (TLS)
- Instrument Landing System (ILS)
- Non-directional beacon (NDB)
- Tactical Air Navigation (TACAN)
- VHF omnidirectional range (VOR)
- Squitter

References

1. http://www.smh.com.au/national/obituaries/engineer-exploded-myths-in-many-fields-20130108-2cell.html
2. Department of Defense and Department of Transportation (December 2001). "2001 Federal Radionavigation Systems" (PDF). Retrieved 5 July 2011.
3. Federal Aviation Administration (2 September 1982). "U.S. National Aviation Standard for the VOR/DME /TACAN Systems".
4. Department of Defense, Department of Homeland Security and Department of Transportation (January 2009). "2008 Federal Radionavigation Plan" (PDF). Retrieved 8 September 2010.

External links

- DME Basics (http://www.avweb.com/news/avionics/183230-1.html)
- UK Navaids Gallery with detailed Technical Descriptions of their operation (http://www.trevord.com /navaids/)
- Flash based instrument simulator with DME (http://www.luizmonteiro.com/Learning_VOR_Sim_2.aspx)
- U.S. National Aviation Handbook for the VOR/DME/TACAN Systems (http://www.faa.gov /regulations_policies/orders_notices/index.cfm/go/document.information/documentID/12082)
- ICAO Annex 10 Volume 1 International Standards & Recommended Practices (http://www.icao.int/)

Categories: Aircraft instruments | Radio navigation | Aids to navigation | Length, distance, or range measuring devices

Appendix B

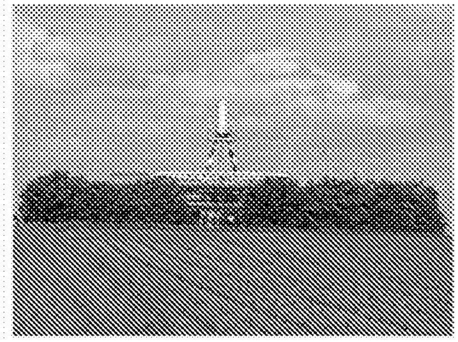
Tactical Air Navigation System (TACAN)

https://en.wikipedia.org/wiki/Tactical_air_navigation_system

Tactical air navigation system

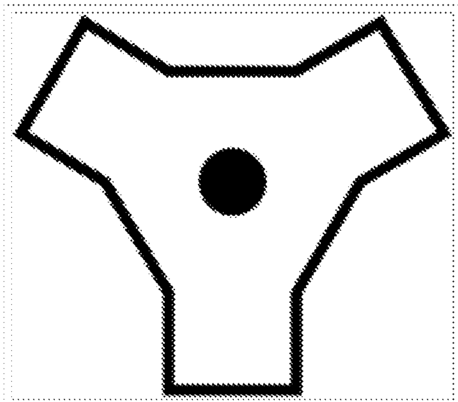
From Wikipedia, the free encyclopedia

A **tactical air navigation system**, commonly referred to by the acronym **TACAN**, is a navigation system used by military aircraft. It provides the user with bearing and distance (slant-range) to a ground or ship-borne station. It is a more accurate version of the VOR/DME system that provides bearing and range information for civil aviation. The DME portion of the TACAN system is available for civil use; at VORTAC facilities where a VOR is combined with a TACAN, civil aircraft can receive VOR/DME readings. Aircraft equipped with TACAN avionics can use this system for en route navigation as well as non-precision approaches to landing fields. The space shuttle is one such vehicle that was designed to use TACAN navigation but later upgraded with GPS as a replacement.[1]



VORTAC TGO (TANGO) Germany. The TACAN antenna is the highest antenna in the center of the image.

The typical TACAN onboard user panel has control switches for setting the channel (corresponding to the desired surface station's assigned frequency), the operation mode for either Transmit/Receive (T/R, to get both bearing and range) or Receive Only (REC, to get bearing but not range). Capability was later upgraded to include an Air-to-Air mode (A/A) where two airborne users can get relative slant-range information. Depending on the installation, Air-to-Air mode may provide range, closure (relative velocity of the other unit), and bearing,[2] though an air-to-air bearing is noticeably less precise than a ground-to-air bearing. A TACAN equipped aircraft cannot receive bearing information from a VOR station.



This symbol denotes a TACAN installation on an aeronautical chart.

Contents

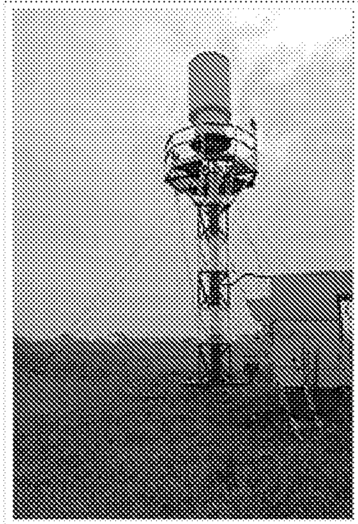
History

The TACAN navigation system is an evolution of radio transponder navigation systems that date back to the British Oboe system of World War II. In the United States many companies were involved with the development of TACAN for military aircraft. Hoffman Electronics- Military Products Division (now NavCom

Defense Electronics (http://www.navcom.com/) was a leader in developing the present TACAN system in the US starting in the late 1950s.

Operation

TACAN in general can be described as the military version of the VOR/DME system. It operates in the frequency band 960-1215 MHz. The bearing unit of TACAN is more accurate than a standard VOR since it makes use of a two-frequency principle, with 15 Hz and 135 Hz components, and because UHF transmissions are less prone to signal bending than VHF.


A US Air Force TACAN Antenna.

The distance measurement component of TACAN operates with the same specifications as civil DMEs. Therefore to reduce the number of required stations, TACAN stations are frequently co-located with VOR facilities. These co-located stations are known as VORTACs. This is a station composed of a VOR for civil bearing information and a TACAN for military bearing information and military/civil distance measuring information. The TACAN transponder performs the function of a DME without the need for a separate, co-located DME. Because the rotation of the antenna creates a large portion of the azimuth (bearing) signal, if the antenna fails, the azimuth component is no longer available and the TACAN downgrades to a DME only mode.

Accuracy

Theoretically a TACAN should provide a 9-fold increase in accuracy compared to a VOR but operational use has shown only an approximate 3-fold increase.[3]

Accuracy of the 135 Hz azimuth component is ±1° or ±63 m at 3.47 km.[4] Accuracy of the DME portion is 926 m (±0.5 nautical mile) or 3 percent of slant range distance, whichever is greater - see FAA 9840.1 1982.[4]

TACAN stations can provide distance up to 390 nautical miles.

Modern TACANs are much more accurate. The requirement now is to have portable TACAN that is IFR certifiable, both Station and Portable systems. The latest modern version of TACAN has been tested to an average error of 0.00 in both range and azimuth, and could be a feasible back-up to future Air Traffic Control Systems and may even be integrated into systems for a seamless back up.

Past TACANs have relied on high output power (up to 10,000 Watts) to ensure good signal in space to overcome nulls present in antenna design and to provide their required 200 mile range. With the advancement of technology, antenna design has improved with higher gain antennas, much shallower nulls, and lighter construction. Now it's feasible to have a 200 nmi range with a 400 Watt TACAN DME Transmitter, making the TACAN package much smaller, more portable and more reliable (Power = Heat which shortens the life of electronics).

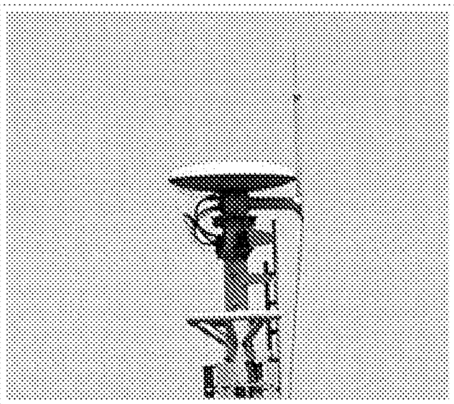
TACAN is getting smaller: Full TACAN coverage can now be provided in a system that can be carried on a single trailer weighing less than 4000 lbs, and set up by two people in less than an hour. TACAN Transceivers can now be as small as lunch boxes (with full coverage and range) and the antennas can be reduced from 800 pounds to less than 100 pounds.

Benefits

TACAN antenna at Shemya, Alaska.

Because the azimuth and range units are combined in one system it provides for simpler installation. Less space is required than a VOR because a VOR requires a large counterpoise and a fairly complex phased antenna system. A TACAN system theoretically might be placed on a building, a large truck, an airplane, or a ship, and be operational in a short period of time. An airborne TACAN receiver can be used in air-to-air mode which allows two cooperating aircraft to find their relative bearings and distance.

Drawbacks



A shipboard TACAN antenna on USS Raleigh (LPD-1) with a lightning rod extending above it.

For military usage a primary drawback is lack of the ability to control emissions (EMCON) and stealth. Naval TACAN operations are designed so an aircraft can find the ship and land. There is no encryption involved, an enemy can simply use the range and bearing provided to attack a ship equipped with a TACAN. Some TACANs have the ability to employ a "Demand Only" mode wherein they will only transmit when interrogated by an aircraft on-channel. It is likely that TACAN will be replaced with a differential GPS system similar to the Local Area Augmentation System called JPALS. The Joint Precision Approach and Landing System has a low probability of intercept to prevent enemy detection and an aircraft carrier version can be used for autoland operations.

Some systems used in the United States modulate the transmitted signal by using a 900 RPM rotating antenna. Since this antenna is fairly large and must rotate 24 hours a day, it can cause reliability issues. Modern systems have antennas that use electronic rotation (instead of mechanical rotation) with no moving parts.

Future

Like all other forms of ground-based aircraft radio navigation currently used, it is likely that TACAN will eventually be replaced by some form of space based navigational system such as GPS.[5]

See also

- Battle of Lima Site 85 (SAC TACAN captured March 1968)
- Distance Measuring Equipment
- VHF Omnidirectional Range
- Global Positioning System
- Wide Area Augmentation System

References

1. Goodman, J.L.; Propst, C.A. (2008), "Operational use of GPS navigation for space shuttle entry", *Position, Location and Navigation Symposium, 2008 IEEE/ION* (May 2008): 731–743, doi:10.1109/PLANS.2008.4570031
2. Rockwell International (July 7, 1992). "Aircraft rendezvous using low data rate two-way TACAN bearing information".
3. Albert Helfrick (2009). "Principle of avionics 5th edition" (book).
4. Department of Transportation and Department of Defense (March 25, 2002). "2001 Federal Radionavigation Systems" (PDF). Retrieved November 27, 2005.
5. Department of Transportation and Department of Defense (March 25, 2002). "2001 Federal Radionavigation Plan" (PDF). Retrieved August 2, 2006.

External links

- Rantec Microwave Systems - Manufacturer of non-rotating TACAN antennas (http://www.rantecmdm.com/tacan.htm) - Complete with antenna internal photos and specs
- Moog Navigation and Surveillance Systems (http://www.moog.com/products/navigation-surveillance-systems/) - Fixed site, shipboard, mobile and man-portable TACAN systems

Wikimedia Commons has media related to ***Tactical air navigation system***.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Tactical_air_navigation_system&oldid=711647097"

Categories: Avionics | Radio navigation | Aircraft instruments | Air navigation

Appendix C

MIL-STD-291C STANDARD TACTICAL AIR NAVIGATION (TACAN) SIGNAL

http://everyspec.com/MIL-STD/MIL-STD-0100-0299/download.php?spec=MIL-STD-291C.011561.pdf

INCH-POUND

MIL-STD-291C
10 February 1998
SUPERSEDING
MIL-STD-291B
13 December 1967

DEPARTMENT OF DEFENSE
INTERFACE STANDARD

STANDARD TACTICAL AIR NAVIGATION (TACAN) SIGNAL

AMSC N/A FSC 5826
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

FOREWORD

1. This standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) any any pertinent data which may be of use in improving this document should be address to Commander, Naval Air Warfare Center Aircraft Division, Code 4.1.4.2B120-3, Highway 547, Lakehurst, NJ 08733-5100, using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

CONTENTS

CONTENTS (Continued)

1. SCOPE

1.1 Scope. This standard defines the Standard TACAN Signal. The characteristics and tolerances specified will ensure compatibility of all airborne and ground equipment.

2. APPLICABLE DOCUMENTS (Not applicable)

3. DEFINITIONS (Not applicable)

4. GENERAL REQUIREMENTS

4.1 TACAN channels. The TACAN system shall operate on the frequencies shown in table I.

4.1.1 Number of channels. There shall be provision of 252 channels, 126 "X" channels numbered 1X through 126X, and 126 "Y" channels numbered 1Y through 126Y. Each channel shall have an interrogating frequency/pulse spacing and reply frequency/pulse spacing as shown in table I. In addition, there shall be provision for 126 pairs of air-to-air (A/A) mode channels as specified in 5.1 and also in table I.

4.1.1.1 Interrogating frequency. The interrogating frequency for the 252 channel TACAN system shall begin with Channel 1 (X or Y) at 1025 megahertz (MHz) and increase in 1 MHz increments until Channel 126 (X or Y) at 1150 MHz is reached. The interrogating pulse spacing shall be 12 microseconds (μsec) for X channels, 36 μsec for Y channels, and 24 μsec for Y mode A/A. (See table I) (NOTE: See 3.4 for definition.)

4.1.1.2 Ground reply frequency. The ground reply frequency for the 252 channel TACAN system shall begin at Channel 1X with 962 MHz (which is 63 MHz lower than the interrogating frequency) and increase in 1 MHz increments until Channel 63X is reached at 1024 MHz. Continuing, Channel 64X will be at ground reply frequency of 1151 MHz (which is 63 MHz higher than the interrogating frequency), and increase in 1 MHz increments until Channel 126X is reached at 1213 MHz. The ground reply pulse spacing for X Channels shall be 12 μsec. For Y Channels, the ground reply frequency shall begin for Channel 1Y with 1088 MHz (which is 63 MHz higher than the interrogating frequency) and increase in 1 MHz increments until Channel 63Y is reached at 1150 MHz. Continuing, Channel 64Y will be at a ground reply frequency of 1025 MHz (which is 63 MHz lower than the interrogating frequency) and increase in 1 MHz increments until Channel 126Y is reached at 1087 MHz. The ground reply pulse spacing for Y channels shall be 30 μsec. (See table I.)

5. DETAILED REQUIREMENTS

5.1 TACAN surface transponder signal. The standard signal, to be radiated and received by the transponder of the TACAN system, shall be vertically polarized and the radiated signal shall have the following characteristics:

5.1.1 Radio frequency (r.f.). The transmitted frequency shall be maintained within plus or minus 0.002 percent of that specified.

5.1.2 R.F. pulse spectrum. The peak effective radiated power contained in each of the two 0.5 MHz bands centered on frequencies plus or minus 0.8 MHz above and below the nominal channel frequency shall not exceed 100 milliwatts (mw), and the peak effective radiated power contained in each of the two 0.5 MHz bands centered on frequencies plus or minus 2.0 MHz above and below the nominal channel frequency shall not exceed 2.0 mw. Each lobe of the spectrum shall be less than the adjacent lobe nearer the nominal channel frequency.

5.1.3 Continuous wave (cw) output. Cw output between pulse pairs shall not exceed 5 microwatts (μw) with the beacon in normal operational mode. The peak signal amplitude for a period of 1 μsec between pulses of a pair on X channels and 19 μsec between pulses of a pair and pulses of the main reference group on Y channels shall be at least 20 decibel (db) below the peak pulse amplitude. During the Y channel auxiliary reference burst group, the energy shall be at least 20 db below the peak pulse amplitude for at least 4 μsec between pulses of the group.

5.2 Pulse shape. The pulse envelope as detected by a linear detector shall have a rounded shape falling within the following limits:

5.2.1 Pulse top. The instantaneous amplitude of the pulse shall not, at any instant between the point of the leading edge which is 95 percent of the maximum voltage amplitude and the point of the trailing edge which is 95 percent of the maximum amplitude, fall below a line which is 95 percent of the maximum voltage amplitude of the pulse and is parallel to the base line.

5.2.2 Pulse rise time. The time required for the leading edge of the pulse to rise from 10 to 90 percent of its maximum voltage amplitude shall be 2.0 ± 0.25 μsec.

5.2.3 Pulse fall time. The time required for the trailing edge of the pulse to fall from 90 percent to 10 percent of its maximum voltage amplitude shall be 2.5 ± 0.5 μsec.

5.2.4 Pulse duration. The pulse duration which is measured between the points on the leading and trailing edges of the pulse which are 50 percent of the maximum voltage amplitude of the pulse shall be 3.5 ± 0.5 μsec.

5.3 Pulse droop. Prior to amplitude modulation by the antenna of the composite r.f. pulse train, the percentage modulation of the pulse train at 15 or 135 Hertz (Hz) shall not exceed 0.08 percent (see 3.5 and 3.6). This shall be measured with the transponder operating normally and shall include the effects of droop and recovery time of the main and auxiliary reference groups.

5.4 Pulse coding. For X channels, the pulses shall be coded in pairs with a spacing which shall be 12 ± 0.10 μsec as measured at 50 percent voltage amplitude points from the leading edge of the first pulse to the leading edge of the second pulse. For Y channels, the ground-to-air function spacing shall be 30 ± 0.10 μsec as measured at 50 percent voltage amplitude points from the leading edge of the first pulse to the leading edge of the second pulse.

5.5 Main reference pulse group. The 15 Hz reference bearing group is called the main reference group: for X channels, it shall consist of a group of 12 pairs of pulses, with the spacing between pairs established as 12 ± 0.10 μsec; for Y channels, it shall consist of a group of 13 single pulses spaced 30± 0.10 μsec. In each case, the repetition rate of the group shall be 15 Hz ± 0.2 percent.

5.6 Auxiliary reference pulse group. The 135 Hz reference bearing group is called the auxiliary reference group: for X channels, it shall consist of 6 pairs of pulses, with the spacing between pairs established as 24 ± 0.10 μsec; for Y channels, it shall consist of a group of 13 single pulses spaced 15 ± 0.10 μsec. In each case, the repetition rate of the group shall be 135 Hz which shall be synchronized with the main reference group; however, the auxiliary group which would otherwise coincide in time with the main reference group shall be removed so that only the main reference group appears in this position in the final output signal.

5.7 Precedence. Random, identity, and distance reply pulses shall not appear during a main or auxiliary reference group.

5.8 Identification signal. The identification signal shall consist of a series of paired pulses spaced as specified in 3.4, transmitted at a repetition rate of 1350 pulse pairs per second (sec) and synchronized so that the first pulse of an identity pair shall occur 740 ± 50 μsec after the first pulse of the preceding auxiliary reference group.

5.8.1 Equalizing pulse pair. To preserve a constant duty cycle and to minimize bearing error during identity signals, an equalizing pair of pulses shall be transmitted 100 ± 10 μsec after each identity pair.

5.8.2 Identity cycle. The random and distance reply pulses shall be replaced by the identity pulses at a recurrence rate of once ever 37.5 sec ± 10 percent. During identity, the beacon code shall be transmitted as dots and dashes (Morse Code) of identity pulses; the spaces between dots and dashes being occupied by distance reply and random pulses. The dots shall be 0.125 sec ± 10 percent; dashes shall be 0.375 sec ± 10 percent. Maximum message length shall not exceed 5.0 seconds.

5.9 Pulse repetition rate. The signal shall have randomly distributed pulses which shall be maintained at a rate of 2700 ± 90 pairs per sec before the reference groups are added; the random pulses shall include any distance replies. The distribution of the random pulse pairs, for no interrogating load, shall fall within the limits shown on Figure 1, for a dead time of 60 μsec.

5.10 Dead time. Dead time is defined as the total time following a decoded pulse pair (from an interrogation or noise) during which there will be no response to subsequent interrogations or noise. The dead time shall not normally exceed 60 µsec and is not usually extended by the echo suppression circuits, but or special cases where the geographical site of the transponder is such as to produce undesirable reflection problems, a longer echo suppression time may be specified; this will tend to increase the average dead time. In extreme cases, this may require compensating pulses to maintain azimuth accuracy. The spacing between any two consecutively transmitted random pulse pairs that are not replies shall be not less than 60 µsec.

5.11 Composite 15 and 135 Hz variable bearing signal. The bearing signal shall be generated by rotating a directional pattern which produces, at a point in space, a composite amplitude modulation of the r.f. pulse signals at 15 and 135 Hz. Viewed from above, the direction of pattern rotation shall be clockwise. For X-mode operation the amplitude modulation shall be synchronized with the 15 Hz main reference group so that at a point due south of the beacon the 10th pulse of the main reference group will coincide with the positive slope point of inflection of the 15 Hz component of the bearing signal and at points geographically spaced by all multiples of 40 degrees from due south, the 12th pulse of each auxiliary reference group shall coincide with the positive slope point of inflection of the 135 Hz component. For Y-Mode operation the coincidence points shall be midway between the 6th and 7th pulses of the 15 Hz reference group, and shall be at the 12th pulse of the 135 Hz reference group. The main reference group shall occur when the maximum of the composite signal is directed due east of the transponder. In the absence of harmonics, the modulation envelope of the detected r.f. pulse signal shall follow this formula:

$$y = 1.0\ A\sin(2\pi ft \pm \theta - \gamma) + B\sin(18\pi ft \pm \varnothing - 9\gamma)$$

Where:

(1) y = normalized composite 15- 135 Hz signal amplitude
(2) A = represents modulation of 15 Hz component
(3) B = represents modulation of 135 Hz component
(4) θ = deviation in electrical degrees from coincidence of the 15 Hz modulation and the main reference group.
(5) $\varnothing$ = deviation in electrical degrees from coincidence of the 135 Hz modulation and the auxiliary reference group.
(6) γ = bearing to the ground or shipboard station from the point of observation.
(7) f = pattern rotation frequency in Hz.

(8) t = time in seconds from the corrected position of the 10th pulse of the X-mode main reference group or 15 μsec after the 6th pulse of the Y-mode main reference group. t is computed from the average position of the 12th pulse of each auxiliary reference group.

Tolerances:

f = 15 Hz ± 0.2 percent
For angles of elevation between -45 and +45 degrees
θ = 0.3 degree maximum
Ø = 0.3 degree maximum
A = 0.21 ± 0.09
B = 0.21 ± 0.09
Sum of A and B not greater than 0.55
Cross polarization effects up to plus or minus 45 degrees from the vertical and within elevation angles of -45 to +45 degrees must be limited such that θ does not exceed 3 degrees and Ø does not exceed 1 degree.

5.11.1 Harmonic content. At vertical angles from the horizon to 6 degrees above the horizon the root means square (r.m.s.) sum of the second through the sixth harmonics of the 15 Hz modulation component of the radiated signal shall not exceed 20 percent. The r.m.s. sum of the harmonics of the 135 Hz modulation component of the radiated signal shall not exceed 15 percent. The amplitude of modulation components radiated at frequencies of 105 Hz, 120 Hz, 150 Hz, and 165 Hz individually shall not exceed 15 percent nor shall the r.m.s. sum of these components exceed 20 percent.

5.12 Distance reply signal. The distance reply signal shall consist of a pair of pulses transmitted in response to a pair of interrogating pulses. The surface transponder shall be capable of delaying the response, when measured from the leading edge of the first interrogating pulse to the leading edge of the first reply pulse, 50 ± 0.1 μsec and 74 ± 0.10 μsec for X-mode and Y-mode. The user then may select the delay that is applicable.

5.12.1 Reply efficiency. The transponder shall reply with not more than 30 percent countdown to 3300 interrogations per second.

5.13 TACAN interrogating signal. The standard signal, to be radiated and received by the airborne equipment of the TACAN system, shall nominally be vertically polarized. The interrogating signal, radiated by the airborne equipment, shall have the following characteristics:

5.13.1 Radio frequency. The frequency of the transmitter output shall be maintained within plus or minus 0.005 percent of its specified frequency.

5.13.2 R.f. pulse spectrum. The energy contained in an 0.5 MHz band centered on a frequency plus or minus 0.8 MHz from the channel frequency shall be at least 23 db below the energy level contained in an 0.5 MHz band centered on the channel frequency. The energy level contained in an 0.5 MHz band centered on a frequency plus or minus 2.0 MHz from the channel frequency shall be at least 38 db below the energy contained in an 0.5 MHz band centered on the channel frequency. Each lobe of the spectrum shall be of less amplitude than the adjacent lobe nearer the multiplied oscillator frequency.

5.13.3 Cw output. Cw output between pulses shall not exceed 0.2 mw.

5.13.4 Pulse shape. The pulse envelope as detected by a linear detector shall fall within the following limits:

5.13.5 Pulse top. The instantaneous amplitude of the pulse shall not, at any instant between the point of leading edge which is 95 percent maximum amplitude and the point of the trailing edge which is 95 percent of the maximum amplitude, fall below a line which is 95 percent of the maximum voltage amplitude of the pulse and is parallel to the base line.

5.13.6 Pulse rise time. The time required for the leading edge of the pulse to rise from 10 to 90 percent shall be 2.0 ± 0.25 µsec.

5.13.7 Pulse fall time. The time required for the trailing edge of the pulse to fall from 90 to 10 percent of its maximum voltage amplitude shall not exceed 3.0 µsec.

5.13.8 Pulse duration. The pulse duration, which is measured between the points on the leading and trailing edges of the pulse which are 50 percent of the maximum voltage amplitude of the pulse, shall be 3.5 ± 0.5 µsec.

5.14 Pulse coding. The pulses shall be coded in pairs, with a spacing which shall be 12 ± 0.5 µsec for X channels, and 36 ± 0.5 µsec for Y channels, as measured at the 50 percent maximum voltage amplitude point from the leading edge of the first pulse to the leading edge of the second pulse.

5.15 Pulse repetition rate. In the air-to-ground mode in the search condition, the interrogating signal from one aircraft shall not exceed 150 pulse pairs per sec; however, an interrogation rate of 135 ± 3 pairs per sec shall be avoided. In the track condition, this number shall not exceed 30 pulse pairs per sec. In the air-to-air mode the interrogations shall not fall below 22 pulses per seconds in both search and track conditions.

5.15.1 Pulse repetition rate variation. The spacing between successive interrogations shall be sufficiently nonuniform to preclude one equipment from locking-on to range replies intended for any other equipment interrogating the same beacon.

5.16 Air-to-Air mode frequency pairing. Sixty-three pairs of Air-to-air (A/A) mode channels in X-mode and 63 pairs in Y-mode shall be available for an A/A link between two airborne interrogator-transponders as shown in table I. Channel 1X or 1Y, transmitting at

1025 MHz, shall receive at 1088 MHz and pair with channel 64X or 64Y transmitting at 1088 MHz and receiving at 1025 MHz. Channel 2X or 2Y, transmitting at 1026 MHz, shall receive at 1089 MHz and pair with channel 65X or 65Y transmitting at 1089 MHz and receiving at 1026 MHz.

5.17 A/A system delay time. The single reply pulse shall occur 62 µsec ± 0.1 µsec in X-mode and 74 µsec 0.1 µsec in Y-mode after receipt of the first pulse of an interrogation pair of pulses. The range indicator of the interrogator shall read 0 miles upon receipt of a reply pulse at the antenna 62 µsec after transmission of the first pulse of an interrogation pair of pulses in X-mode and 74 µsec in Y-mode.

5.18 Signal characteristics. The interrogation pulse pairs shall have characteristics identical with those in air-to-group operation. For X-mode A/A operation the pulse pair spacing shall be 12 ± 0.1 µsec and for Y-mode A/A operation the pulse pair spacing shall be 24 ± 0.1 µsec. Each airborne equipment shall transpond to each received interrogation from other airborne equipment with a single pulse having the same characteristics as the interrogation pulses.

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory).

6.1 Intended use. The TACAN signal characteristics tolerances defined herein are intended for use by all airborne and ground equipments. The air navigation signal characteristics covered by this standard are military unique because they are used with military applications only in air-to-air operation.

6.2 International standardization agreements. Certain provisions of this standard are the subject of international standardization agreement (NATO C-13). When amendment, revision, or cancellation of this specification is proposed which will affect or violate the international agreement concerned, the preparing activity will take appropriate reconciliation action through international standardization channels, including departmental standardization offices, if required.

6.3 Cross reference. This interface standard replaces MIL-STD-291B.

6.4 Subject term (keyword) listing.

Harmonic
Pulse
Radio
Signal
Spectrum
Wave

6.5 Changes from previous issue. Marginal notations are not used in this revision to identify changes with respect to the previous issue due to extent of the changes. There are no technical changes resulting from the transition of this standard from a MILITARY to an INTERFACE STANDARD.

CONCLUDING MATERIAL

Custodians:
Army - AV
Navy - AS
Air Force - 85

Preparing activity:
Navy - AS
(Project 5826-0243)

TABLE I. - TACAN Frequencies.

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
1X	1025	1025	12	1088	962	12
1Y	1025	1025	36	1088	1088	30
2X	1026	1026	12	1089	963	12
2Y	1026	1026	36	1089	1089	30
3X	1027	1027	12	1090	964	12
3Y	1027	1027	36	1090	1090	30
4X	1028	1028	12	1091	965	12
4Y	1028	1028	36	1091	1091	30
5X	1029	1029	12	1092	966	12
5Y	1029	1029	36	1092	1092	30
6X	1030	1030	12	1093	967	12
6Y	1030	1030	36	1093	1093	30
7X	1031	1031	12	1094	968	12
7Y	1031	1031	36	1094	1094	30
8X	1032	1032	12	1095	969	12
8Y	1032	1032	36	1095	1095	30
9X	1033	1033	12	1096	970	12
9Y	1033	1033	36	1096	1096	30
10X	1034	1034	12	1097	971	12
10Y	1034	1034	36	1097	1097	30
11X	1035	1035	12	1098	972	12
11Y	1035	1035	36	1098	1098	30
12X	1036	1036	12	1099	973	12
12Y	1036	1036	36	1099	1099	30
13X	1037	1037	12	1100	974	12
13Y	1037	1037	36	1100	1100	30
14X	1038	1038	12	1101	975	12
14Y	1038	1038	36	1101	1101	30
15X	1039	1039	12	1102	976	12
15Y	1039	1039	36	1102	1102	30
16X	1040	1040	12	1103	977	12
16Y	1040	1040	36	1103	1103	30
17X	1041	1041	12	1104	978	12
17Y	1041	1041	36	1104	1104	30

See footnotes at end of table.

TABLE I. - TACAN Frequencies (Continued)

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
18X	1042	1042	12	1105	979	12
18Y	1042	1042	36	1105	1105	30
19X	1043	1043	12	1106	980	12
19Y	1043	1043	36	1106	1106	30
20X	1044	1044	12	1107	981	12
20Y	1044	1044	36	1107	1107	30
21X	1045	1045	12	1108	982	12
21Y	1045	1045	36	1108	1108	30
22X	1046	1046	12	1109	983	12
22Y	1046	1046	36	1109	1109	30
23X	1047	1047	12	1110	984	12
23Y	1047	1047	36	1110	1110	30
24X	1048	1048	12	1111	985	12
24Y	1048	1048	36	1111	1111	30
25X	1049	1049	12	1112	986	12
25Y	1049	1049	36	1112	1112	30
26X	1050	1050	12	1113	987	12
26Y	1050	1050	36	1113	1113	30
27X	1051	1051	12	1114	988	12
27Y	1051	1051	36	1114	1114	30
28X	1052	1052	12	1115	989	12
28Y	1052	1052	36	1115	1115	30
29X	1053	1053	12	1116	990	12
29Y	1053	1053	36	1116	1116	30
30X	1054	1054	12	1117	991	12
30Y	1054	1054	36	1117	1117	30
31X	1055	1055	12	1118	992	12
31Y	1055	1055	36	1118	1118	30
32X	1056	1056	12	1119	993	12
32Y	1056	1056	36	1119	1119	30
33X	1057	1057	12	1120	994	12
33Y	1057	1057	36	1120	1120	30
34X	1058	1058	12	1121	995	12
34Y	1058	1058	36	1121	1121	30

See footnotes at end of table.

TABLE I. - TACAN Frequencies. (Continued)

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
35X	1059	1059	12	1122	996	12
35Y	1059	1059	36	1122	1122	30
36X	1060	1060	12	1123	997	12
36Y	1060	1060	36	1123	1123	30
37X	1061	1061	12	1124	998	12
37Y	1061	1061	36	1124	1124	30
38X	1062	1062	12	1125	999	12
38Y	1062	1062	36	1125	1125	30
39X	1063	1063	12	1126	1000	12
39Y	1063	1063	36	1126	1126	30
40X	1064	1064	12	1127	1001	12
40Y	1064	1064	36	1127	1127	30
41X	1065	1065	12	1128	1002	12
41Y	1065	1065	36	1128	1128	30
42X	1066	1066	12	1129	1003	12
42Y	1066	1066	36	1129	1129	30
43X	1067	1067	12	1130	1004	12
43Y	1067	1067	36	1130	1130	30
44X	1068	1068	12	1131	1005	12
44Y	1068	1068	36	1131	1131	30
45X	1069	1069	12	1132	1006	12
45Y	1069	1069	36	1132	1132	30
46X	1070	1070	12	1133	1007	12
46Y	1070	1070	36	1133	1133	30
47X	1071	1071	12	1134	1008	12
47Y	1071	1071	36	1134	1134	30
48X	1072	1072	12	1135	1009	12
48Y	1072	1072	36	1135	1135	30
49X	1073	1073	12	1136	1010	12
49Y	1073	1073	36	1136	1136	30
50X	1074	1074	12	1137	1011	12
50Y	1074	1074	36	1137	1137	30
51X	1075	1075	12	1138	1012	12
51Y	1075	1075	36	1138	1138	30

See footnotes at end of table.

TABLE I. - TACAN Frequencies. (Continued)

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
52X	1076	1076	12	1139	1013	12
52Y	1076	1076	36	1139	1139	30
53X	1077	1077	12	1140	1014	12
53Y	1077	1077	36	1140	1140	30
54X	1078	1078	12	1141	1015	12
54Y	1078	1078	36	1141	1141	30
55X	1079	1079	12	1142	1016	12
55Y	1079	1079	36	1142	1142	30
56X	1080	1080	12	1143	1017	12
56Y	1080	1080	36	1143	1143	30
57X	1081	1081	12	1144	1018	12
57Y	1081	1081	36	1144	1144	30
58X	1082	1082	12	1145	1019	12
58Y	1082	1082	36	1145	1145	30
59X	1083	1083	12	1146	1020	12
59Y	1083	1083	36	1146	1146	30
60X	1084	1084	12	1147	1021	12
60Y	1084	1084	36	1147	1147	30
61X	1085	1085	12	1148	1022	12
61Y	1085	1085	36	1148	1148	30
62X	1086	1086	12	1149	1023	12
62Y	1086	1086	36	1149	1149	30
63X	1087	1087	12	1150	1024	12
63Y	1087	1087	36	1150	1150	30
64X	1088	1088	12	1025	1151	12
64Y	1088	1088	36	1025	1025	30
65X	1089	1089	12	1026	1152	12
65Y	1089	1089	36	1026	1026	30
66X	1090	1090	12	1027	1153	12
66Y	1090	1090	36	1027	1027	30
67X	1091	1091	12	1028	1154	12
67Y	1091	1091	36	1028	1028	30
68X	1092	1092	12	1029	1155	12
68Y	1092	1092	36	1029	1029	30
69X	1093	1093	12	1030	1156	12

See footnotes at end of table.

TABLE I. - TACAN Frequencies. (Continued)

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
69Y	1093	1093	36	1030	1030	30
70X	1094	1094	12	1031	1157	12
70Y	1094	1094	36	1031	1031	30
71X	1095	1095	12	1032	1158	12
71Y	1095	1095	36	1032	1032	30
72X	1096	1096	12	1033	1159	12
72Y	1096	1096	36	1033	1033	30
73X	1097	1097	12	1034	1160	12
73Y	1097	1097	36	1034	1034	30
74X	1098	1098	12	1035	1161	12
74Y	1098	1098	36	1035	1035	30
75X	1099	1099	12	1036	1162	12
75Y	1099	1099	36	1036	1036	30
76X	1100	1100	12	1037	1163	12
76Y	1100	1100	36	1037	1037	30
77X	1101	1101	12	1038	1164	12
77Y	1101	1101	36	1038	1038	30
78X	1102	1102	12	1039	1165	12
78Y	1102	1102	36	1039	1039	30
79X	1103	1103	12	1040	1166	12
79Y	1103	1103	36	1040	1040	30
80X	1104	1104	12	1041	1167	12
80Y	1104	1104	36	1041	1041	30
81X	1105	1105	12	1042	1168	12
81Y	1105	1105	36	1042	1042	30
82X	1106	1106	12	1043	1169	12
82Y	1106	1106	36	1043	1043	30
83X	1107	1107	12	1044	1170	12
83Y	1107	1107	36	1044	1044	30
84X	1108	1108	12	1045	1171	12
84Y	1108	1108	36	1045	1045	30
85X	1109	1109	12	1046	1172	12
85Y	1109	1109	36	1046	1046	30
86X	1110	1110	12	1047	1173	12
86Y	1110	1110	36	1047	1047	30

See footnotes at end of table.

TABLE I. - TACAN Frequencies. (Continued)

Airborne 1/ Airborne 2/ Airborne Ground

Channel	Airborne Interrog. Freq. MHz	A/A Mode Transponding Freq. MHz	Interrog. Pulse Spacing µsec	A/A Mode Receiving Freq. MHz	Reply Freq. MHz	Ground Reply Pulse Spacing µsec
87X	1111	1111	12	1048	1174	12
87Y	1111	1111	36	1048	1048	30
88X	1112	1112	12	1049	1175	12
88Y	1112	1112	36	1049	1049	30
89X	1113	1113	12	1050	1176	12
89Y	1113	1113	36	1050	1050	30
90X	1114	1114	12	1051	1177	12
90Y	1114	1114	36	1051	1051	30
91X	1115	1115	12	1052	1178	12
91Y	1115	1115	36	1052	1052	30
92X	1116	1116	12	1053	1179	12
92Y	1116	1116	36	1053	1053	30
93X	1117	1117	12	1054	1180	12
93Y	1117	1117	36	1054	1054	30
94X	1118	1118	12	1055	1181	12
94Y	1118	1118	36	1055	1055	30
95X	1119	1119	12	1056	1182	12
95Y	1119	1119	36	1056	1056	30
96X	1120	1120	12	1057	1183	12
96Y	1120	1120	36	1057	1057	30
97X	1121	1121	12	1058	1184	12
97Y	1121	1121	36	1058	1058	30
98X	1122	1122	12	1059	1185	12
98Y	1122	1122	36	1059	1059	30
99X	1123	1123	12	1060	1186	12
99Y	1123	1123	36	1060	1060	30
100X	1124	1124	12	1061	1187	12
100Y	1124	1124	36	1061	1061	30
101X	1125	1125	12	1062	1188	12
101Y	1125	1125	36	1062	1062	30
102X	1126	1126	12	1063	1189	12
102Y	1126	1126	36	1063	1063	30
103X	1127	1127	12	1064	1190	12
103Y	1127	1127	36	1064	1064	30
104X	1128	1128	12	1065	1191	12

See footnotes at end of table.

TABLE I. - TACAN Frequencies. (Continued)

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
104Y	1128	1128	36	1065	1065	30
105X	1129	1129	12	1066	1192	12
105Y	1129	1129	36	1066	1066	30
106X	1130	1130	12	1067	1193	12
106Y	1130	1130	36	1067	1067	30
107X	1131	1131	12	1068	1194	12
107Y	1131	1131	36	1068	1068	30
108X	1132	1132	12	1069	1195	12
108Y	1132	1132	36	1069	1069	30
109X	1133	1133	12	1070	1196	12
109Y	1133	1133	36	1070	1070	30
110X	1134	1134	12	1071	1197	12
110Y	1134	1134	36	1071	1071	30
111X	1135	1135	12	1072	1198	12
111Y	1135	1135	36	1072	1072	30
112X	1136	1136	12	1073	1199	12
112Y	1136	1136	36	1073	1073	30
113X	1137	1137	12	1074	1200	12
113Y	1137	1137	36	1074	1074	30
114X	1138	1138	12	1075	1201	12
114Y	1138	1138	36	1075	1075	30
115X	1139	1139	12	1076	1202	12
115Y	1139	1139	36	1076	1076	30
116X	1140	1140	12	1077	1203	12
116Y	1140	1140	36	1077	1077	30
117X	1141	1141	12	1078	1204	12
117Y	1141	1141	36	1078	1078	30
118X	1142	1142	12	1079	1205	12
118Y	1142	1142	36	1079	1079	30
119X	1143	1143	12	1080	1206	12
119Y	1143	1143	36	1080	1080	30
120X	1144	1144	12	1081	1207	12
120Y	1144	1144	36	1081	1081	30
121X	1145	1145	12	1082	1208	30
121Y	1145	1145	36	1082	1082	12

See footnotes at end of table.

122X	1146	1146	12	1083	1209	12
122Y	1146	1146	36	1083	1083	30
123X	1147	1147	12	1084	1210	12

TABLE I. - TACAN Frequencies. (Continued)

Channel	Airborne Interrog. Freq. MHz	Airborne 1/ A/A Mode Transponding Freq. MHz	Airborne 2/ Interrog. Pulse Spacing µsec	Airborne A/A Mode Receiving Freq. MHz	Ground Reply Freq. MHz	Ground Reply Pulse Spacing µsec
123Y	1147	1147	36	1084	1084	30
124X	1148	1148	12	1085	1211	12
124Y	1148	1148	36	1085	1085	30
125X	1149	1149	12	1086	1212	12
125Y	1149	1149	36	1086	1086	30
126X	1150	1150	12	1087	1213	12
126Y	1150	1150	36	1087	1087	30

1/ Airborne A/A mode transponding reply shall be a single pulse.
2/ Airborne A/A Y-mode interrogating pulse spacing = 24 µsec

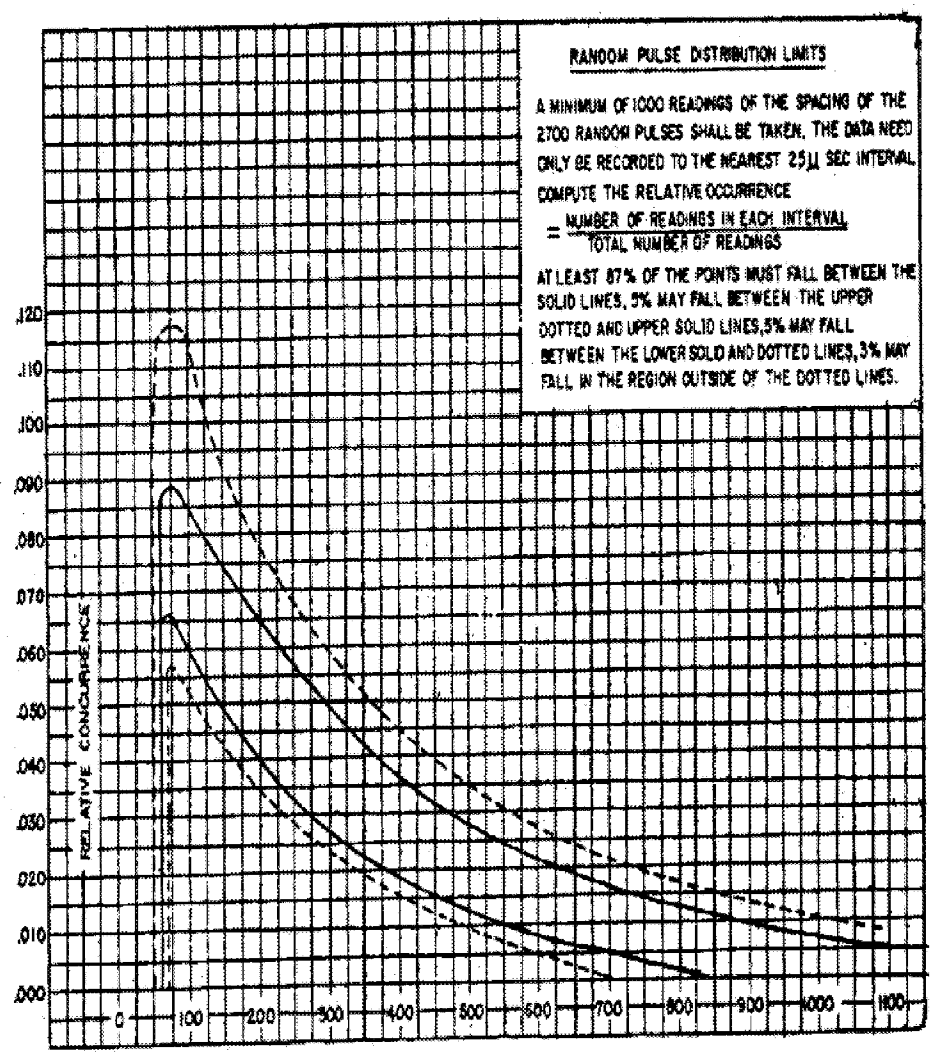


FIGURE 1. Random pulse distribution limits.

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.
NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-STD-291C	2. DOCUMENT DATE (*YYMMDD*)

3. DOCUMENT TITLE
STANDARD TACTICAL AIR NAVIGATION (TACAN) SIGNAL

4. NATURE OF CHANGE (*Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.*)

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME (*Last, First, Middle Initial*)	b. ORGANIZATION	
c. ADDRESS (*Include Zip Code*)	d. TELEPHONE (*Include Area Code*) (1) Commercial: (2) DSN: (*If Applicable*)	7. DATE SUBMITTED (*YYMMDD*)

8. PREPARING ACTIVITY

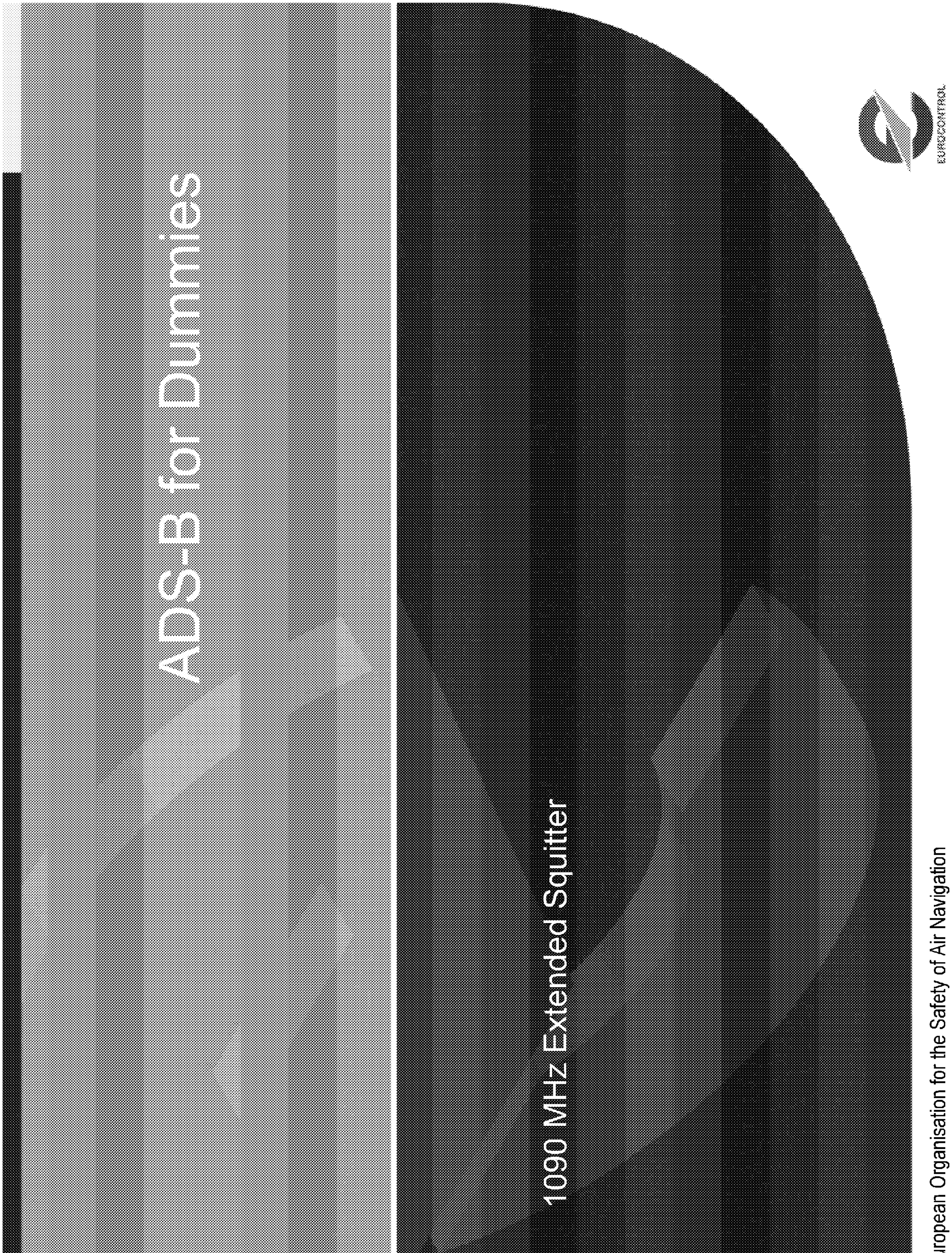
a. NAME COMMANDER NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION	b. TELEPHONE NUMBER (*Include Area Code*) (1) Commercial (732) 323-2628 (2) DSN 624-2628
c. ADDRESS (*Include Zip Code*) CODE 414100B120-3 HIGHWAY 547 LAKEHURST, NJ 08733-5100	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT: Defense Quality and Standardization Office, 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 DSN 289-2340

DD Form 1426, OCT 89 *Previous editions are obsolete* 198/290

Appendix D

ADS-B For Dummies

www.ssd.dhmi.gov.tr/getBinaryFile.aspx?Type=3&dosyaID=195


ADS-B for Dummies
1090 MHz Extended Squitter
European Organisation for the Safety of Air Navigation
EUROCONTROL

Content

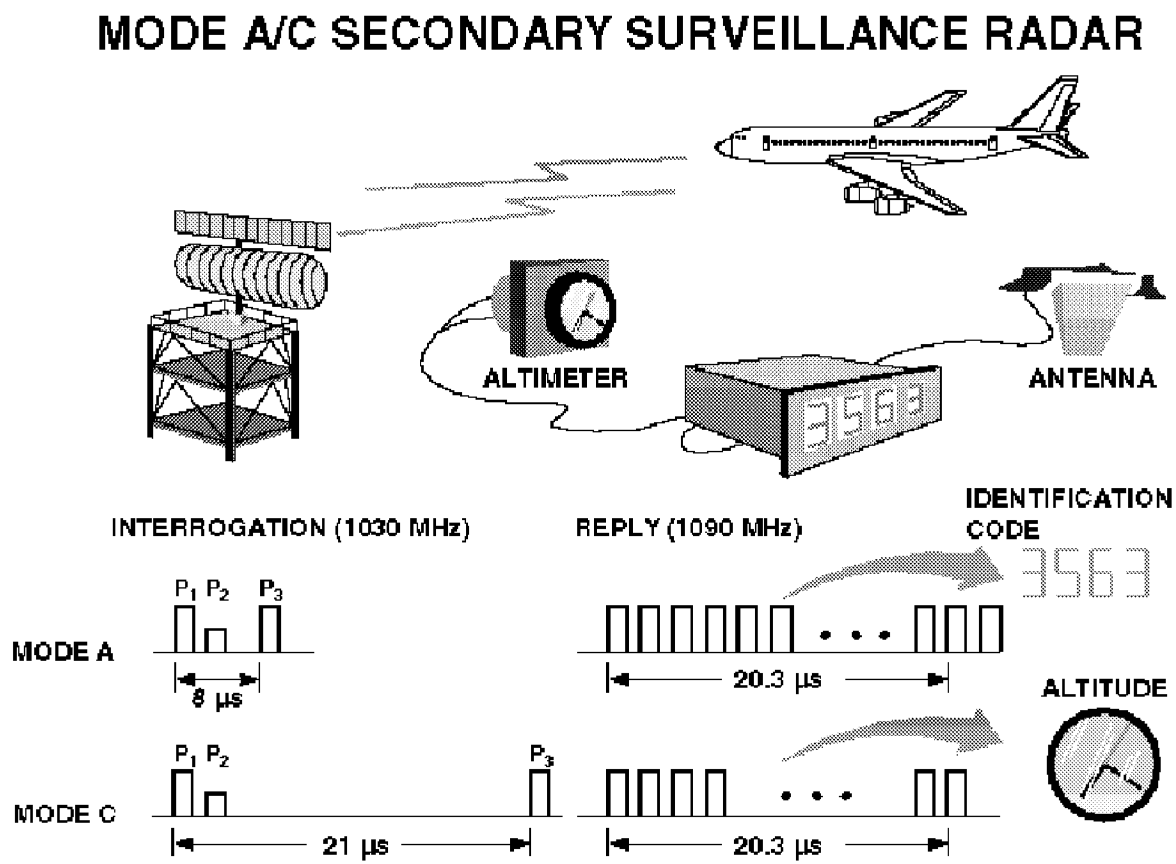
- Mode S overview
- Extended Squitter
- Standards
- Reported ADS-B data
- Reception techniques
- Performance and Capacity
- Equipage
- CASCADE activities

CASCADE

EUROCONTROL

Mode A/C SSR (ATCRBS)

- The SSR system is made up of airborne transponders and ground interrogators/ receivers
- **Mode A** replies convey a target id (Code 3/A)
  - 4096 codes allowed
- **Mode C** replies provide the barometric altitude



CASCADE

EUROCONTROL

Mode S

- Evolutionary improvement of Mode A/C SSR.
  - globally unique a/c identification (24 bits)
    - overcoming the limitation to 4096 Code A addresses
  - selective interrogation
    - to avoid unwanted replies (“fruit”)
  - Interrogator Codes (IC)
    - for unambiguous data exchange with transponders
  - support for the Airborne Collision and Avoidance System (ACAS)
    - acquisition squitter broadcast
  - support for point to point datalink as well as surveillance
  - extension possibilities to
    - ADS-B through the 1090 MHz Extended Squitter (1090ES)
    - multilateration (surface and wide area)
- Backwards compatible with Mode A/C SSR (air/ground)

CASCADE

EUROCONTROL

Mode S Signals

Mode S Reply

Data rate: 1 Mbps

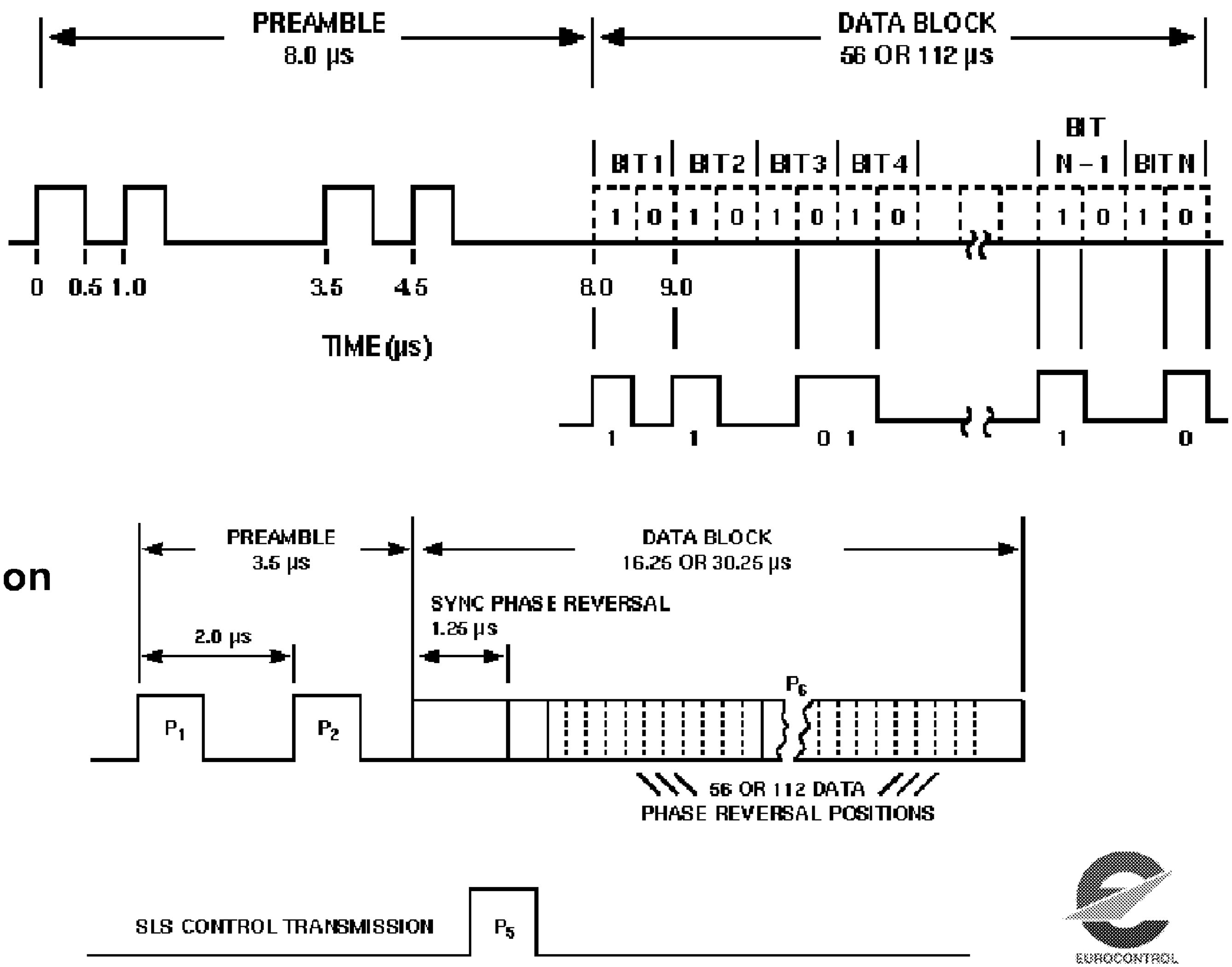
Modulation: PPM

Pulse Position Modulation: Pulse transmitted in the 1st or 2nd half of the bit period (indicating a 1 or 0, respectively).

Mode S Interrogation

Data rate: 4 Mbps

Modulation: DPSK



CASCADE

EUROCONTROL

Mode S Data Block

SURVEILLANCE INTERROGATION AND REPLY

FORMAT NO. (5 Bits)	SURV. & COMM. CONTROL (27 BITS)	ADDRESS/PARITY (24 BITS)	56 BITS

SURVEILLANCE/COMMUNICATION INTERROGATION AND REPLY - COMM-A AND COMM-B

FORMAT NO. (5 Bits)	SURV. & COMM. CONTROL (27 BITS)	MESSAGE FIELD (56 BITS)	ADDRESS/PARITY (24 BITS)	112 BITS

COMMUNICATION INTERROGATION AND REPLY - EXTENDED LENGTH MESSAGE (ELM)

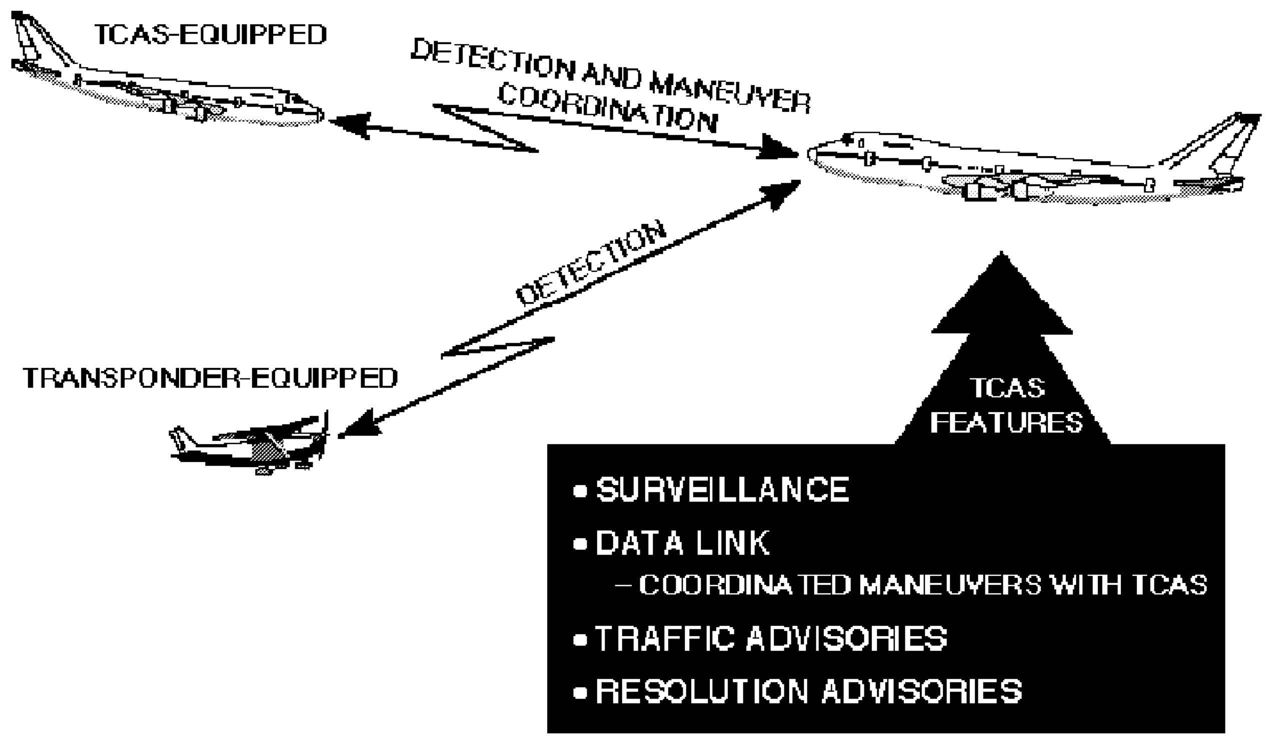
FORMAT NO. (2 Bits)	COMM. CONTROL (6 BITS)	MESSAGE FIELD (80 BITS)	ADDRESS/PARITY (24 BITS)	112 BITS

CASCADE

EUROCONTROL

TCAS/ACAS Operation

- Mode S transponders broadcast acquisition squitters for identification
- TCAS interrogates nearby traffic and derives distance and bearing from the replies
- TCAS generates TAs and RAs for display on cockpit HMI

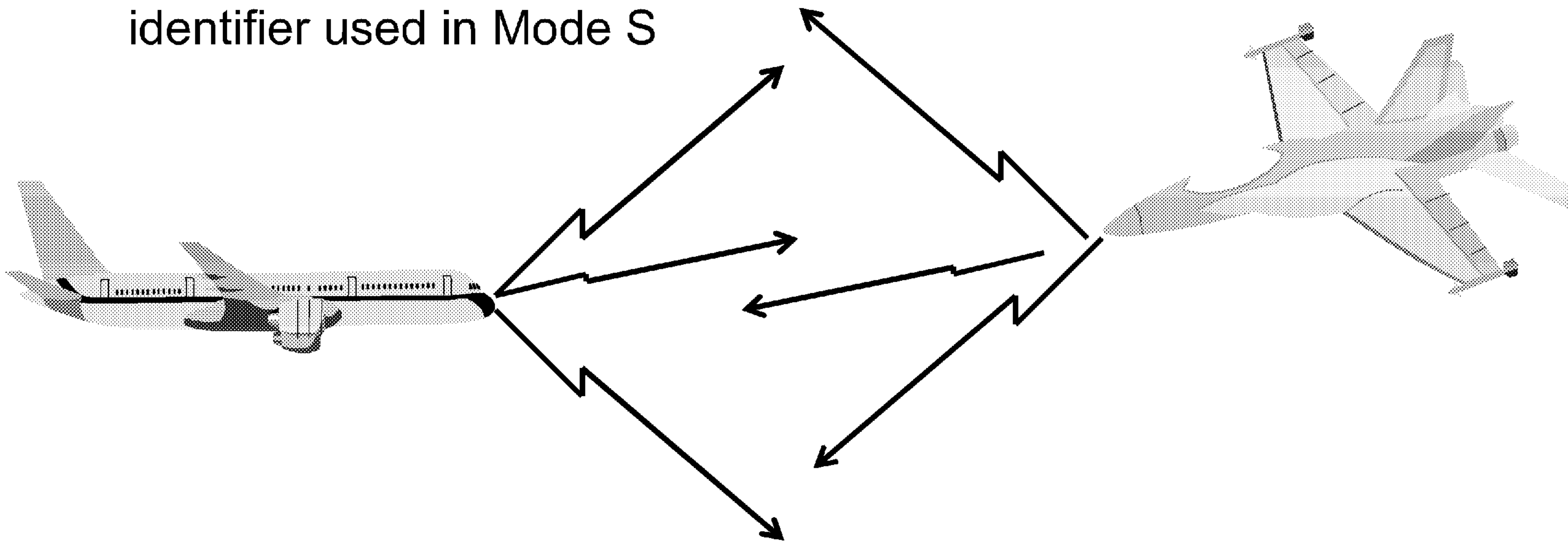


CASCADE

EUROCONTROL

Mode S Acquisition Squitter

- The Mode S transponder outputs an unsolicited transmission once per second to enable ACAS to acquire Mode S equipped aircraft
  - carries only the ICAO 24 bit a/c address, which is a unique aircraft identifier used in Mode S



MODE S SHORT SQUITTER (56 BITS)

8 bit CONTROL	24 bit A/C ADDRESS	24 bit PARITY

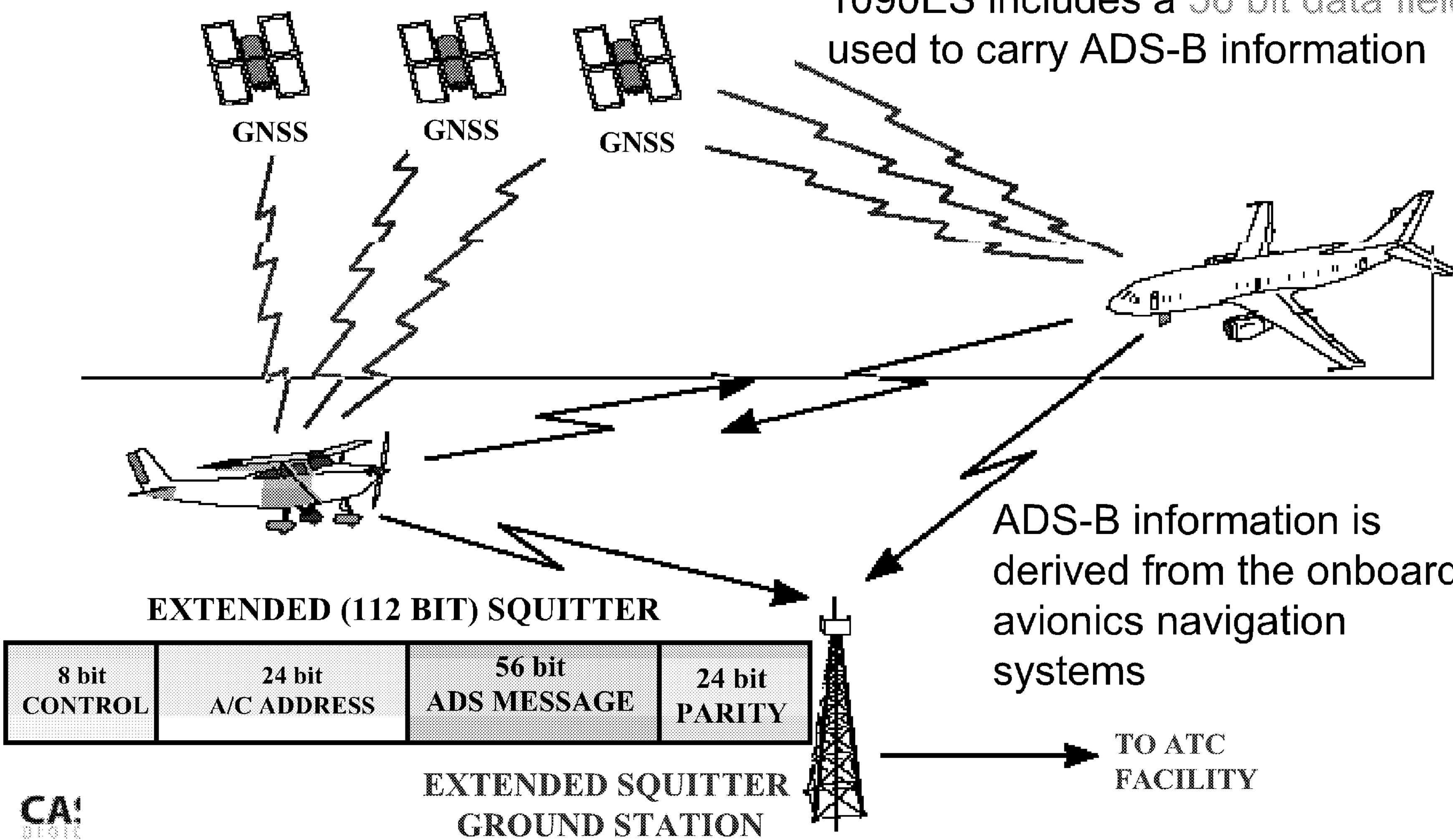
TRANSMITTED ONCE PER SECOND

CASCADE

EUROCONTROL

1090 MHz (Mode S) Extended Squitter

1090ES includes a 56 bit data field used to carry ADS-B information



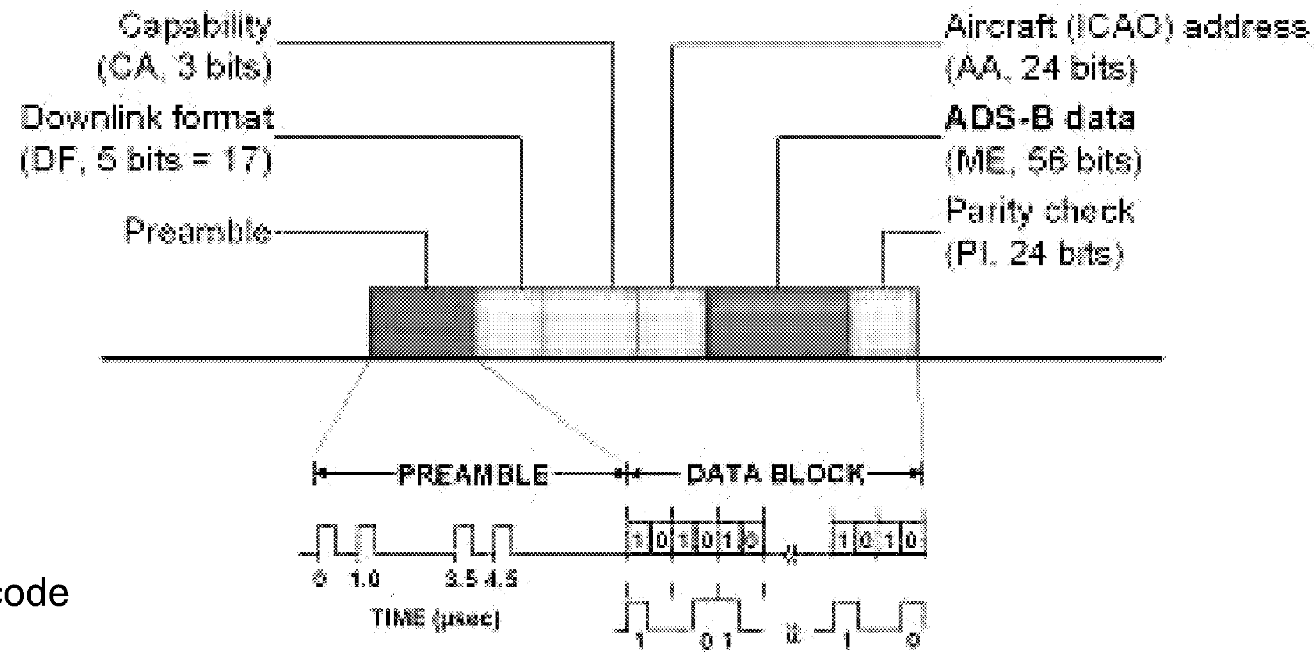
ADS-B information is derived from the onboard avionics navigation systems

CAS

EUROCONTROL

Extended Squitter Format

- **Preamble:** Allows synchronisation on reception
- **DF** = Message type
  - **11** Acq squitter
  - **17** ADS-B
  - **18** TIS-B
  - **19** Military
- **CA**= subtype
- **PI** = error detection code



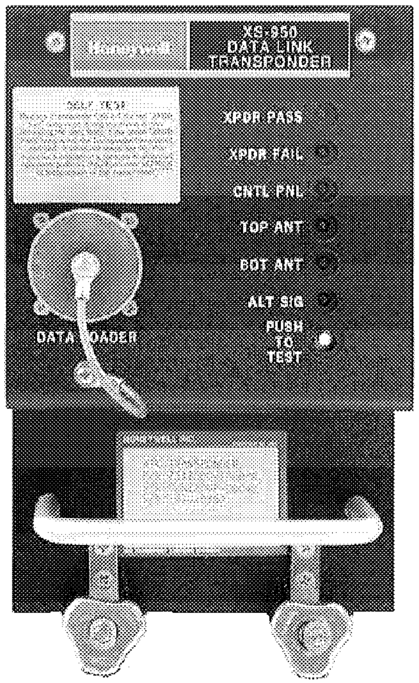
Total duration = 120μs (8μs preamble and 112 μs data block)

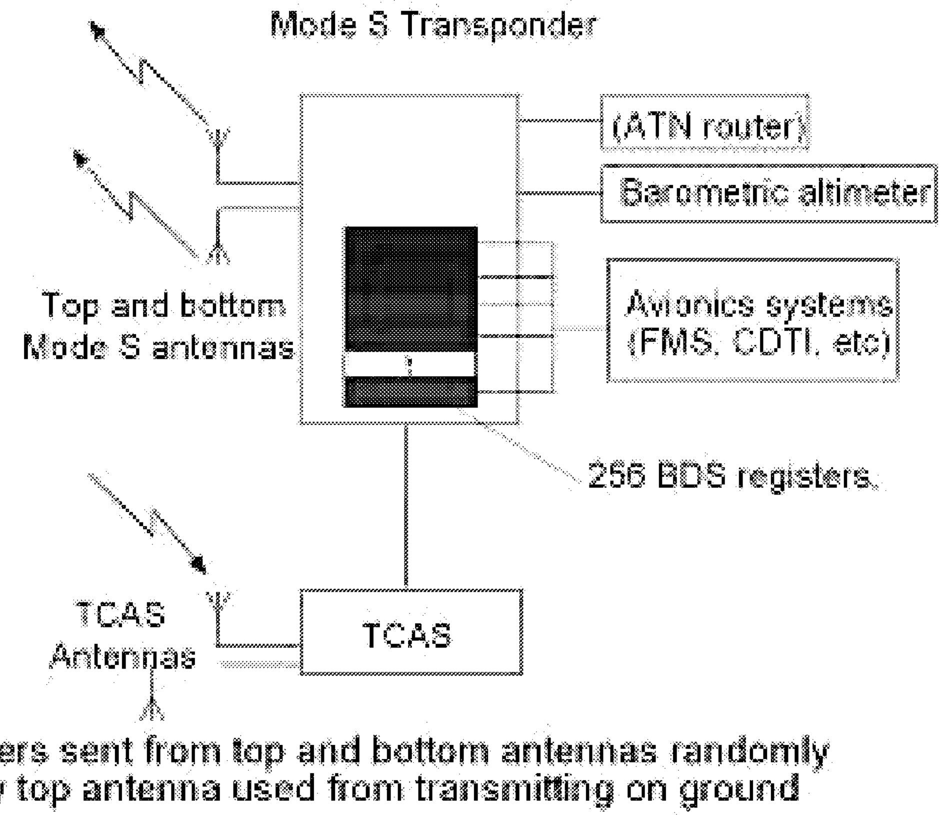
Data block transmitted using Pulse Position Modulation

CASCADE

EUROCONTROL

Mode S Transponder





- Transponders maintain avionics data in the Binary Data Store (BDS) Registers (56 bit wide).

CASCADE

EUROCONTROL

BDS Registers

- BDS Registers are specified in the ICAO Manual of Mode S Specific Services and the Mode S SARPs
  - BDS registers are also referred to as GICB registers because they can be downlinked via “Ground Initiated Comm B transactions”
- Each register contains the data payload of a particular Mode S reply or extended squitter
- Registers not updated within a fixed period are cleared by the transponder
- Registers are identified by a two digit hex number
  - for example BDS 05h or BDS 0,5 is the position squitter
- Certain BDS registers refer specifically to 1090ES

CASCADE

EUROCONTROL

BDS Registers for 1090ES

- Sixteen registers may feed 1090ES transmissions
  - Commonly used are:
    - BDS 05h Ext. Squitter Airborne Position
    - BDS 06h Ext. Squitter Surface Position
    - BDS 07h Ext. Squitter Status
      - transmitted only in reply to interrogation
    - BDS 08h Ext. Squitter A/C Id & Category
    - BDS 09h Ext. Squitter Airborne Velocity
    - BDS 0Ah Extended Squitter Event Report
    - BDS 61h Ext. Squitter Emergency/Priority Status
      - transmitted once per second during an emergency
    - BDS 62h Target State and Status (DO-260A only)
    - BDS 65h Aircraft Operational Status

CASCADE

EUROCONTROL

Position Squitter

- **Format:** Ext. squitter type (plus flags)
- **Latitude/Longitude:** Aircraft Position
- **CPR:** Compact Position Reporting
- **Time:** UTC time flag.
- **Single antenna Flag:** Single or dual antennas
- **Movement:** Ground speed
- **Status**: Validity Flag
- **Track**: Direction of movement

Airborne position squitter

Number of bits	Contents
5	Format type code
2	Surveillance status
1	Single antenna flag
12	Altitude
1	Time
1	CPR format
17	CPR encoded latitude
17	CPR encoded longitude
56 bits total	

TX rate = 2 /sec

Accuracy ~5.1m

Surface position squitter

Number of bits	Contents
5	Format type code
7	Movement
1	Status
7	Ground track
1	Time
1	CPR format
17	CPR encoded latitude
17	CPR encoded longitude
56 bits total	

TX rate = 1/sec

Accuracy ~1.2m

CASCADE

EUROCONTROL

Velocity and Identity Squitters

- **Subtype:** Ground or airspeed flag
- **IFR**:ADS-B Equipage class
- **A/C category**: a/c (small/ medium/large) or vehicle or glider or ...

Airborne velocity squitter

Number of bits	Contents
5	Format type code
3	Subtype
1	Intent change flag
1	IFR capability flag
3	Velocity uncertainty
10 + 1	East-West velocity + sign
10 + 1	North-South velocity + sign
9 + 1 + 1	Vertical rate + sign + source
2	Turn indicator
7 + 1	Geometric height diff. from barometric + sign
56 bits total	

TX rate = 2 /sec

Aircraft identification squitter

Number of bits	Contents
5	Format type code
3	Aircraft category
6	Callsign Character 1
6	Callsign Character 2
6	Callsign Character 3
6	Callsign Character 4
6	Callsign Character 5
6	Callsign Character 6
6	Callsign Character 7
6	Callsign Character 8
56 bits total	

TX rate = 0.2 /sec

CASCADE

EUROCONTROL

1090ES Standards

- ICAO Mode S Ext. Squitter SARPs (Annex 10 Am. 77)
  - defines the DF17, DF18 messages
- Transponder MOPS
  - EUROCAE **ED-73B** and RTCA **DO-181C**
- 1090 ADS-B System MOPS
  - EUROCAE **ED-102** = RTCA **DO-260**
  - RTCA **DO-260A**
- Avionics Form and Fit
  - AEEC Characteristic **ARINC 718A** and EUROCAE **ED-86**
- Safety regulatory standards
  - JAA Technical Service Order **TSO 2C112A** for transponder **ED-73A**
  - FAA **TSO C112** for transponder **DO-181** and **TSO C166** for ADS-B system **DO-260/260A**

CASCADE

EUROCONTROL

DO-260 versus DO-260A

- **DO 260A** added
  - new message "**Target State and Status**" (CA=29)
    - replaces DO-260 intent squitter [BDS 62h]
  - separate accuracy and integrity indications for position
    - **NIC/NAC/SIL** instead of **NUC**
  - expanded a/c type and ADS-B reporting capabilities
  - broadcast of **Mode A Code**
  - support for **TIS-B** squitter (DF18)
- maintaining backwards compatibility
- and expanding the **enhanced decoding techniques** already defined in DO-260 [as options]

CASCADE

EUROCONTROL

DO-260/DO-260A Change 1

- Recently RTCA published Change 1 to DO-260/260A
  - clarification of **NUC** calculation from **GPS** error signals
    - enables unambiguous indication of integrity [DO-260]
  - optional broadcast of **Mode A Code** in DO-260 transponders
    - useful for ADS-B report correlation with SSR data
  - clarification of aircraft "**on ground condition**"
    - was ambiguous in both DO-260 and DO-260A
  - removal of "trajectory intent" and "a/c coordination" squitters
    - squitters not used in practice [DO-260]
  - provisions for ADS-B squitter re-broadcast
    - useful for improving ADS-B coverage
- EUROCAE has not adopted Change 1
  - approval of ED-126 may lead to a reconsideration of the need

CASCADE

EUROCONTROL

Target State and Status Squitter

- DO-260A only (BDS 62h)

Number of Bits	Contents
5	Format Type = 29
2	SubType=0
18	Target Altitude and Flags
14	Target Heading/Track
7	NACp, NICb, SIL
5	Reserved
2	ACAS status and RA status
3	A/c emergency/priority status
56	Total

CASCADE

EUROCONTROL

1090ES Performance

- Range and Capacity are the critical 1090ES performance characteristics
- Air-air or air-ground **range** defines the area within which targets will be reported with acceptable **quality**
  - quality refers to accuracy, integrity, update rate …
    - application dependent requirements
- Air-air or air-ground **capacity** refers to the maximum number of targets that can be monitored with adequate quality within the prescribed range
- Range and capacity depend on the 1090 MHz interference ("fruit") and decoder performance
    - replies to SSR/Mode S/ACAS interrogations
    - short and extended squitters broadcasted from ACAS and ADS-B
- 1090 fruit depends on
  - civil and military SSR/Mode S interrogators
    - Fixed ground civil surveillance infrastructure
    - Fixed and tactical military systems
  - aircraft traffic density and ACAS/ADS-B equipage

CASCADE

EUROCONTROL

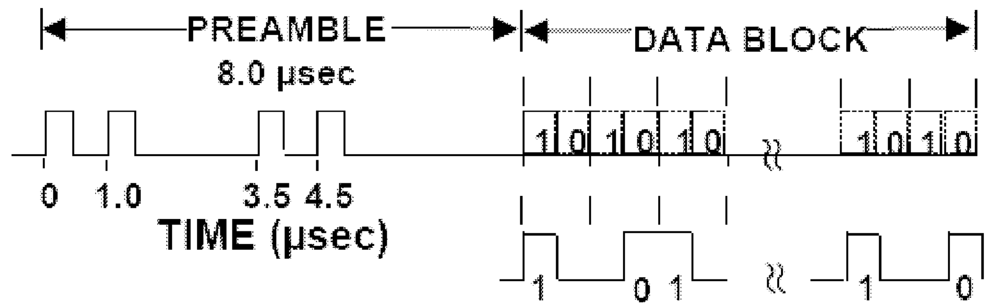
1090ES Range and Capacity

- MOPS compliant 1090ES nominal range (with low fruit <4Kmsg/sec) is
  - >90 nmi air to air
  - >150 nmi air to ground
- 1090ES range drops with increasing fruit
  - Air to air range is the most sensitive
    - on the ground, sector antennas can reduce fruit and improve range
  - enhanced decoding techniques can improve resistance to fruit
- The dominant fruit today is Mode A/C replies
  - Core Europe is the area with the highest fruit levels in the world
    - measured in Frankfurt in 2001 at 33K replies/sec
- Fruit is expected to grow almost linearly with traffic growth unless significant de-commissioning of SSR takes place

CASCADE

EUROCONTROL

1090ES decoding techniques



- Squitter reception entails
  - Preamble detection
  - Bit and confidence declaration
  - Error detection and correction
- Current decoding techniques are designed for narrow beam SSR and short range ACAS operations
  - effective only for low interference levels < 4K Mode A/C msg/sec ("fruit")
  - can handle only one overlapping Mode A/C fruit
- Enhanced decoding techniques provide improvements for all 3 reception stages and are designed to handle multiple overlapping Mode A/C fruit
  - can handle >40K Mode A/C fruit
  - **but do not protect better against short and long squitters**

CASCADE

EUROCONTROL

1090ES equipage

- Current ADS-B 1090ES avionics equipage types:
  - ADS-B capable Mode S transponder and ACAS
    - products in the market today
  - ADS-B capable Mode S transponder and standalone ADS-B receiver
    - Standalone receivers are just appearing in the market
- New Airbus/Boeing a/c come wired for ADSB-out
  - Airbus conforms to DO-260
  - equipment is certified only on non interference basis
  - no provision for ADSB-in
  - suitability of ADS-B data largely depends on type/quality of GPS connection
- A non transponder 1090ES ADS-B solution would be feasible but is not standardised (yet)
  - highly desirable for vehicles and non transponder equipped GA
- 1090ES ground stations are available from a number of vendors
  - Mostly as part of multilateration solutions
  - Standards and certification procedures still in development

CASCADE

EUROCONTROL

Summary

- 1090ES is an extension of the Mode S technology
  - no new spectrum required
  - recent Mode S transponders can be used for ADSB-out
    - growing number of a/c squittering ADS-B
      - but ADS-B data quality is not certified
  - airborne receiver needed for ADSB-in
- Further standardization work needed
    - ADS-B application requirements must be clarified
    - utility of DO-260A and Change 1 features needs to be validated
    - form/fit and certification standards need to be updated
    - standards for ground stations must be developed
- Risk of eventual 1090 MHz band congestion in Core Europe depending on
    - evolution of air traffic density
    - evolution of civil and military SSR/Mode S infrastructure
    - could be countered with more sophisticated receiver systems

CASCADE

EUROCONTROL

CASCADE Activities on 1090ES

- ADS-B application requirements development
  - Joint EUROCAE/RTCA development of standards through the Requirements Focus Group (RFG)
    - leading to updated certification standards for 1090ES equipage
    - contributing to ICAO standardization
- ADS-B application validation on 1090ES
  - 1090ES equipment specification development
    - airborne and ground ADS-B systems
    - validation tools
  - 1090ES experiments and flight trials
    - Operational and technical feasibility and performance assessments
- Business case development for 1090ES applications
- Support to pre-operational implementations
  - 1090ES airborne equipage monitoring
  - Pioneer airlines scheme
    - Support to aircraft installation certification to ED-126
  - Support to deployment for ADS-B 1090ES ground infrastructures

CASCADE

EUROCONTROL

Appendix E

Mode S - Differential Phase shift Keying (DPSK)

http://www.radartutorial.eu/13.ssr/sr23.en.html

Mode S - Differential Phase shift Keying (DPSK)

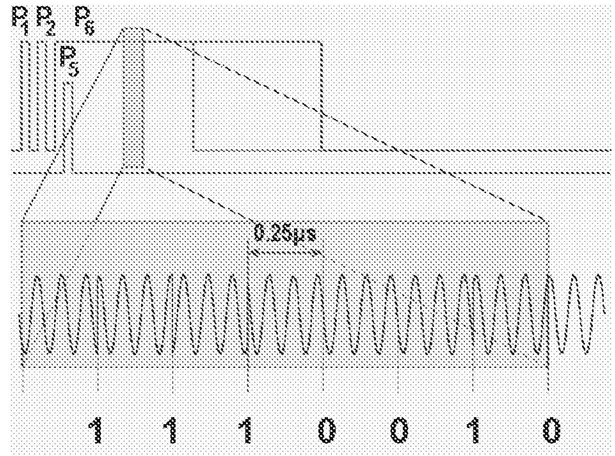


Figure: Mode S - differential phase shift keying (DPSK)

Mode S Uplink interrogations use into the P_6 pulse **D**ifferential **P**hase **S**hift **K**eying (**DPSK**) to modulate the data in the uplink format. It is a type of phase modulation that conveys data by changing the phase of the carrier wave. All subsequent information in the P_6 pulse is coded as 180° phase reversals of the carrier frequency. DPSK is a kind of phase shift keying which avoids the need for a coherent reference signal at the receiver. Each reversal must have a duration of 0.08 µs. Each received phase section has a duration of 0.25 µs and is known as a "**chip**" The DPSK decoder compares the phase between two consecutive chips and verify what the data must have been.

In ICAO Annex 10 Volume 4 is the interrogation data format described as follows: The interrogation data block shall consist of the sequence of 56 or 112 data chips positioned after the data phase reversals within P_6. A 180-degree carrier phase reversal preceding a chip shall characterize that chip as a binary ONE. The absence of a preceding phase reversal shall denote a binary ZERO.

After the sync phase reversal all subsequent phase reversals indicate the 56 or 112 bit P_6 information. All subsequent timing is taken from the point of the first phase reversal. The series of chips starts 0.5 µs after the sync reversal. At the end of P_6 pulse there is a guard interval of 0.5 µs to ensure that distinct transmissions do not interfere with one another.

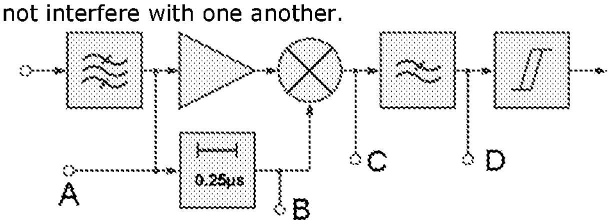


Figure 2: Block diagram of DPSK receiver

Whether the interrogation is short or a long pulse, the total duration of the P_6 pulse is either 16.25 µs (56 data chips) or 30.25 µs (112 data chips). The P_6 begins with an initial phase reversal at the start of the P_6 pulse with a length of 1.25 µs. This is known as the sync phase reversal. To supress antenna sidelobes the pulse P_5 is transmitted by an omnidirectional antenna. This pulse overlays the sync phase reversal and the transponder cannot decode the interrogation.

Figure 2 shows an evident option method of demodulation. At this DPSK decoder, the original sequence is recovered from the demodulated differentially encoded signal through a complementary process. The whole received signal is delayed for exact 0.25 microseconds. The origin and the delayed part will be compared. If the signals are in phase to each other, there is a lower output than if the phases (and the maximum amplitudes) have a contrary magnitude. From this output signal, the original serial bit pattern can be restored, which is indicated only by a low pass filter with the following threshold device.

In Figure 3 the signal (C) at the output of the mixer is shown, formed by superposition of the delayed signal (B) and the undelayed original (A). An allocation of the output level to a bit can only be done, if by the synchronous phase reversal at the beginning of the P_6 pulse triggers a counter to clock a shift register.

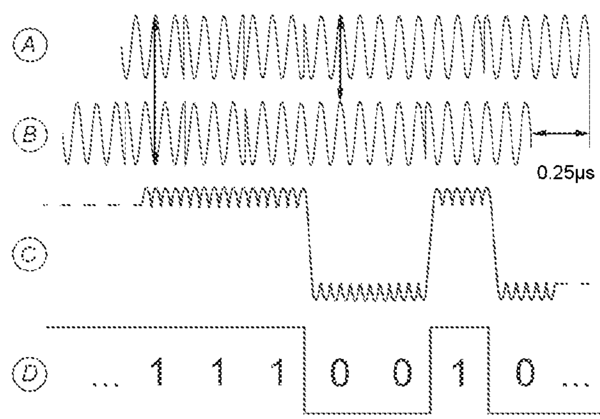


Figure 3: Decoder wave analysis

<u>Appendix F</u>

Secondary Surveillance Radar

Downloaded from Wikipedia 4/2/2016

https://en.wikipedia.org/wiki/Secondary_surveillance_radar

Secondary surveillance radar

From Wikipedia, the free encyclopedia

Secondary surveillance radar (**SSR**)[1] is a radar system used in air traffic control (ATC), that not only detects and measures the position of aircraft i.e. range and bearing, but also requests additional information from the aircraft itself such as its identity and altitude. Unlike primary radar systems that measure only the range and bearing of targets by detecting reflected radio signals, SSR relies on targets equipped with a radar transponder, that replies to each interrogation signal by transmitting a response containing encoded data. SSR is based on the military identification friend or foe (IFF) technology originally developed during World War II, therefore the two systems are still compatible. **Monopulse secondary surveillance radar** (**MSSR**), **Mode S**, **TCAS** and **ADS-B** are similar modern methods of secondary surveillance.

SSR antenna of Deutsche Flugsicherung at Neubrandenburg, in Mecklenburg/Western Pomerania

Contents

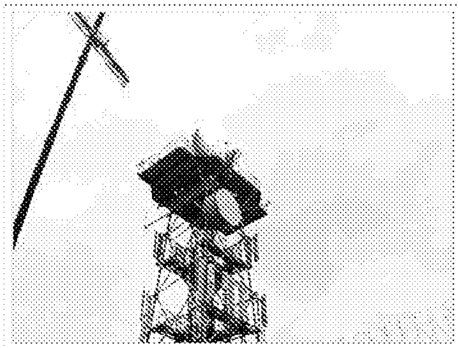
Overview

Appendix - 64

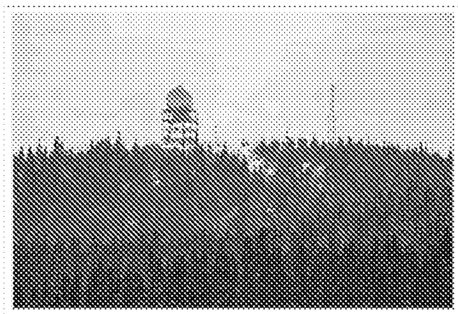
Primary radar

The rapid wartime development of radar had obvious applications for air traffic control (ATC) as a means of providing continuous surveillance of air traffic disposition. Precise knowledge of the positions of aircraft would permit a reduction in the normal procedural separation standards, which in turn promised considerable increases in the efficiency of the airways system. This type of radar (now called a *primary radar*) can detect and report the position of anything that reflects its transmitted radio signals including, depending on its design, aircraft, birds, weather and land features. For air traffic control purposes this is both an advantage and a disadvantage. Its targets do not have to co-operate, they only have to be within its coverage and be able to reflect radio waves, but it only indicates the position of the targets, it does not identify them. When primary radar was the only type of radar available, the correlation of individual radar returns with specific aircraft typically was achieved by the controller observing a directed turn by the aircraft. Primary radar is still used by ATC today as a backup/complementary system to secondary radar, although its coverage and information is more limited. [2][3][4]

Secondary radar


Installation of mode S antenna on top of existing primary antenna

The need to be able to identify aircraft more easily and reliably led to another wartime radar development, the Identification Friend or Foe (IFF) system, which had been created as a means of positively identifying friendly aircraft from enemy. This system, which became known in civil use as secondary surveillance radar (SSR), or in the USA as the air traffic control radar beacon system (ATCRBS), relies on a piece of equipment aboard the aircraft known as a "transponder." The transponder is a radio receiver and transmitter pair which receives on 1030 MHz and transmits on 1090 MHz. The target aircraft transponder replies to signals from an interrogator (usually, but not necessarily, a ground station co-located with a primary radar) by transmitting a coded reply signal containing the requested information.[5]


Independent secondary surveillance radar (ISSR), designation YMT, north of Chibougamau, Quebec, Canada

Both the civilian SSR and the military IFF have become much more complex than their war-time ancestors, but remain compatible with each other, not least to allow military aircraft to operate in civil airspace. Today's SSR can provide much more detailed information, for example, the aircraft altitude, as well as enabling the direct exchange of data between aircraft for collision avoidance. Most SSR systems rely on Mode C transponders, which report the aircraft pressure altitude. On the ground, the pressure altitude is adjusted, based on local air pressure readings, to calculate the true altitude of the aircraft. Inside the aircraft, pilots use a similar procedure, by adjusting their altimeter settings with respect to the local air pressure. Pilots may obtain the local air pressure information from air traffic control or from the Automatic Terminal Information Service (ATIS). If the altimeter setting is wrong, the transponder may report the wrong pressure altitude for the aircraft. This has led to accidents, such as the case of Aeroperú Flight 603.[6]

Given its primary military role of reliably identifying friends, IFF has much more secure (encrypted) messages to prevent "spoofing" by the enemy, and is used on many types of military platforms including air, sea and land vehicles.

Standards and specifications

The International Civil Aviation Organization (ICAO) is a branch of the United Nations and its headquarters are in Montreal, Canada. It publishes annexes to the Convention and Annex 10 addresses Standards and Recommended Practices for Aeronautical Telecommunications. The objective is to ensure that aircraft crossing international boundaries are compatible with the Air Traffic Control systems in all countries that may be visited. Volume III, Part 1 is concerned with digital data communication systems including the data link functions of Mode S while volume IV defines its operation and signals in space.[7]

The American Radio Technical Commission for Aeronautics (RTCA) and the European Organization for Civil Aviation Equipment (Eurocae) produce *Minimum Operational Performance Standards* for both ground and airborne equipment in accordance with the standards specified in ICAO Annex 10. Both organisations frequently work together and produce common documents.

ARINC (Aeronautical Radio, Incorporated) is an airline run organisation concerned with the form, fit and function of equipment carried in aircraft. Its main purpose is to ensure competition between manufacturers by specifying the size, power requirements, interfaces and performance of equipment to be located in the equipment bay of the aircraft.

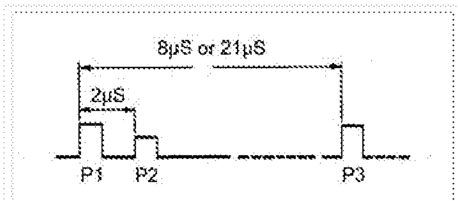
Operation

The purpose of SSR is to improve the ability to detect and identify aircraft while automatically providing the Flight Level (pressure altitude) of an aircraft. An SSR ground station transmits interrogation pulses on 1030 MHz (continuously in Modes A, C and selectively, in Mode S) as its antenna rotates, or is electronically scanned, in space. An aircraft transponder within line-of-sight range 'listens' for the SSR interrogation signal and transmits a reply on 1090 MHz that provides aircraft information. The reply sent depends on the interrogation mode. The aircraft is displayed as a tagged icon on the controller's radar screen at the measured bearing and range. An aircraft without an operating transponder still may be observed by primary radar, but would be displayed to the controller without the benefit of SSR derived data. It is typically a requirement to have a working transponder in order to fly in controlled air space and many aircraft have a back-up transponder to ensure that condition is met.[8]

Interrogation modes

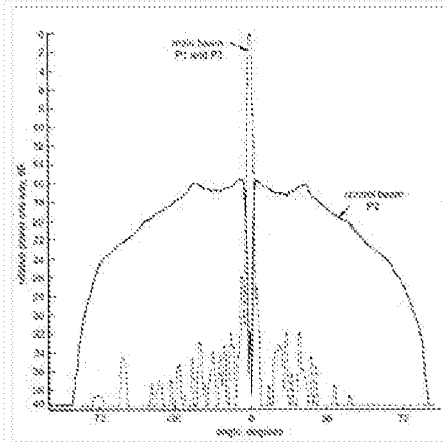
There are several modes of interrogation, each indicated by the difference in spacing between two transmitter pulses, known as P1 and P3.[7] Each mode produces a different response from the aircraft. A third pulse, P2, is for side lobe suppression and is described later. Not included are additional military (or IFF) modes, which are described in Identification Friend or Foe.

Mode	P1–P3 Pulse spacing	Purpose
A	8 μs	identity
B	17 μs	identity
C	21 μs	altitude
D	25 μs	undefined
S	3.5 μs	multipurpose



Mode A and C interrogation format

A mode-A interrogation elicits a 12-pulse reply, indicating an identity number associated with that aircraft. The 12 data pulses are bracketed by two framing pulses, F1 and F2. The X pulse is not used. A mode-C interrogation produces an 11-pulse response (pulse D1 is not used), indicating aircraft altitude as indicated by its altimeter in 100-foot increments. Mode B gave a similar response to mode A and was at one time used in Australia. Mode D has never been used operationally.



Sum and Control antenna beams

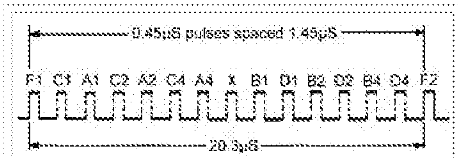
The new mode, Mode S, has different interrogation characteristics. It comprises pulses P1 and P2 from the antenna main beam to ensure that Mode-A and Mode-C transponders do not reply, followed by a long phase-modulated pulse.[7]

The ground antenna is highly directional but cannot be designed without sidelobes. Aircraft could also detect interrogations coming from these sidelobes and reply appropriately. However these replies can not be differentiated from the intended replies from the main beam and can give rise to a false aircraft indication at an erroneous bearing. To overcome this problem the ground antenna is provided with a second, mainly omni-directional, beam with a gain which exceeds that of the sidelobes but not that of the main beam. A third pulse, P2, is transmitted from this second beam 2 μs after P1. An aircraft detecting P2 stronger than P1 (therefore in the sidelobe and at the incorrect main lobe bearing), does not reply.[7]

Deficiencies

A number of problems are described in an ICAO publication of 1983 entitled *Secondary Surveillance Radar Mode S Advisory Circular*.[9]

Mode A



Mode A and C reply format

Although 4,096 different identity codes available in a mode A reply may seem enough, once particular codes have been reserved for emergency and other purposes, the number is significantly reduced. Ideally an aircraft would keep the same code from take-off until landing even when crossing international boundaries, as it is used at the air traffic control centre to display the aircraft's callsign using a process known as code/callsign conversion. Clearly the same mode A code should not be given to two aircraft at the same time as the controller on the ground could be given the wrong callsign with which to communicate with the aircraft.[7]

Mode C

The mode C reply provides height increments of 100 feet, which was initially adequate for monitoring aircraft separated by at least 1000 feet. However, as airspace became increasingly congested, it became important to monitor whether aircraft were not moving out of their assigned flight level. A slight change of a few feet could cross a threshold and be indicated as the next increment up and a change of 100 feet. Smaller increments were desirable.

Fruit

Since all aircraft reply on the same frequency of 1090 MHz, a ground station will also receive aircraft replies originating from responses to other ground stations. These unwanted replies are known as FRUIT (False Replies Unsynchronized with Interrogator Transmissions or alternatively False Replies Unsynchronized In Time). Several successive fruit replies could combine and appear to indicate an aircraft which does not exist. As air transport expands and more aircraft occupy the airspace, the amount of fruit generated will also increase.[9]

Garble

Fruit replies can overlap with wanted replies at a ground receiver, thus causing errors in extracting the included data. A solution is to increase the interrogation rate so as to receive more replies, in the hope that some would be clear of interference. The process is self-defeating as increasing the reply rate only increases the interference to other users and vice versa.[9]

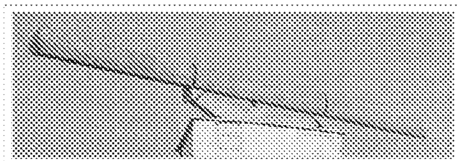
Synchronous garble

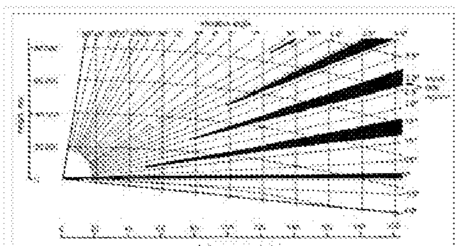
If two aircraft paths cross within about two miles slant range from the ground interrogator, their replies will overlap and the interference caused will make their detection difficult. Typically the controller will lose the longer range, and later to reply, aircraft just when the former may be most interested in monitoring them closely.[9]

Capture

While an aircraft is replying to one ground interrogation it is unable to respond to another interrogation, reducing detection efficiency. For a Mode A or C interrogation the transponder reply may take up to 120 μs before it can reply to a further interrogation.[9]

Antenna


Original SSR antenna providing a narrow horizontal beam and a wide vertical beam


Regions of weak signal due to ground reflection

The ground antenna has a typical horizontal 3 dB beamwidth of 2.5° which limits the accuracy in determining the bearing of the aircraft. Accuracy can be improved by making many interrogations as the antenna beam scans an aircraft and a better estimate can be obtained by noting where the replies started and where stopped and taking the centre of the replies as the direction of the aircraft. This is known as a sliding window process.[1]

The early system used an antenna known as a *hogtrough*. This has a large horizontal dimension to produce a narrow horizontal beam and a small vertical dimension to provide cover from close to the horizon to nearly overhead. There were two problems with this antenna. First, nearly half the energy is directed at the ground where it is reflected back up, and interferes with, the upward energy causing deep nulls at certain elevation angles and loss of contact with aircraft. Second, if the surrounding ground is sloping, then the reflected energy is partly offset horizontally, distorting the beam shape and the indicated bearing of the aircraft. This was particularly important in a monopulse system with its much improved bearing measurement accuracy.[10]

Developments to address the deficiencies

The deficiencies in modes A and C were recognised quite early in the use of SSR and in 1967 Ullyatt published a paper[11] and in 1969 an expanded paper,[12] which proposed improvements to SSR to address the problems. The essence of the proposals was new interrogation and reply formats. Aircraft identity and altitude were to be included in the one reply so collation of the two data items would not be needed. To protect against errors a simple parity system was proposed – see *Secondary Surveillance Radar – Today and Tomorrow*.[13] Monopulse would be used to determine the bearing of the aircraft thereby reducing to one the number of interrogations/replies per aircraft on each scan of the antenna. Further each interrogation would be preceded by main beam pulses P1 and P2 separated by 2 μs so that transponders operating on modes A and C would take it as coming from the antenna sidelobe and not reply and not cause unnecessary fruit.[12]

The FAA were also considering similar problems but were assuming that a new pair of frequencies would be required. Ullyatt showed that the existing 1030 MHz and 1090 MHz frequencies could be retained and the existing ground interrogators and airbornes transponders, with suitable modifications, could be used. The result was a Memorandum of Understanding between the US and the UK to develop a common system. In the US the programme was called DABS (Discrete Address Beacon System), and in the UK Adsel (Address selective).[14]

Monopulse, which means single pulse, had been used in military track-and-follow systems whereby the antenna was steered to follow a particular target by keeping the target in the centre of the beam. Ullyatt proposed the use of a continuously rotating beam with bearing measurement made wherever the pulse may arrive in the beam.[15]

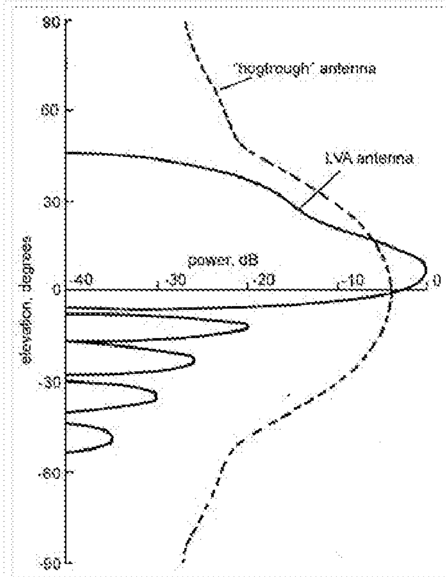
The FAA engaged Lincoln Laboratory of MIT to further design the system and it produced a series of ATC Reports defining all aspects of the new joint development.[16] Notable additions to the concept proposed by Ullyatt was the use of a more powerful 24-bit parity system using a cyclic redundancy code, which not only ensured the accuracy of the received data without the need for repetition but also allowed errors caused by an overlapping fruit reply to be corrected. Further the proposed aircraft identity code also comprised 24 bits with 16 million permutations. This allowed each aircraft to be wired with its own unique address. Blocks of addresses are allocated to different countries[17] and further allocated to particular airlines so that knowledge of the address could identify a particular aircraft. The Lincoln Laboratory report ATC 42 entitled *Mode S Beacon System: Functional Description* gave details on the proposed new system.[18]

The two countries reported the results of their development in a joint paper, *ADSEL/DABS – A Selective Address Secondary Surveillance Radar*.[14] This was followed at a conference at ICAO Headquarters in Montreal, at which a low-power interrogation constructed by Lincoln Laboratory successfully communicated with an upgraded commercial SSR transponder of UK manufacture.

The only thing needed was an international name. Much had been made of the proposed new features but the existing ground SSR interrogators would still be used, albeit with modification, and the existing airbound transponders, again with modification. The best way of showing that this was an evolution not a revolution was to still call it SSR but with a new mode letter. Mode S was the obvious choice, with the S standing for select. In 1983 ICAO issued an advisory circular, which described the new system.[9]

Improved antenna

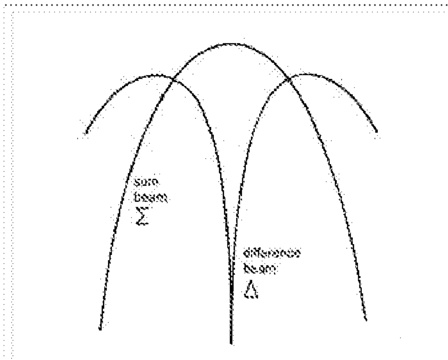
The problem with the existing standard "hogtrough" antenna was caused by the energy radiated toward the ground, which was reflected up and interfered with the upwards directed energy. The answer was to shape the vertical beam. This necessitated a vertical array of dipoles suitably fed to produce the desired shape. A five-foot vertical dimension was found to be optimum and this has become the international standard.[10]



Comparison of the vertical beam shapes of the old and new antennas

Monopulse secondary surveillance radar

The new Mode S system was intended to operate with just a single reply from an aircraft, a system known as monopulse. The accompanying diagram shows a conventional main or "sum" beam of an SSR antenna to which has been added a "difference" beam. To produce the sum beam the signal is distributed horizontally across the antenna aperture. This feed system is divided into two equal halves and the two parts summed again to produce the original sum beam. However the two halves are also subtracted to produce a difference output. A signal arriving exactly normal, or boresight, to the antenna will produce a maximum output in the sum beam but a zero signal in the difference beam. Away from boresight the signal in the sum beam will be less but there will be a non-zero signal in the difference beam. The angle of arrival of the signal can be determined by measuring the ratio of the signals between the sum and difference beams. The ambiguity about boresight can be resolved as there is a 180° phase change in the difference signal either side of boresight. Bearing measurements can be made on a single pulse, hence monopulse, but accuracy can be improved by averaging measurements made on several or all of the pulses received in a reply from an aircraft. A monopulse receiver[15] was developed early in the UK Adsel programme and this design is still used widely today. Mode S reply pulses are deliberately designed to be similar to mode A and C replies so the same receiver can be used to provide improved bearing measurement for the SSR mode A and C system with the advantage that the interrogation rate can be substantially reduced thereby reducing the interference caused to other users of the system.[19]



Antenna main beam with difference beam

Lincoln Laboratory exploited the availability of a separate bearing measurement on each reply pulse to overcome some of the problems of garble whereby two replies overlap making associating the pulses with the two replies. Since each pulse is separately labelled with direction this information can be used to unscramble two overlapping mode A or C replies. The process is presented in ATC-65 "The ATCRBS Mode of DABS".[20] The approach can be taken further by also measuring the strength of each reply pulse and using that as a discriminate as well.[1] The following table compares the performance of conventional SSR, monopulse SSR (MSSR) and Mode S.[19]

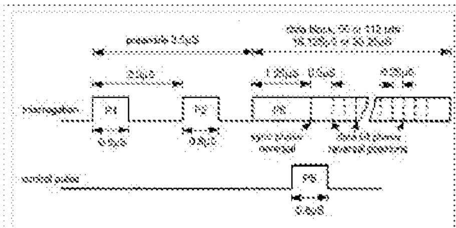
Appendix - 70

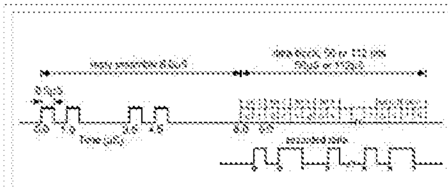
	Standard SSR	Monopulse SSR	Mode S
Replies per scan	20–30	4–8	1
Range accuracy	230 m rms	13 m rms	7 m rms
Bearing accuracy	0.08° rms	0.04° rms	0.04° rms
Height resolution	100 ft (30 m)	100 ft	25 ft (7.6 m)
Garble resistance	poor	good	best
Data capacity (uplink)	0	0	56–1,280 bits
Data capacity (downlink)	23 bits	23 bits	56–1,280 bits
Identity permutations	4,096	4,096	16 million

The MSSR replaced most of the existing SSRs by the 1990s and its accuracy provided for a reduction of separation minima in en-route ATC from 10 nautical miles (19 km; 12 mi) to 5 nautical miles (9.3 km; 5.8 mi)[21]

MSSR resolved many of the system problems of SSR, as changes to the ground system only, were required. The existing transponders installed in aircraft were unaffected. It undoubtedly resulted in the delay of Mode S.[16]

Mode S


Mode S interrogation, short and long


Mode S reply, short and long

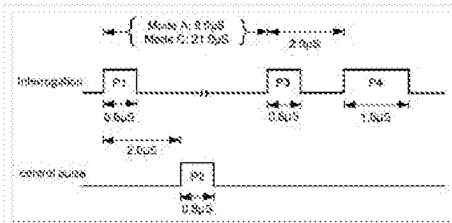
A more detailed description of Mode S is given in the Eurocontrol publication *Principles of Mode S and Interrogator Codes*[8] and the ICAO circular 174-AN/110 *Secondary Surveillance Radar Mode S Advisory Circular*.[9] The 16 million permutations of the 24 bit aircraft address codes have been allocated in blocks to individual states and the assignment is given in ICAO Annex 10, Volume III, Chapter 9.[17]

A mode S interrogation comprises two 0.8 μs wide pulses,[18] which are interpreted by a mode A & C transponder as coming from an antenna sidelobe and therefore a reply is not required. The following long P6 pulse is phase modulated with the first phase reversal, after 1.25 μs, synchronising the transponder's phase detector. Subsequent phase reversals indicate a data bit of 1, with no phase reversal indicating a bit of value 0. This form of modulation provides some resistance to corruption by a chance overlapping pulse from another ground interrogator. The interrogation may be short with P6 = 16.125 μs, mainly used to obtain a position update, or long, P6 = 30.25 μs, if an additional 56 data bits are included. The final 24 bits contain both the parity and address of the aircraft. On receiving an interrogation, an aircraft will decode the data and calculate the parity. If the remainder is not the address of the aircraft then either the interrogation was not intended for it or it was corrupted. In either case it will not reply. If the ground station was expecting a reply and did not receive one then it will re-interrogate.[9]

The aircraft reply[18] consists of a preamble of four pulses spaced so that they cannot be erroneously formed from overlapping mode A or C replies. The remaining pulses contain data using pulse position amplitude modulation. Each 1 μs interval is divided into two parts. If a 0.5 μs pulse occupies the first half and there is no pulse in the second half then a binary 1 is indicated. If it is the other way round then it represents a binary 0. In effect the data is transmitted twice, the second time in inverted form. This format is very resistant to error due to a garbling reply from another aircraft. To cause a hard error one pulse has to be cancelled and a second pulse inserted in the other half of the bit period. Much more likely is that both halves are confused and the decoded bit is flagged as "low confidence".[20]

The reply also has parity and address in the final 24 bits. The ground station tracks the aircraft and uses the predicted position to indicate the range and bearing of the aircraft so it can interrogate again and get an update of its position. If it is expecting a reply and if it receives one then it checks the remainder from the parity check against the address of the expected aircraft. If it is not the same then either it is the wrong aircraft and a re-interrogation is necessary, or the reply has been corrupted by interference by being garbled by another reply. The parity system has the power to correct errors as long as they do not exceed 24 μs, which embraces the duration of a mode A or C reply, the most expected source of interference in the early days of Mode S. The pulses in the reply have individual monopulse angle measurements available, and in some implementations also signal strength measurements, which can indicate bits that are inconsistent with the majority of the other bits, thereby indicating possible corruption. A test is made by inverting the state of some or all of these bits (a 0 changed to a 1 or vice versa) and if the parity check now succeeds the changes are made permanent and the reply accepted. If it fails then a re-interrogation is required.[9]

Mode S operates on the principle that interrogations are directed to a specific aircraft using that aircraft's unique address. This results in a single reply with aircraft range determined by the time taken to receive the reply and monopulse providing an accurate bearing measurement. In order to interrogate an aircraft its address must be known. To meet this requirement the ground interrogator also broadcasts All-Call interrogations, which are in two forms.[9]


Mode A/C/S All-Call interrogation

In one form, the Mode A/C/S All-Call looks like a conventional Mode A or C interrogation at first and a transponder will start the reply process on receipt of pulse P3. However a Mode S transponder will abort this procedure upon the detection of pulse P4, and instead respond with a short Mode S reply containing its 24 bit address. This form of All-Call interrogation is now not much used as it will continue to obtain replies from aircraft already known and give rise to unnecessary interference. The alternative form of All-Call uses short Mode S interrogation with a 16.125 μs data block. This can include an indication of the interrogator transmitting the All-Call with the request that if the aircraft has already replied to this interrogator then do not reply again as aircraft is already known and a reply unnecessary.[9]

The Mode S interrogation can take three forms:

name	form	use
Surveillance	short	position update
Comm-A	long	contains 56 data bits
Comm-C	long	up to 16 long interrogations strung together to transmit up to 1280 bits

The first five bits, known as the uplink field (UF) in the data block indicate the type of interrogation. The final 24 bits in each case is combined aircraft address and parity. Not all permutations have yet been allocated but those that have are shown:[9]

UF	application
00000	short air-air surveillance (TCAS)
00100	surveillance, altitude request
00101	surveillance, Mode A identity request}
01011	Mode S only All-Call
10000	long air-air surveillance (TCAS)
10100	Comm-A including altitude request
10101	Comm-A including Mode A identity request
11	Comm-C (extended length message)

Similarly the Mode S reply can take three forms:[9]

name	form	use
Surveillance	short	position update
Comm-B	long	contains 56 data bits
Comm-D	long	up to 16 long interrogations strung together to transmit up to 1280 bits

The first five bits, known as the downlink field (DF) in the data block indicate the type of reply. The final 24 bits in each case is combined aircraft address and parity. Eleven permutations have been allocated.[9]

DF binary	DF decimal	application
00000	0	short air-air surveillance (TCAS)
00100	4	surveillance, altitude reply
00101	5	surveillance, Mode A identity reply
01011	11	All-Call reply containing aircraft address
10000	16	long air-air surveillance (TCAS)
10001	17	extended squitter
10010	18	TIS-B
10011	19	military extended squitter
10100	20	Comm-B including altitude reply
10101	21	Comm-B reply including Mode A identity
10110	22	military use
11	24	up to 16 long replies strung together to transmit up to 1280 bits

A transponder equipped to transmit Comm-B replies is fitted with 256 data registers each of 56 bits. The contents of these registers are filled and maintained from on-board data sources. If the ground system requires this data then it requests it by a Surveillance or Comm-A interrogation.[9]

ICAO Annex 10 Volume III, Chapter 5 lists the contents of all those currently allocated. A reduced number are required for current operational use.[22][23] Other registers are intended for use with TCAS and ADS-B. The Comm-B Data Selector (BDS) numbers are in hexadecimal notation.

register	data
BDS 6,0	magnetic heading
BDS 6,0	indicated airspeed
BDS 6,0	Mach number
BDS 6,0	vertical rate
BDS 5,0	roll angle
BDS 5,0	track angle rate
BDS 5,0	true track angle
BDS 5,0	ground speed
BDS 4,0	selected vertical intent

Extended squitter

Starting in 2009, the ICAO defined an "extended squitter" mode of operation;[24] it supplements the requirements contained in ICAO Annex 10, Volumes III and IV. The first edition specified earlier versions of extended squitter messages:

Version 0

Extends Mode S to deal with basic ADS-B exchanges, to add traffic information broadcast (TIS-B) format information, as well as uplink and downlink broadcast protocol information.

Version 1

Better describes surveillance accuracy and integrity information (navigation accuracy category, navigation integrity category, surveillance integrity level), and additional parameters for TIS-B and ADS-B rebroadcast (ADS-R).

Version 2

The second edition introduced yet a new version of extended squitter formats and protocols to:[25]

- enhance integrity and accuracy reporting
- add a number of additional parameters to support identified operational needs for the use of ADS-B not covered by Version 1 (including capabilities to support airport surface applications)
- modify several parameters, and remove a number of parameters, which are no longer required to support ADS-B applications

See also

- Air traffic control radar beacon system, all encompassing description
- Automatic dependent surveillance-broadcast, free flight enhancement
- Traffic collision avoidance system

- Transponder landing system

References

1. *Secondary Surveillance Radar*, Stevens M.C. Artech House, ISBN 0-89006-292-7
2. "Air Traffic Services Surveillance Systems, Including An Explanation of Primary and Secondary Radar". www.airwaysmuseum.com. Retrieved 2009-06-20.
3. "AIR TRAFFIC CONTROL RADAR". Argos Press. Retrieved 2009-06-20.
4. "Secondary Surveillance Radar in ATC Systems: A description of the advantages and implications to the controller of the introduction of SSR facilities". Aircraft Engineering and Aerospace Technology. Retrieved 2009-06-20.
5. Illman, Paul E. (1998). *The pilot's radio communications handbook (Fifth Edition, Paperback)*. McGraw-Hill. p. 111. ISBN 0-07-031832-8.
6. Aeroperú Flight 603 Final Report (unofficial English translation) (http://www.skybrary.aero/bookshelf/books/1719.pdf) (Archive (http://www.webcitation.org/644kQDbbb)) hosted at SKYbrary The original Spanish report, available via mail, is by the Accident Investigation Board, Directorate General of Air Transport, Ministry of Transportation and Communications.
7. ICAO Annex 10, Volume IV
8. *Principles of Mode S Operation and Interrogator Codes* (https://www.eurocontrol.int/sites/default/files/publication/files/surveillance-modes-principles-of-modes-operation-and-interrogator-codes-20030318.pdf)
9. ICAO Circular 174-AN/110 *Secondary Surveillance Radar Mode S Advisory Circular*
10. Stevens, M.C. "Multipath and interference effects in secondary surveillance radar systems", Proc. Inst.Electr. Eng., Part F, 128(1), 43–53, 1981
11. Ullyatt, C. *Secondary radar in the era of auto-tracking*, IEE Comf. Pub., 28, 140, 1967
12. Ullyatt, C. *Sensors for the ATC environment with special reference to SSR*, Electron. Civil Aviat., 3, C1–C3, 1969
13. Stevens, M. C., *Secondary Surveillance Radar – Today and Tomorrow*, SERT Avionics Symposium, Swansea, July 1974.
14. Bowes R.C., Drouilhet P.R., Weiss H.G. and Stevens M.C., *ADSEL/DABS – A Selective Address Secondary Surveillance Radar*,AGARD Conference Proceedings No. 188. 20th Symposium of the Guidance and Control Panel held in Cambridge, Massachusetts, USA, 20–23 May 1975
15. Stevens, M.C. *Precision secondary radar*, Proc. Inst. Electr. Eng., 118(12), 1729–1735, 1971
16. *The Story of Mode S: An Air Traffic Control Data Link Technology (http://mit.edu/6.933/www/Fall2000/mode-s/)*: Mode S Today, Chang E., Hu R., Lai D., Li R., Scott Q., Tyan T., December 2000
17. *ICAO Annex 10* (PDF). ICAO https://web.archive.org/web/20080815000000*/http://www.smalluas.com/download/ICAO_Annex_10_Volume_III.pdf. Archived from the original (PDF) on 2008-11-22. Retrieved 2014-03-29. Missing or empty `|title=` (help); `|chapter=` ignored (help)
18. Orlando V.A., Drouilhet P.R. (August 1986). "ATC-42 Mode S Beacon System: Functional Description (Rev D)" (PDF). Lincoln Laboratory. Retrieved March 29, 2014.
19. Stevens, M.C. S*urveillance in the Mode S Era*, CAA/IEE Symposium on ATC, London. March 1990
20. Gertz J. L. (January 1977). "ATC-65 The ATCRBS Mode of DABS" (PDF). Lincoln Laboratory (MIT). Retrieved March 29, 2014.
21. FAA (2004). *Aviation System Capital Investment Plan*. DIANE Publishing Company. ISBN 978-0-7881-3348-0.
22. Manual on Mode S Specific Services, Panel Working Group B *Surveillance and Conflict Resolution Systems*, September 2001
23. *Carriage of SSR Mode S Transponders for IFR Flights Operating as General Traffic*, www.caa.co.uk/docs/810/
24. ICAO (2008). *ICAO Doc 9871, Technical Provisions for Mode S and Extended Squitter* (1 ed.). International Civil Aviation Organization. ISBN 978-92-9231-117-9.
25. ICAO (2012). *ICAO Doc 9871, Technical Provisions for Mode S and Extended Squitter* (2 ed.). International Civil Aviation Organization. ISBN 978-92-9249-042-3.

Further reading

Industry specifications

- *Annex 10 - Volume IV - Surveillance Radar and Collision Avoidance Systems* (http://store1.icao.int/index.php/publications/annexes/10-aeronautical-telecommunications/annex-10-volume-iv-surveillance-radar-and-collision-avoidance-systems-english-printed.html); 4th Edition; ICAO; 280 pages; 2007.
- *DO-181E Minimum Operational Performance Standards for ATCRBS / Mode S Airborne Equipment* (http://www.rtca.org/store_product.asp?prodid=933); Rev E; RTCA; 2011.

External links

- Eurocontrol Advanced Surface Movement and Ground Control System (A-SMGCS) (http://www.eurocontrol.int/airports/gallery/content/public/pdf/13_A-SMGCS_Mode-S_Transponder-in-an-Airport-Environment_v1-1_20050503.pdf)
- Eurocontrol reference Mode S Home page (http://www.eurocontrol.int/msa/public/standard_page/nv_modes_homepage.html)
- Radar Basics (http://www.radartutorial.eu/index.en.html)
- "ATCRBS" (http://www.flightglobal.com/pdfarchive/view/1961/1961%20-%200860.html) a 1961 *Flight* article on SSR

Categories: Radio stations and systems ITU

Electronic Acknowledgement Receipt

EFS ID:	25381786
Application Number:	14146202
International Application Number:	
Confirmation Number:	7721
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Customer Number:	23497
Filer:	Jed Margolin
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	04-APR-2016
Filing Date:	02-JAN-2014
Time Stamp:	05:53:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Arguments/Remarks Made in an Amendment	jm_adsb2_response.pdf	7114379 590a0f71675c934bbfe17dd6e2408509ad357089	no	95

Warnings:

Information:

Total Files Size (in bytes):	7114379

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

23497 7590 01/21/2016

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

EXAMINER	
BRAINARD, TIMOTHY A	

ART UNIT	PAPER NUMBER
3648	

MAIL DATE	DELIVERY MODE
01/21/2016	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 14/146,202	Applicant(s) MARGOLIN, JED	
	Examiner TIMOTHY A. BRAINARD	Art Unit 3648	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 2/4/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) 1-20 is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.
6)☐ Claim(s) _____ is/are allowed.
7)☒ Claim(s) 1-20 is/are rejected.
8)☐ Claim(s) _____ is/are objected to.
9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.
11)☒ The drawing(s) filed on 1/2/2014 is/are: a)☒ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.
3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
4) ☐ Other: _____.

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

3. Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-14 of **U.S. Patent No. 8643534** in view of **Wu** et al (US 20110156878). **U.S. Patent No. 8643534** claims (claim 1) system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) an ADS-B receiver; (c) an ADS-B antenna; (d) an ADS-B antenna multiplexer; (e) an ADS-B processor; (f) a radar processor; (h) a display; whereby (i) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B multiplexer is configured to allow either said ADS-B transmitter or said ADS-B receiver to use said ADS-B antenna, (j) said ADS-B processor and said radar processor are configured to work together, (k) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through said ADS-B antenna multiplexer to said ADS-B antenna, (1) said transmitted signal is reflected by a target producing a reflected signal, (m) said reflected signal is received by said ADS-B antenna, and said ADS-B antenna multiplexer is configured to send said reflected signal to said ADS-B receiver, (n) said radar processor is configured to process said reflected signal from said ADS-B receiver

and said transmitted signal from said ADS-B transmitter to determine a range to said target (claim 1), (claim 2) (a) if said range to said target does not match a possible position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item, (b) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target, (c) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target, (d) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target and said radar processor is configured to note said discrepancy on said display as a second attention item, and (e) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item (claim 2) (claim 4) said radar processor is incorporated into said ADS-B processor (claim 3), (claim 5) a system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) an ADS-B receiver; (c) a first ADS-B antenna; (d) a second ADS-B antenna; (e) an antenna controller; (f) an ADS-B antenna multiplexer; (g) an ADS-B processor; (h) a radar processor; (j) a display; whereby (k) said second ADS-B antenna is directional, and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna, (1) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, (m) said ADS-B processor and said radar processor are configured to work together, (n) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer, (o) said transmitted signal is reflected by a target producing a reflected signal, (p) said reflected signal is received by either or both said first ADS-B antenna and said second ADS-B antenna, and said ADS-B antenna multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said ADS-B receiver, (q) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (r) said radar processor is configured to use the direction of said second ADS-B antenna to determine a bearing to said target, (t) said radar processor is configured to display said range and said bearing on said display (claim 1), (claim 6) (a) if said range and said bearing to said target do not match the position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item, (b) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target, (c) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target, (d) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target, and said radar processor is configured to note said discrepancy on said display as a second attention item, and (e) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item (claim 2), (claim 8) said radar processor is incorporated into said ADS-B processor (claim 3), (claim 9) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna (claim 4), (claim 10) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (claim 5), (claim 11) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna (claim 6), (claim 12) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (claim 7), (claim 13) system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) a first ADS-B receiver; (c) a first ADS-B antenna; (d) a second ADS-B receiver; (e) a second ADS-B antenna; (0 an antenna controller; (g) an ADS-B antenna multiplexer; (h) an ADS-B processor; (i) a radar processor; (k) a display; whereby (1) said second ADS-B antenna is directional and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna, (m) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said first ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said second ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, (n) said ADS-B processor and said radar processor work together, (o) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer, (p) said transmitted signal is reflected by a target producing a reflected signal, (q) said reflected signal is received by either or both said first ADS-B antenna or said second ADS-B antenna, and said ADS-B multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said second ADS-B receiver, (r) said radar processor is configured to process said reflected signal from said second ADS- B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (s) said radar processor is configured to use the direction of said second antenna to determine a bearing to said target, (u) said radar processor is configured to display said range and said bearing on said display (claim 8), (claim 14) (a) if said range and said bearing to said target do not match the position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item, (b) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target, (c) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target, (d) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target, and said radar processor is configured to note said discrepancy on said display as a second attention item, and (e) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item (claim 9) (claim 16) said radar processor is incorporated into said ADS-B processor (claim 10), (claim 17) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna (claim 11), (claim 18) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (claim 12), (claim 19) aid second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna (claim 13), (claim 20) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (claim 14). **U.S. Patent No. 8643534** does not teach said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal and said datastream comparator is incorporated into said radar processor. **Wu** teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify **U.S. Patent No. 8643534** to include said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new or unexpected results.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 3-5, 7-8, 13, and 15-16 are rejected under 35 U.S.C. 103 as being unpatentable over Margolin (US 20110169684) in view of Wu et al (US 20110156878). **Margolin** teaches (claim 1) a system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) an ADS-B receiver; (c) an ADS-B antenna; (d) an ADS-B antenna multiplexer; (e) an ADS-B processor; (f) a radar processor; (g) a datastream comparator; (h) a display; whereby (i) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B multiplexer is configured to allow either said ADS-B transmitter or said ADS-B receiver to use said ADS-B antenna, (j)

said ADS-B processor and said radar processor are configured to work together, (k) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through said ADS-B antenna multiplexer to said ADS-B antenna, (1) said transmitted signal is reflected by a target producing a reflected signal, (m) said reflected signal is received by said ADS-B antenna, and said ADS-B antenna multiplexer is configured to send said reflected signal to said ADS-B receiver, (n) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (o) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and (p) said radar processor is configured to display said range on said display (claim 1) (claim 4) said radar processor is incorporated into said ADS-B processor (claim 2), (claim 5) a system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) an ADS-B receiver; (c) a first ADS-B antenna; (d) a second ADS-B antenna; (e) an antenna controller; (f) an ADS-B antenna multiplexer; (g) an ADS-B processor; (h) a radar processor; (i) a datastream comparator; (j) a display; whereby (k) said second ADS-B antenna is directional, and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna, (1) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, (m) said ADS-B processor and said radar processor are configured to work together, (n) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer, (o) said transmitted signal is reflected by a target producing a reflected signal, (p) said reflected signal is received by either or both said first ADS-B antenna and said second ADS-B antenna, and said ADS-B antenna multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said ADS-B receiver, (q) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (r) said radar processor is configured to use the direction of said second ADS-B antenna to determine a bearing to said target, (s) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and (t) said radar processor is configured to display said range and said bearing on said display (claim 3), (claim 8) said radar processor is incorporated into said ADS-B processor (claim 4), (claim 13) system for sensing aircraft and other objects comprising: (a) an ADS-B transmitter; (b) a first ADS-B receiver; (c) a first ADS-B antenna; (d) a second ADS-B receiver; (e) a second ADS-B antenna; (0 an antenna controller; (g) an ADS-B antenna multiplexer; (h) an ADS-B processor; (i) a radar processor; (j) a datastream comparator; (k) a display; whereby (1) said second ADS-B antenna is directional and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna, (m) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said first ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said second ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, (n) said ADS-B processor and said radar processor work together, (o) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer, (p) said transmitted signal is reflected by a target producing a reflected signal, (q) said reflected signal is received by either or both said first ADS-B antenna or said second ADS-B antenna, and said ADS-B multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said second ADS-B receiver, (r) said radar processor is configured to process said reflected signal from said second ADS- B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target, (s) said radar processor is configured to use the direction of said second antenna to determine a bearing to said target, (t) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and (u) said radar processor is configured to display said range and said bearing on said display (claim 3), (claim 16) said radar processor is incorporated into said ADS-B processor (claim 4). **Margolin** does not teach said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal and said datastream comparator is incorporated into said radar processor. **Wu** teaches said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal (para 7), (claim 3, 7, and 15) said datastream comparator is incorporated into said radar processor (para 39). It would have been obvious to modify **Margolin** to include said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal because it is merely a substitution of a well-known method to determine distance with no new or unexpected results. It would have been obvious to modify **Margolin** to include said datastream comparator is incorporated into said radar processor because it is merely one method to apply to using multiple processors in a radar device.

6. Claims 9-12 and 17-20 are rejected under 35 U.S.C. 103 as being unpatentable over Margolin in view of Wu as applied to claim 5 and 13 above, and further in view of **Donovan** (US 20100090882). **Donovan** teaches (claim 9, 11, 17, and 19) said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and (claim 10, 12, 18, and 20) said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array (para 29). It would have been obvious to modify **Donovan** to include said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna and said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array

because it is merely an implementation to control the ADS-B antenna with no new or unexpected results.

Allowable Subject Matter

7. Claims 2, 6, and 14 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TIMOTHY A. BRAINARD whose telephone number is (571)272-2132. The examiner can normally be reached on Monday - Friday 9:00 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tashiana Adams can be reached on (571) 270-5228. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/TIMOTHY A BRAINARD/
Primary Examiner, Art Unit 3648

Notice of References Cited	Application/Control No. 14/146,202	Applicant(s)/Patent Under Reexamination MARGOLIN, JED	
	Examiner TIMOTHY A. BRAINARD	Art Unit 3648	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,643,534 B2	02-2014	Margolin; Jed	G01S5/12	342/146
*	B	US-2011/0156878 A1	06-2011	Wu; Ryan Haoyun	G01S5/0081	340/10.1
*	C	US-2010/0090882 A1	04-2010	Donovan; Timothy P.	G01S13/781	342/32
*	D	US-2011/0169684 A1	07-2011	Margolin; Jed	G01S5/12	342/30
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7721

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/146,202	01/02/2014 **RULE**	342	3648	

APPLICANTS

INVENTORS

Jed Margolin, VC Highlands, NV;

** **CONTINUING DATA** *************************

This appln claims benefit of 61/887,338 10/05/2013

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☐ No Verified and Acknowledged / Timothy A Brainard / Examiner's Signature	☐ Met after Allowance Initials	NV	4	20	3

ADDRESS

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430
UNITED STATES

TITLE

ADS-B Radar

FILING FEE RECEIVED		
730	FEES: Authority has been given in Paper No.____________ to charge/credit DEPOSIT ACCOUNT No.____________ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other ________________ ☐ Credit

Index of Claims	Application/Control No. 14146202	Applicant(s)/Patent Under Reexamination MARGOLIN, JED
	Examiner TIMOTHY A BRAINARD	**Art Unit** 3648

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☐ **T.D.** ☐ **R.1.47**

CLAIM		DATE								
Final	Original	01/06/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US- 2013/0176163	07-11-2013	Margolin	
	4	US- 5,153,836	10-06-1992	Fraughton, et al.	Abstract
	6	US- 7,414,567	08-19-2008	Zhang, et al.	Cols 3, 6, 7, 8
	8	US- 2011/0140950	09-16-2011	Anderson	Abstract
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4] -Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
	7	EP 2136222 A1	12-23-2009	Persson, et al.	Page 3	

Examiner Signature	/TIMOTHY A BRAINARD/	Date Considered	01/06/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.A.B/

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	2	14 CFR § 91.113(b) Right-of-way rules: Except water operations.	
	3	14 CFR § 91.115(a) Right-of-way rules: Water operations.	
	5	Gulf of Mexico Helo Ops Ready for ADS-B, Aviation Week & Space Technology, FRANCIS FIORINO, 02/26/2007, page 56.	
	9	Sensing Requirements for Unmanned Air Vehicles, AFRL's Air Vehicles Directorate, Control Sciences Division, Systems Development Branch, Wright-Patterson AFB OH, June 2004, http://www.afrlhorizons.com/Briefs/Jun04/VA0306.html .	
	10	Presentation entitled, Developing Sense & Avoid Requirements for Meeting an Equivalent Level of Safety (6MB | ppt), given by RUSS WOLFE, Technology IPT Lead, Access 5 Project at UVS Tech 2006. 18 January 2006.	
	11	Presentation: Integration into the National Airspace System (NAS) given by JOHN TIMMERMAN of the FAA's Air Traffic Organization (July 12, 2005)	
	12	Zone Ready for Drone, April 7, 2006, on the web site for the FAA's Air Traffic Organization Employees, http://www.ato.faa.gov/DesktopDefault.aspx?tabindex=4&tabid=17&itemid=937&mid=103	
	13	Quadrennial Roles and Missions Review Report, Department of Defense, January 2009, Page 29 (PDF page 37) www.defenselink.mil/news/Jan2009/QRMFinalReport_v26Jan.pdf	
	14	Automatic Dependent Surveillance Broadcast (ADS-B) Surveillance Development for Air Traffic Management, PDF Page 5. www.airbus.com/fileadmin/media_gallery/files/brochures_publications/FAST47_5.adsb.pdf	

Examiner Signature	/TIMOTHY A BRAINARD/	Date Considered	01/06/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.A.B/

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Art Unit	
Examiner Name	
Attorney Docket Number	

Sheet 3 of 3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	15	Exploiting the Automatic Dependent Surveillance Broadcast System Via False Target Injection; Thesis by DOMENIC MAGAZU III, CAPTAIN, USAF; AFIT/GCO/ENG/12-07; Department of the Air Force, Air University; Air Force Institute of Technology; March 2012. PDF Pages 49-54. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA561697	
	16	Security of ADS-B: State of the Art and Beyond MARTIN STROHMEIER (University of Oxford, United Kingdom), VINCENT LENDERS (armasuisse, Switzerland), IVAN MARTINOVIC (University of Oxford, United Kingdom); 7/13/2013 http://arxiv-web3.library.cornell.edu/pdf/1307.3664	

Examiner Signature	/TIMOTHY A BRAINARD/	Date Considered	01/06/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.A.B/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	25	(ads-b automatic near3 dependent near3 broadcast$4) same (multiplex$4 switch$3) near5 antenna$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 10:46
S2	28	(ads-b automatic near3 dependent near3 broadcast$4) same (multiplex$4 switch$3) near10 antenna$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 10:47
S3	47	(ads-b automatic near3 dependent near3 broadcast$4) same3 (multiplex$4 switch$3) near10 antenna$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 10:47
S4	13	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 same (datastream data) near14 compar$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 11:08
S5	205	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and (datastream data) near14 compar$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 11:09
S6	205	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and ((datastream data) near14 compar$4 correlat$4 near14 transmit$4 near14 reciev$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 11:15
S7	0	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and (correlat$4 near14 transmit$4 near14 reciev$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 11:15
S8	23	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and (correlat$4 near14 transmit$4 near14 receiv$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 11:16
S9	26	((Jed) near2 (Margolin)).INV.	US-PGPUB; USPAT;	OR	ON	2016/01/06 17:37

			USOCR			
S10	3	(US-20150097714-$ or US-20130176163-$ or US-20110169684-$).did.	US-PGPUB	OR	ON	2016/01/06 17:37
S11	3709	((G01S13/9303 OR G01S11/02 OR G01S13/003 OR G01S5/12 OR G01S13/42).CPC. OR (342/118 OR 342/29 OR 342/30).CCLS. OR (G01S13/93 OR G01S13/00 OR G01S13/75).IPCR.)	US-PGPUB	OR	ON	2016/01/06 17:38
S12	13	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and (gps global$3 near4 position$3) near4 spoof$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 17:45
S13	14	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and (gps global$3 near4 position$3) near8 spoof$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 17:45
S14	12	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and doppler$3 near15 radial$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 17:48
S15	13	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and doppler$3 same radial$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 18:01
S16	875	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 18:07
S17	100	((ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 18:07
S18	107	((ads-b automatic near3 dependent near3 broadcast$4) and radar$2).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 18:07
S19	8	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2 and mechanic$4 near4 (scan$3 scann$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/06 18:53
S20	30	(ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2	US-PGPUB; USPAT;	OR	ON	2016/01/06 18:53

		and electronic$4 near4 (scan$3 scann$3)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S22	3	"20110169684"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/01/08 14:34

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S21	100	((ads-b automatic near3 dependent near3 broadcast$4) same3 radar$2).clm.	US-PGPUB; USPAT	OR	ON	2016/01/06 18:07

1/13/2016 5:38:14 PM
C:\Users\tbrainard\Documents\EAST\Workspaces\14146202.wsp

Search Notes	Application/Control No. 14146202	Applicant(s)/Patent Under Reexamination MARGOLIN, JED
	Examiner TIMOTHY A BRAINARD	Art Unit 3648

CPC- SEARCHED

Symbol	Date	Examiner
G01S13/9303; G01S11/02; G01S13/003; G01S5/12; G01S13/42	1/6/2015	TAB

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
342	29, 30, 118	1/6/2016	TAB

SEARCH NOTES

Search Notes	Date	Examiner
updated east search -- see attached	1/6/2015	TAB

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/146,202	01/02/2014	Jed Margolin	

CONFIRMATION NO. 7721

PUBLICATION NOTICE

OC000000074510545

23497
JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

Title:ADS-B Radar

Publication No.US-2015-0097714-A1
Publication Date:04/09/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/146,202	01/02/2014	Jed Margolin	

CONFIRMATION NO. 7721

23497
JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

NEW OR REVISED PPD NOTICE

OC000000069262675

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 04/09/2015. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.

The following is an example of an acceptable property rights statement. Statements of this type are, of course, only suitable for situations in which NO Agency funds or other considerations were involved in the making or conception of the invention. While this example is in the form of a declaration, a sworn document is equally acceptable.

I(We) Jed Margolin

citizens of United States of America

residing at 1981 Empire Rd., VC Highlands, NV

declare:

That I(we) made and conceived the invention described and claimed in patent application:

Serial Number 14/146,202 filed in the United States of America on 01/02/2014

titled ADS-B Radar

(check and complete either I or II below)

☐ I. *(For Inventors Employed by an Organization)* That I(We) made and conceived this invention while employed by __________.
That the invention is related to the work I am (we are) employed to perform and was made within the scope of my (our) employment duties; That the invention was made during working hours and with the use of facilities, equipment, materials, funds, information and services of __________.
Other relevant facts are __________.

That to the best of my (our) knowledge and belief (and/or) based upon information provided by __________ of __________.

--OR--

☒ II. *(For Self-Employed Inventors)* That I (we) made and conceived this invention on my (our) own time using only my (our) own facilities, equipment, materials, funds, information and services. Other relevant factors are __________.

(check III and/or IV below as appropriate)

That to the best of my (our) knowledge and belief:

☒ III. The invention was not made or conceived in the course of, or in connection with, or under the terms of any contract, subcontract or arrangement entered into with or for the benefit of the United States Atomic Energy Commission or its successors: Energy Research and Development Administration or the Department of Energy.

--AND/OR--

☒ IV. The invention was not made (conceived or first actually reduced to practice) under nor is there any relationship of the invention to the performance of any work under any contract of the National Aeronautics and Space Administration.

The undersigned inventors(s) declare further that all statements made herein of his or her (their) own knowledge are true and that all statements made on information and belief are believed to be true and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Inventor's Signature: Jed Margolin

Post Office Address: 1981 Empire Rd, Reno, NV 89521-7430

Date: 02/04/2014

Inventor's Signature: __________

Post Office Address: __________

Date: __________

Electronic Acknowledgement Receipt

EFS ID:	18109972
Application Number:	14146202
International Application Number:	
Confirmation Number:	7721
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Customer Number:	23497
Filer:	Jed Margolin
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	04-FEB-2014
Filing Date:	02-JAN-2014
Time Stamp:	15:15:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Any request going to L and R	nasa_statement_signed.pdf	81273 9cbadae0603527b1350a91d887e35d3d715baf85	no	1

Warnings:

Information:

Total Files Size (in bytes):	81273

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

01/31/2014

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

EXAMINER	

ART UNIT	PAPER NUMBER
3646	

MAIL DATE	DELIVERY MODE
01/31/2014	PAPER

IF NO RESPONSE TO THIS NOTICE IS RECEIVED WITHIN FORTY-FIVE DAYS, A FORMAL REQUIRMENT WILL BE ISSUED

The subject matter of this application appears to "have significant utility in the conduct of aeronautical and space activities" as recited in 42 U.S.C. 2457 (National Aeronautics and Space Administration (NASA)).

Accordingly, no patent can issue on this application unless applicant(s) file a statement (under oath or in the form of a declaration as provided by 37 CFR 1.68) setting forth (1) the full facts concerning the circumstances under which the invention was made and conceived and (2) the relationship (if any) of the invention to the performance of any work under any contract or other arrangement with the Agency(ies) noted above. On the 2nd page of this form is an example of an acceptable format for this statement. The language appearing in paragraphs III and/or IV of the example must appear if applicant is attempting to establish that no relationship (under item 2 above) exists.

If the invention disclosed in this application was developed under a contract, grant or cooperative agreement between the Agency indicated above and a person, small business or non-profit organization and rights to the invention have been determined by specific reference to 35 U.S.C. 202 in the contract, grant or cooperative agreement, then the applicant need not submit the statement described above. Instead, applicant may file a verified statement (under oath or in the form of a declaration, 37 CFR 1.68) setting forth the information required by 35 U.S.C. 202(c)(6).

IF NO STATEMENT HAS BEEN RECIEVED WITHIN FORTY-FIVE DAYS OF THE MAIL DATE INDICATED ABOVE, a formal 30 day requirement for statement will then be issued. No provision is made for extension of the statutory thirty-day period for response to the formal requirement and the penalty for failure to file an acceptable and timely statement is abandonment of the application. Therefore, applicants are strongly encouraged to submit a statement at this time in order to avoid the issuance of a formal requirement.

IT IS IMPORTANT TO NOTE that the statement must accurately represent the property rights situation of the claimed invention if and when the application is found allowable. Thus, if during prosecution before the examiner, the claimed invention is so altered or the property rights situation so changes to impact the accuracy of a statement submitted earlier, a supplemental statement must be filed. Failure to submit such additional information where appropriate may be considered a false representation of material facts and render the patent owner vulnerable to loss of patent rights and other sanctions as set forth in the statutes. The PTO will not review allowed applications for this possibility. The responsibility for complying with the statutes rests with the applicants.

Any questions regarding this requirment should be directed to Licensing and Review at (571)-272-8203.

PLEASE DIRECT ALL COMMUNICATIONS RELATING TO THIS MATTER TO THE ATTENTION OF MAIL STOP L&R.

FORM PTOL-456 (Rev. 07-08)

The following is an example of an acceptable property rights statement. Statements of this type are, of course, only suitable for situations in which NO Agency funds or other considerations were involved in the making or conception of the invention. While this example is in the form of a declaration, a sworn document is equally acceptable.

I(We) ______________________________

citizens of ______________________________

residing at ______________________________

declare:

That I(we) made and conceived the invention described and claimed in patent application:

Serial Number ______________ filed in the United States of America on ______________

titled ______________________________

(check and complete either I or II below)

❑ I. *(For Inventors Employed by an Organization)* That I(We) made and conceived this invention while employed by ______________. That the invention is related to the work I am (we are) employed to perform and was made within the scope of my (our) employment duties; That the invention was made during working hours and with the use of facilities, equipment, materials, funds, information and services of ______________. Other relevant facts are ______________ ______________.

That to the best of my (our) knowledge and belief (and/or) based upon information provided by ______________

of ______________.

--OR--

❑ II. *(For Self-Employed Inventors)* That I (we) made and conceived this invention on my (our) own time using only my (our) own facilities, equipment, materials, funds, information and services. Other relevant factors are ______________ ______________.

(check III and/or IV below as appropriate)

That to the best of my (our) knowledge and belief:

❑ III. The invention was not made or conceived in the course of, or in connection with, or under the terms of any contract, subcontract or arrangement entered into with or for the benefit of the United States Atomic Energy Commission or its successors: Energy Research and Development Administration or the Department of Energy.

--AND/OR--

❑ IV. The invention was not made (conceived or first actually reduced to practice) under nor is there any relationship of the invention to the performance of any work under any contract of the National Aeronautics and Space Administration.

The undersigned inventors(s) declare further that all statements made herein of his or her (their) own knowledge are true and that all statements made on information and belief are believed to be true and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Inventor's Signature: ______________________________

Post Office Address: ______________________________

Date: ______________________________

Inventor's Signature: ______________________________

Post Office Address: ______________________________

Date: ______________________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/146,202	01/02/2014	Jed Margolin		7721

01/31/2014

JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

EXAMINER	

ART UNIT	PAPER NUMBER
3646	

MAIL DATE	DELIVERY MODE
01/31/2014	PAPER

IF NO RESPONSE TO THIS NOTICE IS RECEIVED WITHIN FORTY-FIVE DAYS, A FORMAL REQUIRMENT WILL BE ISSUED

The subject matter of this application appears to "have significant utility in the conduct of aeronautical and space activities" as recited in 42 U.S.C. 2457 (National Aeronautics and Space Administration (NASA)).

Accordingly, no patent can issue on this application unless applicant(s) file a statement (under oath or in the form of a declaration as provided by 37 CFR 1.68) setting forth (1) the full facts concerning the circumstances under which the invention was made and conceived and (2) the relationship (if any) of the invention to the performance of any work under any contract or other arrangement with the Agency(ies) noted above. On the 2nd page of this form is an example of an acceptable format for this statement. The language appearing in paragraphs III and/or IV of the example must appear if applicant is attempting to establish that no relationship (under item 2 above) exists.

If the invention disclosed in this application was developed under a contract, grant or cooperative agreement between the Agency indicated above and a person, small business or non-profit organization and rights to the invention have been determined by specific reference to 35 U.S.C. 202 in the contract, grant or cooperative agreement, then the applicant need not submit the statement described above. Instead, applicant may file a verified statement (under oath or in the form of a declaration, 37 CFR 1.68) setting forth the information required by 35 U.S.C. 202(c)(6).

IF NO STATEMENT HAS BEEN RECIEVED WITHIN FORTY-FIVE DAYS OF THE MAIL DATE INDICATED ABOVE, a formal 30 day requirement for statement will then be issued. No provision is made for extension of the statutory thirty-day period for response to the formal requirement and the penalty for failure to file an acceptable and timely statement is abandonment of the application. Therefore, applicants are strongly encouraged to submit a statement at this time in order to avoid the issuance of a formal requirement.

IT IS IMPORTANT TO NOTE that the statement must accurately represent the property rights situation of the claimed invention if and when the application is found allowable. Thus, if during prosecution before the examiner, the claimed invention is so altered or the property rights situation so changes to impact the accuracy of a statement submitted earlier, a supplemental statement must be filed. Failure to submit such additional information where appropriate may be considered a false representation of material facts and render the patent owner vulnerable to loss of patent rights and other sanctions as set forth in the statutes. The PTO will not review allowed applications for this possibility. The responsibility for complying with the statutes rests with the applicants.

Any questions regarding this requirment should be directed to Licensing and Review at (571)-272-8203.

PLEASE DIRECT ALL COMMUNICATIONS RELATING TO THIS MATTER TO THE ATTENTION OF MAIL STOP L&R.

FORM PTOL-456 (Rev. 07-08)

The following is an example of an acceptable property rights statement. Statements of this type are, of course, only suitable for situations in which NO Agency funds or other considerations were involved in the making or conception of the invention. While this example is in the form of a declaration, a sworn document is equally acceptable.

I(We) ______________________________

citizens of ______________________________

residing at ______________________________

declare:

That I(we) made and conceived the invention described and claimed in patent application:

Serial Number ______________ filed in the United States of America on ______________

titled ______________________________

(check and complete either I or II below)

☐ I. *(For Inventors Employed by an Organization)* That I(We) made and conceived this invention while employed by ______________________.
That the invention is related to the work I am (we are) employed to perform and was made within the scope of my (our) employment duties; That the invention was made during working hours and with the use of facilities, equipment, materials, funds, information and services of ______________________.
Other relevant facts are ______________________
______________________.
That to the best of my (our) knowledge and belief (and/or) based upon information provided by
____
of ______________________.

--OR--

☐ II. *(For Self-Employed Inventors)* That I (we) made and conceived this invention on my (our) own time using only my (our) own facilities, equipment, materials, funds, information and services. Other relevant factors are ______________________
______________________.

(check III and/or IV below as appropriate)

That to the best of my (our) knowledge and belief:
☐ III. The invention was not made or conceived in the course of, or in connection with, or under the terms of any contract, subcontract or arrangement entered into with or for the benefit of the United States Atomic Energy Commission or its successors: Energy Research and Development Administration or the Department of Energy.

--AND/OR--

☐ IV. The invention was not made (conceived or first actually reduced to practice) under nor is there any relationship of the invention to the performance of any work under any contract of the National Aeronautics and Space Administration.

The undersigned inventors(s) declare further that all statements made herein of his or her (their) own knowledge are true and that all statements made on information and belief are believed to be true and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Inventor's Signature: ______________________________

Post Office Address: ______________________________

Date: ______________________________

Inventor's Signature: ______________________________

Post Office Address: ______________________________

Date: ______________________________

PATENT APPLICATION FEE DETERMINATION RECORD
Substitute for Form PTO-875

Application or Docket Number
14/146,202

APPLICATION AS FILED - PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
			TOTAL	730		TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

AMENDMENT A

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/146,202	01/02/2014	3646	730		20	3

CONFIRMATION NO. 7721

23497
JED MARGOLIN
1981 EMPIRE ROAD
RENO, NV 89521-7430

FILING RECEIPT

OC000000066114682

Date Mailed: 01/17/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Jed Margolin, VC Highlands, NV;

Applicant(s)

Jed Margolin, VC Highlands, NV;

Power of Attorney: The patent practitioners associated with Customer Number 23497

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/887,338 10/05/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

ADS-B Radar

Preliminary Class

342

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/AIA/15 (03-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	
First Named Inventor	Jed Margolin
Title	ADS-B Radar
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

1. [✔] **Fee Transmittal Form** (PTO/SB/17 or equivalent)
2. [✔] **Applicant asserts small entity status.** See 37 CFR 1.27
3. [ ] **Applicant certifies micro entity status.** See 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
4. [✔] **Specification** [*Total Pages* 22] Both the claims and abstract must start on a new page. *(See MPEP § 608.01(a) for information on the preferred arrangement)*
5. [✔] **Drawing(s)** (35 U.S.C. 113) [*Total Sheets* 4]
6. **Inventor's Oath or Declaration** [*Total Pages* 1] *(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))*
   - a. [✔] Newly executed (original or copy)
   - b. [ ] A copy from a prior application (37 CFR 1.63(d))
7. [✔] **Application Data Sheet** ** See note below.* See 37 CFR 1.76 (PTO/AIA/14 or equivalent)
8. **CD-ROM or CD-R** in duplicate, large table, or Computer Program (*Appendix*)
   - [ ] Landscape Table on CD
9. **Nucleotide and/or Amino Acid Sequence Submission** (*if applicable, items a. – c. are required*)
   - a. [ ] Computer Readable Form (CRF)
   - b. [ ] Specification Sequence Listing on:
     - i. [ ] CD-ROM or CD-R (2 copies); or
     - ii. [ ] Paper
   - c. [ ] Statements verifying identity of above copies

ACCOMPANYING APPLICATION PAPERS

10. [ ] **Assignment Papers** (cover sheet & document(s)) Name of Assignee ____________
11. [ ] **37 CFR 3.73(c) Statement** (*when there is an assignee*) [ ] **Power of Attorney**
12. [ ] **English Translation Document** (*if applicable*)
13. [✔] **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    - [✔] Copies of citations attached
14. [ ] **Preliminary Amendment**
15. [ ] **Return Receipt Postcard** (*MPEP § 503*) (*Should be specifically itemized*)
16. [ ] **Certified Copy of Priority Document(s)** (*if foreign priority is claimed*)
17. [ ] **Nonpublication Request** Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
18. [ ] **Other:** ____________

***Note**: (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must** be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS

[✔] The address associated with Customer Number: 23497 **OR** [ ] Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Jed Margolin/	Date	01/02/2014
Name (Print/Type)	Jed Margolin	Registration No. (Attorney/Agent)	

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	ADS-B Radar

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number ____________________

filed on ____________________.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Jed Margolin   Date (Optional) : 01/02/2014

Signature: Jed Margolin

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

PTO/SB/17 (03-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Examiner Name	
Art Unit	
Practitioner Docket No.	

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

TOTAL AMOUNT OF PAYMENT ($) 730

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ____________

☐ Deposit Account Deposit Account Number: ____________ Deposit Account Name: ____________

For the above-identified deposit account, the Director is hereby authorized to (check all that apply):

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayment of fee(s)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES (U = undiscounted fee; S = small entity fee; M = micro entity fee)

	FILING FEES			SEARCH FEES			EXAMINATION FEES			
Application Type	**U ($)**	**S ($)**	**M ($)**	**U ($)**	**S ($)**	**M ($)**	**U ($)**	**S ($)**	**M ($)**	**Fees Paid ($)**
Utility	280	140*	70	600	300	150	720	360	180	730
Design	180	90	45	120	60	30	460	230	115	
Plant	180	90	45	380	190	95	580	290	145	
Reissue	280	140	70	600	300	150	2,160	1,080	540	
Provisional	260	130	65	0	0	0	0	0	0	

* The $140 small entity status filing fee for a utility application is further reduced to $70 for a small entity status applicant who files the application via EFS-Web.

2. EXCESS CLAIM FEES

Fee Description	**Undiscounted Fee ($)**	**Small Entity Fee ($)**	**Micro Entity Fee ($)**
Each claim over 20 (including Reissues)	80	40	20
Each independent claim over 3 (including Reissues)	420	210	105
Multiple dependent claims	780	390	195

Total Claims 20 -20 or HP = **Extra Claims** 0 x **Fee ($)** ____ = **Fee Paid ($)** 0

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims 3 -3 or HP = **Extra Claims** 0 x **Fee ($)** ____ = **Fee Paid ($)** 0

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims
Fee ($) ____ **Fee Paid ($)** 0

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $400 ($200 for small entity) ($100 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets 22 - 100 = **Extra Sheets** 0 / 50 = **Number of each additional 50 or fraction thereof** 0 (round **up** to a whole number) x **Fee ($)** ____ = **Fee Paid ($)** 0

4. OTHER FEE(S) **Fees Paid ($)**

Non-English specification, $130 fee (no small or micro entity discount) 0

Non-electronic filing fee under 37 CFR 1.16(t) for a utility application, $400 fee ($200 small or micro entity) 0

Other (e.g., late filing surcharge): ____________ 0

SUBMITTED BY

Signature	/Jed Margolin/	Registration No. (Attorney/Agent)	Telephone 775-847-7845
Name (Print/Type)	Jed Margolin		Date 01/02/2014

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US- 2013/0176163	07-11-2013	Margolin	
	4	US- 5,153,836	10-06-1992	Fraughton, et al.	Abstract
	6	US- 7,414,567	08-19-2008	Zhang, et al.	Cols 3, 6, 7, 8
	8	US- 2011/0140950	09-16-2011	Anderson	Abstract
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number[4] -Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
	7	EP 2136222 A1	12-23-2009	Persson, et al.	Page 3	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Jed Margolin
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	2	14 CFR § 91.113(b) Right-of-way rules: Except water operations.	
	3	14 CFR § 91.115(a) Right-of-way rules: Water operations.	
	5	Gulf of Mexico Helo Ops Ready for ADS-B, Aviation Week & Space Technology, FRANCIS FIORINO, 02/26/2007, page 56.	
	9	Sensing Requirements for Unmanned Air Vehicles, AFRL's Air Vehicles Directorate, Control Sciences Division, Systems Development Branch, Wright-Patterson AFB OH, June 2004, http://www.afrlhorizons.com/Briefs/Jun04/VA0306.html .	
	10	Presentation entitled, Developing Sense & Avoid Requirements for Meeting an Equivalent Level of Safety (6MB | ppt), given by RUSS WOLFE, Technology IPT Lead, Access 5 Project at UVS Tech 2006. 18 January 2006.	
	11	Presentation: Integration into the National Airspace System (NAS) given by JOHN TIMMERMAN of the FAA's Air Traffic Organization (July 12, 2005)	
	12	Zone Ready for Drone, April 7, 2006, on the web site for the FAA's Air Traffic Organization Employees, http://www.ato.faa.gov/DesktopDefault.aspx?tabindex=4&tabid=17&itemid=937&mid=103	
	13	Quadrennial Roles and Missions Review Report, Department of Defense, January 2009, Page 29 (PDF page 37) www.defenselink.mil/news/Jan2009/QRMFinalReport_v26Jan.pdf	
	14	Automatic Dependent Surveillance Broadcast (ADS-B) Surveillance Development for Air Traffic Management, PDF Page 5. www.airbus.com/fileadmin/media_gallery/files/brochures_publications/FAST47_5.adsb.pdf	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	**Jed Margolin**
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	15	Exploiting the Automatic Dependent Surveillance Broadcast System Via False Target Injection; Thesis by DOMENIC MAGAZU III, CAPTAIN, USAF; AFIT/GCO/ENG/12-07; Department of the Air Force, Air University; Air Force Institute of Technology; March 2012. PDF Pages 49-54. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA561697	
	16	Security of ADS-B: State of the Art and Beyond MARTIN STROHMEIER (University of Oxford, United Kingdom), VINCENT LENDERS (armasuisse, Switzerland), IVAN MARTINOVIC (University of Oxford, United Kingdom); 7/13/2013 http://arxiv-web3.library.cornell.edu/pdf/1307.3664	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

UNITED STATES PATENT APPLICATION FOR
FOR

ADS-B RADAR

INVENTOR: JED MARGOLIN

ADS-B RADAR

CROSS REFERENCES TO RELATED APPLICATIONS

[001] This application claims the benefit of U.S. Provisional Application No. 61/887,338 filed on October 5, 2013. The present invention is an improvement on U.S. Patent Application 13/594,815 (Publication 2013/0176163) **System for sensing aircraft and other objects** by the present inventor and is hereby incorporated by reference herein. [*IDS Cite 1*]

BACKGROUND OF THE INVENTION - Field of Invention

[002] This invention relates to the field of sensing aircraft and other objects and is part of the See and Avoid (SAA) function for manned aircraft and the Detect, Sense and Avoid (DSA) function for remotely piloted vehicles (RPVs) and unmanned aerial vehicles (UAVs). RPV is an older term for UAV. Drone is another older term for UAV. "UCAV" shall mean "Unmanned Combat Aerial Vehicle." UCAV is also sometimes defined as an "Uninhabited Combat Aerial Vehicle." UCAV is a UAV that is intended for use in combat. UAS means "Unmanned Aerial System." UCAS means "Unmanned Combat Air System." The characteristics all these vehicles have in common is that there is no human pilot onboard, and although they may be operated autonomously they can also be controlled by a remotely located operator or pilot. The term UAV shall be used as a generic term for such vehicles. Detect, Sense, and Avoid (DSA) is also commonly called Sense and Avoid (SAA) since "Detect" and "Sense" mostly mean the same thing. This invention is directed to the "See" in "See and Avoid" and the "Sense" in "Sense and

Avoid." Automatic Dependent Surveillance-Broadcast (ADS-B) is the system by which an aircraft periodically transmits a message comprising its identification, location, altitude, and heading. The term "datastream" means the stream of data comprising the ADS-B message. The term "bitstream" means the same as "datastream."

BACKGROUND OF THE INVENTION – Prior Art

[003] In an aircraft with the pilot onboard, Sense and Avoid is called See and Avoid. FAA Regulations do not give much guidance for seeing other aircraft.

Right-of-way rules: Except water operations 14 CFR § 91.113(b) [*IDS Cite 2*]:

> (b) General. When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft. When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and may not pass over, under, or ahead of it unless well clear.

Right-of-way rules: Water operations 14 CFR § 91.115(a) [*IDS Cite 3*]

> (a) *General.* Each person operating an aircraft on the water shall, insofar as possible, keep clear of all vessels and avoid impeding their navigation, and shall give way to any vessel or other aircraft that is given the right-of-way by any rule of this section.

When operating under Visual Flight Rules the idea is to look out small windows providing a limited field of view and hope you see any nearby aircraft in time to avoid a collision. This is made more difficult because of the wide range of aircraft sizes and speeds. (Is it a large aircraft far away or a small aircraft much closer?) This is even more difficult under instrument flight rules where there may be no visibility.

[004] UAVs have special problems sensing other aircraft.

1. If the UAV is flown manually by a remote pilot looking at the video produced by a camera mounted in the nose of the aircraft the field of view will be too limited to see other aircraft other than those directly ahead.

2. If the UAV is flown autonomously there is no human pilot. If the flight is supervised by a human operator the problem remains that the field of view from a camera mounted in the nose of the aircraft will be too limited.

[005] A system by which an aircraft periodically transmits its identification, location, altitude, and heading is taught by U.S. Patent 5,153,836 **Universal dynamic navigation, surveillance, emergency location, and collision avoidance system and method** issued October 10, 1992 to Fraughton et al. [*IDS Cite 4*] and was materially adopted by the FAA as Automatic Dependent Surveillance-Broadcast (ADS-B). According to the article **Gulf of Mexico Helo Ops Ready for ADS-B** in Aviation Week & Space Technology (02/26/2007, page 56) [*IDS Cite 5*]:

> By the end of 2010, FAA expects to have the ADS-B system tested and operationally acceptable for the NAS, with Houston Center providing services in the Gulf region. By 2013, all of the U.S. is scheduled to be covered with ground infrastructure.

[006] The ADS-B system is used as a radar in U.S. Patent 7,414,567 **ADS-B radar system** issued August 19, 2008 to Zhang et al. [*IDS Cite 6*] Zhang modifies the standard ADS-B equipment by providing for random phase modulation that is added to a standard ADS-B waveform utilizing it as a primary radar signal. Phase coherent radio-frequency electronics are used for modulations and de-modulations and the phase modulator can be inserted bit by bit at a 180 degree phase shift per bit change. (See Column 3, lines 49 – 64)

One of Zhan's reasons for introducing random phase modulation is to raise the transmit spectrum sidelobes. (See Column 8, lines 23-27).

The reason why raising the transmit spectrum sidelobes is desirable appears to be because (1) raising the peaks in the transmit spectrum will increase the peaks in the spectrum of a reflected target signal and (2) the peaks in the spectrum of the reflected signal are used to compute the angles-of-arrival of the reflected target signal, i.e. the target. (See Column 7, lines 10-26)

Note that determining the angles-of-arrival of a signal cannot be done with a single omnidirectional antenna. It requires more than one antenna. Indeed, Zahn uses two antenna arrays, i.e two arrays of antennas. See Column 6, lines 39-45:

> Referring again to FIG. 1, antenna system 50 includes a plurality of antennas, which, in the embodiment shown, include a top circular array antenna 51, and a bottom circular array antenna 52. The arrays include individual elements 53 (FIG. 4). Circular array antennas 51 and 52 may be of a 4- or 8-element type as is common for TCAS systems or a 16-element type antenna.

Another reason for introducing random phase modulation is for identifying the reflected signal. See Column 6, lines 26 – 36:

> The phase shift is inserted pulse-by-pulse, and the pulse-position modulation with phase shifting is synthesized digitally at the I/Q baseband and up-converted to 1090 MHz carrier frequency. In the embodiment shown, a 180.degree. phase shift is added pulse-by-pulse in a random manner. In addition, the random phase shift code is put in memory during each message transmission. When reflected pulses are received, the system will try to match the amplitude and phase changes from pulse to pulse in a pulse-compression or matched filtering process, as discussed below in further detail.

There is a weakness in Zahn's system when the target is an Adversary. The Adversary can receive Zahn's signal, see that the phase of the bits is being changed, and know that Zahn is using his ADS-B Radar. The Adversary will have to assume he has been detected and has lost the element of surprise. As a result, Zahn has also lost an element of surprise because there is value in detecting an Adversary who does not know he has been detected. The invention of the current inventor teaches such a system.

[007] In European Patent Application EP2136222 **Validity check of vehicle position information** published 12/23/2009 (Persson, et al.) [*IDS Cite 7*] ADS-B is not used as a radar. Instead, Persson assumes that the target is broadcasting ADS-B signals. The direction to the target is determined using a directional antenna. The range to the target is determined when the target is sending a proper time-synchronized ADS-B signal. If the target is not broadcasting a valid ADS-B signal then radar must be used. See page 3, paragraphs 19, 20, and 21.

[008] U. S. Patent Application Publication Number 20110140950 **Validity check of vehicle position information transmitted over a time-synchronized data link** published June 16, 2011 [*IDS Cite 8*] contains the same disclosure as the above European Patent Application EP2136222. The title makes it clear that the invention requires a time-synchronized data link. Note that the U.S. Patent Application Publication lists only Svante Anderson as the inventor. Svante Anderson is listed as a co-inventor on the European Patent Application.

[009] Where ADS-B is relied upon to prevent mid-air collisions, an aircraft that does not have the equipment installed (or ADS-B is broken or has been deliberately turned off) is a hazard to itself and other aircraft in the vicinity.

BACKGROUND OF THE INVENTION – Current Practice in Flying UAVs

[010] The current practice in flying UAVs in civilian airspace is typified by the report **Sensing Requirements for Unmanned Air Vehicles** by AFRL's Air Vehicles Directorate, Control Sciences Division, Systems Development Branch, Wright-Patterson AFB OH, June 2004, which relies on computer-intelligence to use sensors to sense and avoid other aircraft. [*IDS Cite 9*]

[011] According to the presentation entitled **Developing Sense & Avoid Requirements for Meeting an Equivalent Level of Safety** given by Russ Wolfe, Technology IPT Lead, Access 5 Project at UVS Tech 2006 this had not changed as of January 18, 2006. [*IDS Cite 10*] Access 5 was a national project sponsored by NASA and Industry with participation by the FAA and DOD to introduce high altitude long endurance (HALE) remotely operated aircraft (ROA) to routine flights in the National Airspace System (NAS). Access 5 started in May 2004 but when NASA withdrew its support (and funding) the Industry members decided not to spend their own money and Access 5 was dissolved at the end of 2005.

[012] The presentation **Integration into the National Airspace System (NAS)** given by John Timmerman of the FAA's Air Traffic Organization (July 12, 2005) essentially says that under current UAS Operations in the NAS UAVs should not harm other aircraft or the public. (Page 3: "***While ensuring 'no harm' to other NAS customers and public***") [*IDS Cite 11*]

[013] The article **Zone Ready for Drone**, April 7, 2006, on the web site for the FAA's Air Traffic Organization Employees states that [*IDS Cite 12*],

> Since March 29, a temporary flight restriction … has limited access to the airspace along almost 350 miles of the border, expanding an earlier TFR near Nogales. The restriction is in effect nightly from 6 p.m. to 9 a.m., although that time can be expanded by issuance of a Notice to Airmen. Aircraft wishing to fly in the TFR when it is active must receive authorization from air traffic control prior to entry. Once in, pilots are required to maintain two-way communication with ATC and transmit a discrete transponder code.

The reason for the TFR is to enable Predator UAVs to patrol the border. The article quotes Stephen Glowacki, a Systems Safety and Procedures specialist with the FAA's Air Traffic Organization as saying:

> This is an extreme situation that has been presented to us," states Stephen Glowacki, a Systems Safety and Procedures specialist with the FAA's Air Traffic Organization, stressing the nation's security. "We have been working with U.S. Customs and Border Protection to try and answer this situation."
>
> Inserting UASs into the National Airspace System is not a simple feat. According to Glowacki, the technology and certification that will permit unmanned aircraft to "see and avoid" other air traffic is still eight to ten years away. In the mean time, a carefully controlled environment is needed.

[014] From **Quadrennial Roles and Missions Review Report**, Department of Defense, January 2009, page 29 [*IDS Cite 13*]:

> <u>U.S. Joint Forces Command Joint UAS Center of Excellence has identified three areas necessary to ensure access to applicable classes of the National Airspace System:</u> (1) Airworthiness Certification; (2) establishment of standardized basic UAS qualifications consistent with Federal Aviation Administration guidelines for each class of airspace; and <u>(3) development of sense and avoid technology</u>. Working with the Services, the U.S. Joint Forces Command Joint UAS Center of Excellence will ensure these areas are addressed during UAS development.

(Emphasis added.)

OBJECTIVES

[015] Therefore, an objective of the present invention is to improve the ADS-B system by using ADS-B as a radar system for sensing aircraft and other objects so that aircraft equipped with ADS-B can detect target aircraft not equipped with ADS-B, or the target aircraft's ADS-B is broken or has been deliberately turned off, or a false ADS-B signal is being emitted.

SUMMARY OF THE INVENTION

[016] Automatic Dependent Surveillance-Broadcast (ADS-B) can be improved by using the signal transmitted from an ADS-B unit as a radar transmitter with the ADS-B receiver used to receive reflections. In a first preferred embodiment a standard omni-directional antenna is used to receive the reflections of the ADS-B signal. The time delays between the transmitted signal and the reflections are used to determine the range of other aircraft and match the range and number of targets to the ADS-B signals normally received. Doppler analysis can be used to confirm the speeds of the targets. The integrity of a reflected signal is determined by comparing the datastream of the reflected signal with the datastream of the transmitted signal. If more than one such reflected signal is received by the ADS-B receiver then the closest reflected signal is a true target and the other reflected signals are either from additional aircraft farther away or are being caused by an unfriendly target transmitting a delayed version of the reflected signal. In order for an adversary target aircraft to produce a false signal corresponding to a range that is closer than its true position it would have to exactly predict the datastreams being transmitted. The ADS-B messages transmitted in the datastream contain items such as

- Aircraft identification
- Absolute bearing/2D distance
- Heading/Tracking
- Wake vortex category
- Relative altitude/Absolute altitude
- Ground speed
- Vertical velocity

See **Automatic Dependent Surveillance Broadcast (ADS-B) Surveillance Development for Air Traffic Management** [*IDS Cite 14, PDF page 5*].

A more detailed description can be found in **Exploiting the Automatic Dependent Surveillance Broadcast System Via False Target Injection**; Thesis by Domenic Magazu III, Captain, USAF [*IDS Cite 15, PDF pages 49-54*].

It is unlikely that all of these parameters can be predicted exactly. However, if an aircraft using ADS-B as a radar has reason to believe it is receiving false reflected signals it can randomly vary its transmission times.

By using the ADS-B datastream to determine the integrity of reflected signals, there is no difference in the transmitted signal between the ADS-B radar system and an ADS-B system that does not use the transmitted signal for radar. An adversary target will have no way of knowing if he has been detected. The user of the ADS-B radar can use the tactic of acting as though he has not detected the adversary target. At some point the tactic can change, such as by shooting down the adversary target.

[017] In a second preferred embodiment a directional receive antenna is used to give both the range and bearing to aircraft and other objects in the vicinity of the user's aircraft even when other aircraft are not equipped with ADS-B.

The use of a directional antenna requires the ability to aim the antenna. This can be done by physically aiming the antennas (such as when the antenna uses a parabolic dish reflector) or by using an active electronically scanned array. Because each area must be separately scanned the time to detect and locate targets is increased according to the directionality of the antenna. The use of a directional antenna reduces the radio frequency noise received that is produced by the Sun, except when the antenna is pointed at the Sun. (The level of the sun's contribution depends on the solar flux.) It also reduces the noise received that is produced by the Earth (about 290K.), except when the antenna is pointed at the Earth.

Again, by using the ADS-B datastream to determine the integrity of reflected signals, there is no difference in the transmitted signal between the ADS-B radar system and an ADS-B system that does not use the transmitted signal for radar. An adversary target will have no way of knowing if he has been detected. The user of the ADS-B radar can use the tactic of acting as though he has not detected the adversary target. At some point the tactic can change, such as by shooting down the adversary target.

[018] In a third preferred embodiment a separate receiver is used with the directional antenna to make it possible to receive and process radar returns without the risk of missing ADS-B messages from other aircraft.

[019] There is a possible issue when the target is close enough that the ADS-B message is still being sent when the beginning of the reflected signal has started coming back. The ADS-B message using the 1090 ES Data Link is 120 us long. See Figure 4. At the speed of light (186,300 miles/sec) this corresponds to approximately 22.4 miles. Since this includes the trip to the target and back again it means a range to the target of approximately 11.2 miles. However, because of causality we know that the end of the reflected ADS-B message must happen after the end of the transmitted ADS-B message. The transmitted signal and the received reflection signal will overlap but cannot overlap completely. The question is how much of the non-overlapped reflection signal do we need in order to verify with good probability that we are receiving our own reflected ADS-B message and not the ADS-B message from another aircraft. Again referring to Figure 4, the ADS-B message ends with 24 bits of CRC (cyclic redundancy check) which is an error detection and correction code that allows up to 5 bits in the ADS-B message to be corrected. The probability that an ADS-B message from another aircraft will have the same CRC as the User's ADS-B message is very small. The 24-bit CRC code is 24 us long, which corresponds to a range to the target of approximately 2.2 miles.

The use of a directional antenna in the second and third embodiments makes it even less likely that the signal being received is from another aircraft so the number of bits required to give a good probability that the signal being received is a valid reflection can be decreased, thereby decreasing the minimum range of detection.

Thus, the datastream comparator can be configured so that it does not need to compare the complete ADS-B message in order to verify with good probability that the signal being received is a reflection and not another aircraft's ADS-B signal.

BRIEF DESCRIPTION OF THE DRAWINGS

[020] The invention may best be understood by referring to the following description and accompanying drawings which illustrate the invention. In the drawings:

[021] FIG. 1 is a general illustration showing an ADS-B system used as a radar, using omni-directional antennas.

[022] FIG. 2 is a general illustration showing an ADS-B system used as a radar, using a separate directional receiving antenna.

[023] FIG. 3 is a general illustration showing an ADS-B system used as a radar, using a separate directional receiving antenna and a separate receiver.

[024] FIG. 4 is a reproduction of Figure 2 from **Security of ADS-B: State of the Art and Beyond** by Strohmeier, Lenders, and Martinovic (*IDS cite 16*)

DETAILED DESCRIPTION

[025] In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it is understood that the invention may be practiced without these specific details. In other instances well-known circuits, structures, and techniques have not been shown in detail in order not to obscure the invention.

[026] Figure 1 is a general illustration showing an ADS-B system used as a radar, using omni-directional antennas. ADS-B Transmitter 103 periodically transmits a message containing the present aircraft's unique ID, GPS coordinates, and other data using Omni-Directional antenna 101. When ADS-B Transmitter 103 is not transmitting, ADS-B Receiver 104 is listening for messages transmitted by other aircraft containing their unique ID, GPS coordinates, and other data. An Antenna Multiplexer (Antenna Mux 102) is used to route the signals from Omni-Directional Antenna 101 to ADS-B Transmitter 103 and ADS-B Receiver 104. Omni-Directional Antenna 106 is used with GPS Receiver 107 to provide the GPS coordinates of the present aircraft. All of this is controlled by ADS-B Processor 105.

ADS-B operation is improved by using the signal produced by ADS-B Transmitter 103 as a radar with reflected signals received by ADS-B Receiver 104 under the control of ADS-B Processor 105 and Radar Processor 108.

Datastream Comparator 109 determines the integrity of a reflected signal by comparing the datastream of the reflected signal with the datastream of the transmitted signal.

If the number and range of targets reported by radar do not match the number and range of aircraft reported by ADS-B then there is an aircraft out there that does not have ADS-B, it is broken or has been disabled, or there is a false ADS-B signal present.

The results are displayed on Display 110.

Datastream Comparator 109 may be combined with Radar Processor 108. Radar Processor 108 may be combined with ADS-B Processor 105.

[027] In Figure 2, a separate directional antenna (Directional Antenna 201) is selected by Antenna Mux 205 to receive the reflected signals. The advantage of using a separate antenna for this function is that it is directional, as opposed to Omni-Directional Antenna 101. Directional Antenna 201 can also be used by ADS-B Transmitter 103 in order to strengthen radar returns from a specific target or to increase the range of the system in a specific direction.

Directional Antenna 201 is controlled by Antenna Controller 202 under the direction of Radar Processor 203 which also controls the radar function through ADS-B Processor 105. Directional Antenna 201 and Antenna Controller 202 may be a system that mechanically aims Directional Antenna 201 or the combination may be an electronically scanned array.

Datastream Comparator 109 determines the integrity of a reflected signal by comparing the datastream of the reflected signal with the datastream of the transmitted signal.

If the number, range, and bearing of targets reported by radar do not match the number, range, and bearing of aircraft reported by ADS-B then there is an aircraft out there that does not have ADS-B, it is broken or has been disabled, or there is a false ADS-B signal present.

The results are displayed on Display 204.

Datastream Comparator 109 may be combined with Radar Processor 203. Radar Processor 203 may be combined with ADS-B Processor 105.

[028] In Figure 3, as an alternative to sharing ADS-B Receiver 104, Directional Antenna 201 can be used with its own receiver. Antenna Mux 301 routes Directional Antenna 201 to Receiver 302 whose output goes to ADS-B Processor 303 to make it possible to receive and process radar returns without the risk of missing ADS-B messages from other aircraft.

The integrity of a reflected signal is determined by comparing the datastream of the reflected signal with the datastream of the transmitted signal.

If the number, range, and bearing of targets reported by radar do not match the number, range, and bearing of aircraft reported by ADS-B then there is an aircraft out there that does not have ADS-B, it is broken or has been disabled, or there is a false ADS-B signal present.

The results are displayed on Display 204.

Datastream Comparator 109 may be combined with Radar Processor 203. Radar Processor 203 may be combined with ADS-B Processor 303.

[029] While preferred embodiments of the present invention have been shown, it is to be expressly understood that modifications and changes may be made thereto.

CLAIMS

I claim:

1. A system for sensing aircraft and other objects comprising:

(a) an ADS-B transmitter;

(b) an ADS-B receiver;

(c) an ADS-B antenna;

(d) an ADS-B antenna multiplexer;

(e) an ADS-B processor;

(f) a radar processor;

(g) a datastream comparator;

(h) a display;

whereby

(i) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B multiplexer is configured to allow either said ADS-B transmitter or said ADS-B receiver to use said ADS-B antenna,

(j) said ADS-B processor and said radar processor are configured to work together,

(k) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through said ADS-B antenna multiplexer to said ADS-B antenna,

(l) said transmitted signal is reflected by a target producing a reflected signal,

(m) said reflected signal is received by said ADS-B antenna, and said ADS-B antenna multiplexer is configured to send said reflected signal to said ADS-B receiver,

(n) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target,

(o) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and

(p) said radar processor is configured to display said range on said display.

2. The system of claim 1 whereby

(a) if said range to said target does not match a possible position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item,

(b) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target,

(c) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target,

(d) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target and said radar processor is configured to note said discrepancy on said display as a second attention item, and

(e) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

3. The system of claim 1 wherein said datastream comparator is incorporated into said radar processor.

4. The system of claim 1 wherein said radar processor is incorporated into said ADS-B processor.

5. A system for sensing aircraft and other objects comprising:

(a) an ADS-B transmitter;

(b) an ADS-B receiver;

(c) a first ADS-B antenna;

(d) a second ADS-B antenna;

(e) an antenna controller;

(f) an ADS-B antenna multiplexer;

(g) an ADS-B processor;

(h) a radar processor;

(i) a datastream comparator;

(j) a display;

whereby

(k) said second ADS-B antenna is directional, and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna,

(l) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna,

(m) said ADS-B processor and said radar processor are configured to work together,

(n) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer,

(o) said transmitted signal is reflected by a target producing a reflected signal,

(p) said reflected signal is received by either or both said first ADS-B antenna and said second ADS-B antenna, and said ADS-B antenna multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said ADS-B receiver,

(q) said radar processor is configured to process said reflected signal from said ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target,

(r) said radar processor is configured to use the direction of said second ADS-B antenna to determine a bearing to said target,

(s) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and

(t) said radar processor is configured to display said range and said bearing on said display.

6. The system of claim 5 whereby

(a) if said range and said bearing to said target do not match the position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item,

(b) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target,

(c) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target,

(d) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target, and said radar processor is configured to note said discrepancy on said display as a second attention item, and

(e) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

7. The system of claim 5 wherein said datastream comparator is incorporated into said radar processor.

8. The system of claim 5 wherein said radar processor is incorporated into said ADS-B processor.

9. The system of claim 5 wherein said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna.

10. The system of claim 5 wherein said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array.

11. The system of claim 6 wherein said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna.

12. The system of claim 6 wherein said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array.

13. A system for sensing aircraft and other objects comprising:

(a) an ADS-B transmitter;

(b) a first ADS-B receiver;

(c) a first ADS-B antenna;

(d) a second ADS-B receiver;

(e) a second ADS-B antenna;

(f) an antenna controller;

(g) an ADS-B antenna multiplexer;

(h) an ADS-B processor;

(i) a radar processor;

(j) a datastream comparator;

(k) a display;

whereby

(l) said second ADS-B antenna is directional and said radar processor is configured to control said antenna controller which is configured to control the direction of said second ADS-B antenna,

(m) said ADS-B processor is configured to control said ADS-B antenna multiplexer, and said ADS-B antenna multiplexer is configured to allow said ADS-B transmitter to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said first ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna, and said ADS-B antenna multiplexer is also configured to allow said second ADS-B receiver to use either said first ADS-B antenna or said second ADS-B antenna,

(n) said ADS-B processor and said radar processor work together,

(o) said ADS-B processor is configured to periodically cause said ADS-B transmitter to emit a transmitted signal through either said first ADS-B antenna or said second ADS-B antenna through said ADS-B antenna multiplexer,

(p) said transmitted signal is reflected by a target producing a reflected signal,

(q) said reflected signal is received by either or both said first ADS-B antenna or said second ADS-B antenna, and said ADS-B multiplexer is configured to select either said first ADS-B antenna or said second ADS-B antenna and send said reflected signal to said second ADS-B receiver,

(r) said radar processor is configured to process said reflected signal from said second ADS-B receiver and said transmitted signal from said ADS-B transmitter to determine a range to said target,

(s) said radar processor is configured to use the direction of said second antenna to determine a bearing to said target,

(t) said datastream comparator is configured to compare the datastream of said transmitted signal and the datastream from said reflected signal, and

(u) said radar processor is configured to display said range and said bearing on said display.

14. The system of claim 13 whereby

(a) if said range and said bearing to said target do not match the position of said target as reported by ADS-B messages from said target said radar processor is configured to note this on said display as a first attention item,

(b) said radar processor is configured to use the change in the positions of said target as reported by said ADS-B messages received from said target to calculate a reported radial velocity of said target,

(c) said radar processor is configured to use the Doppler shift of said reflected signal to calculate a measured radial velocity of said target,

(d) a discrepancy between said reported radial velocity of said target and said measured radial velocity of said target indicates a system error comprising GPS spoofing, failure of the ADS-B system on said target, or deliberate misreporting by said target, and said radar processor is configured to note said discrepancy on said display as a second attention item, and

(e) a receipt of said ADS-B messages from said target that is not confirmed by a reflected signal indicates that a false ADS-B signal is being broadcast and said radar processor is configured to note said false ADS-B signal on said display as a third attention item.

15. The system of claim 13 wherein said datastream comparator is incorporated into said radar processor.

16. The system of claim 13 wherein said radar processor is incorporated into said ADS-B processor.

17. The system of claim 13 wherein said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna.

18. The system of claim 13 wherein said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array.

19. The system of claim 14 wherein said second ADS-B antenna and said antenna controller comprise a mechanically aimed antenna.

20. The system of claim 14 wherein said second ADS-B antenna and said antenna controller comprise an active electronically scanned antenna array.

ABSTRACT OF THE DISCLOSURE

The reliability and safety of Automatic Dependent Surveillance-Broadcast (ADS-B) are improved by using the signals transmitted from an ADS-B unit as a radar transmitter with a receiver used to receive reflections.

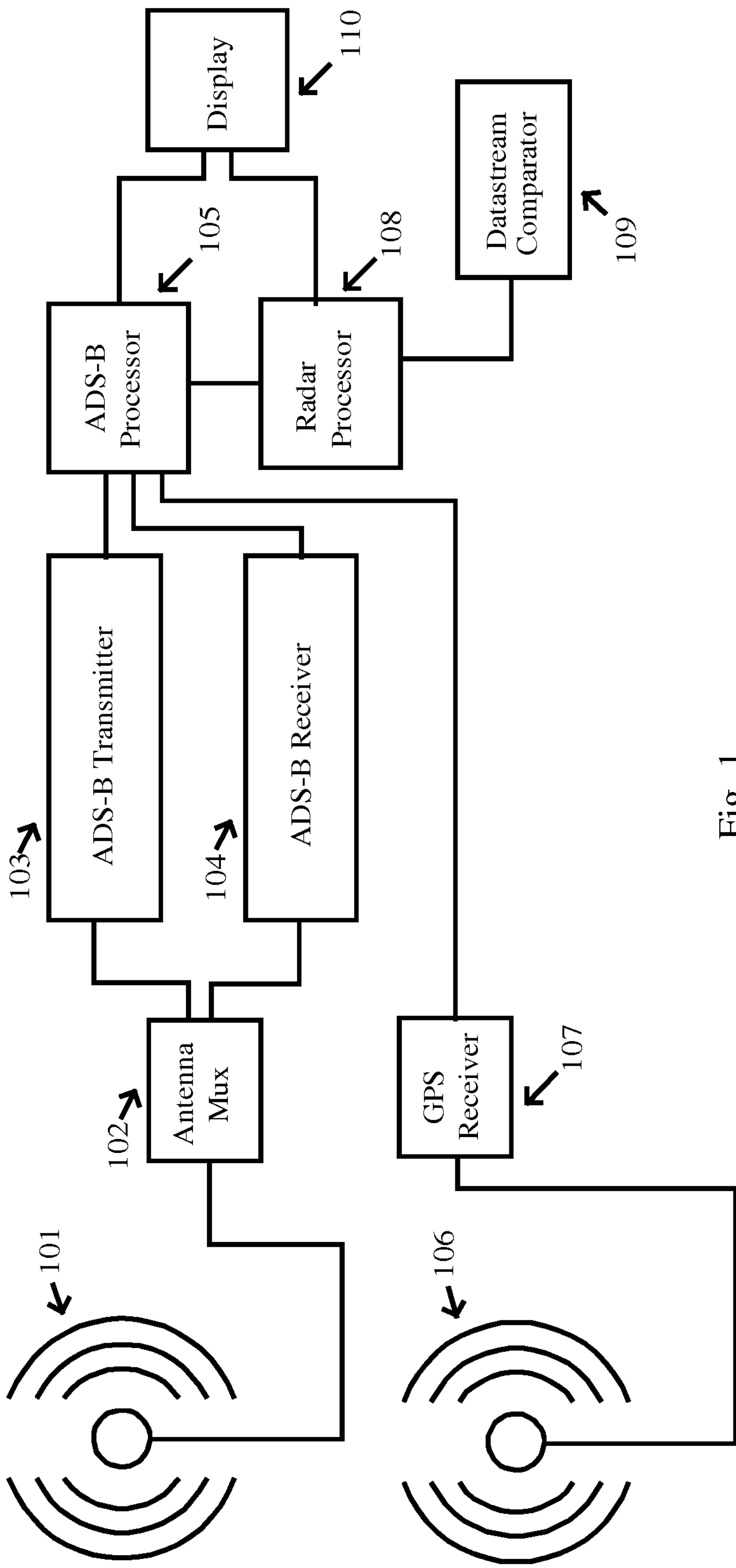
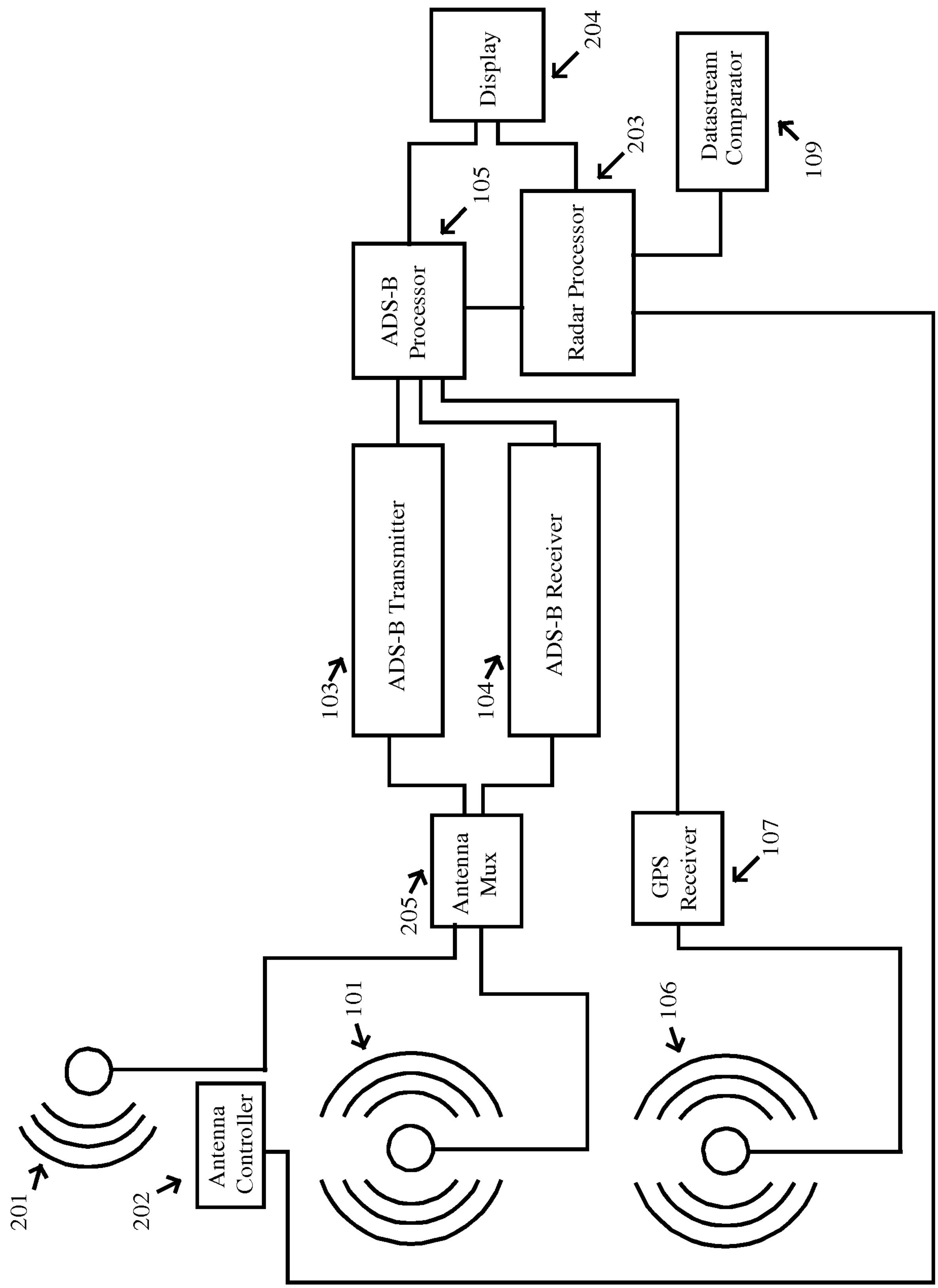

Display
110
ADS-B Processor
105
Radar Processor
108
Datastream Comparator
109
ADS-B Transmitter
103
ADS-B Receiver
104
Antenna Mux
102
GPS Receiver
107
101
106

Fig. 1



Display
204
Datastream Comparator
109
203
105
ADS-B Processor
Radar Processor
ADS-B Transmitter
103
ADS-B Receiver
104
Antenna Mux
205
GPS Receiver
107
101
106
201
202
Antenna Controller

Fig. 2

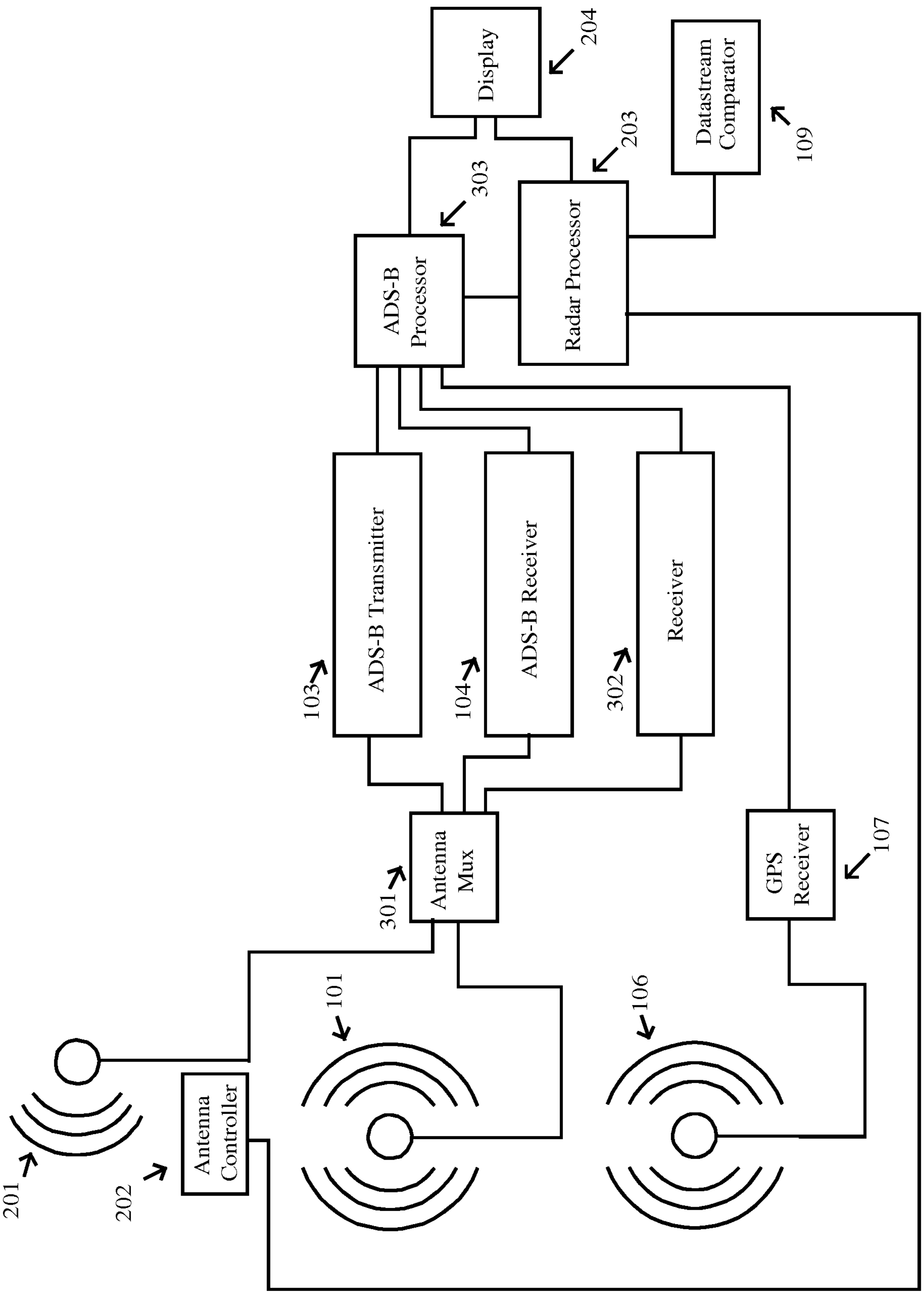

Display
204
Datastream Comparator
109
203
303
ADS-B Processor
Radar Processor
ADS-B Transmitter
103
ADS-B Receiver
104
Receiver
302
Antenna Mux
301
GPS Receiver
107
101
106
201
Antenna Controller
202

Fig. 3

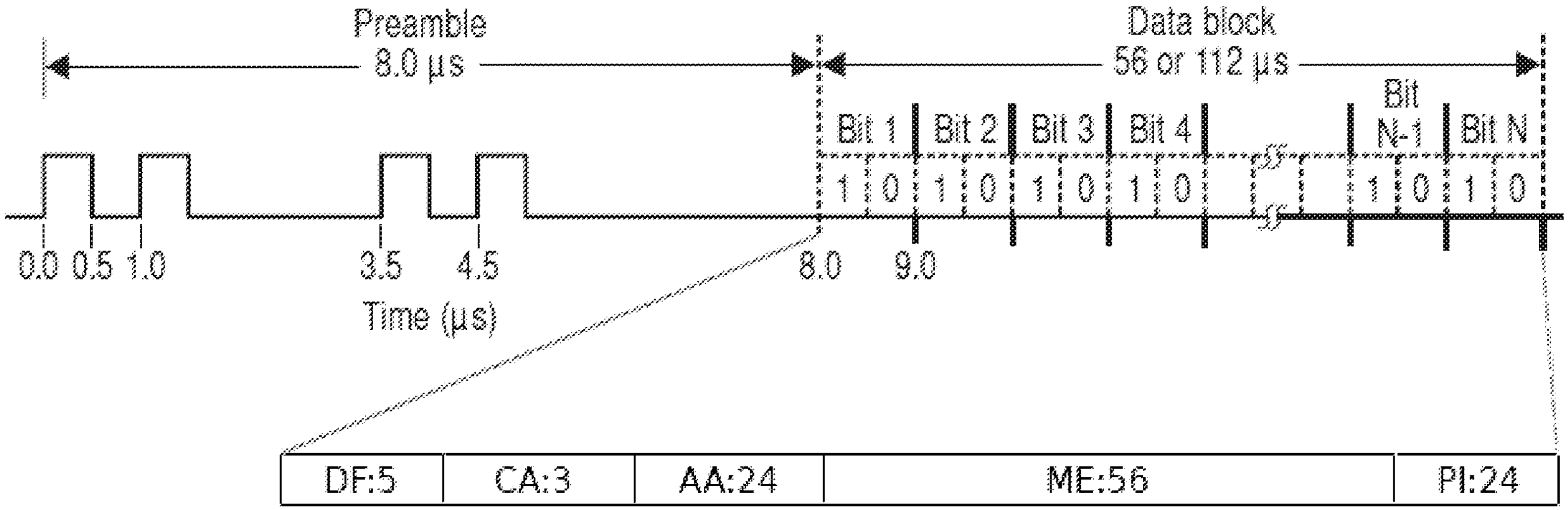


Figure 2. 1090 ES Data Link [1]

Fig. 4 (Prior Art)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 136 222 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
23.12.2009 Bulletin 2009/52

(51) Int Cl.:
G01S 13/76 *(2006.01)* *G08G 5/04* *(2006.01)*

(21) Application number: **08158503.6**

(22) Date of filing: **18.06.2008**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA MK RS

(71) Applicant: **SAAB AB**
581 88 Linköping (SE)

(72) Inventors:
- **Persson, Andreas**
  587 25 Linköping (SE)
- **Andersson, Svante**
  602 22 Norrköping (SE)

(74) Representative: **Herbjörnsen, Rut et al**
Albihns AB
P.O. Box 5581
114 85 Stockholm (SE)

(54) Validity check of vehicle position information

(57) The present invention provides a method for validating received positional data in vehicle surveillance applications wherein vehicles transmit positional data indicating their own position to surrounding vehicles, such as an ADS-B-based aircraft surveillance application. The method involves the steps of:
receiving, with a radio direction finding antenna arrangement of a receiving unit, a signal carrying positional data indicating an alleged position of a vehicle, transmitted from a radio source;
estimating the bearing from the receiving unit to said radio source utilizing said radio direction finding antenna arrangement and the received signal;
estimating the distance between the receiving unit and the radio source based on the time of flight for a signal travelling there between at known speed;
calculating an estimated position of the radio source based on the estimated bearing and the estimated distance, and
determining a deviation value indicating the deviation/coincidence between the alleged position of a vehicle according to the received positional data and the estimated position of the radio source.

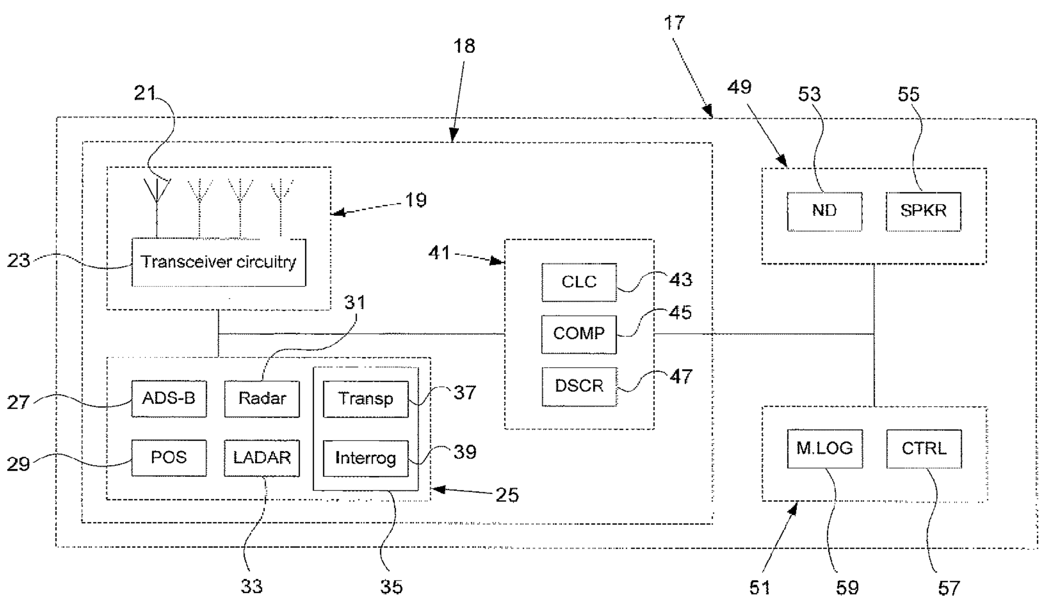


Fig. 5

Printed by Jouve, 75001 PARIS (FR)

Description

Technical Field

[0001] The present invention relates to the field of traffic surveillance, and more particularly to a method for validating positional data allegedly indicating the position of a vehicle.

Background Art

Traffic Surveillance and Traffic Management

[0002] Surveillance of air traffic is today managed by air traffic control (ATC) systems using primary and secondary radar. ATC systems currently under development use other or complementary techniques in the surveillance of air traffic. One such system is called automatic dependent surveillance-broadcast (ADS-B) which, on a long time scale, is expected to gradually replace current systems as a source for ATC information.
[0003] The basic idea of the ADS-B system is that all aircraft broadcast their own state vector, comprising position and status information, to all nearby aircraft and ground stations. Thus each aircraft has a complete picture of the surrounding traffic and the traffic close to a ground station can be monitored on ground.
[0004] Central to the ADS-B concept is the airborne data link (transponder) enabling the intended functionality. There are currently three different types of data links under consideration; Mode S ES, VDL Mode 4 and UAT.
[0005] Mode S ES is an extension of the conventional Mode S secondary surveillance radar system. VDL Mode 4 is a newly developed standard for a data link transponder compatible with ADS-B requirements. UAT is only considered for general aviation in the US.

Collision Avoidance and Separation Provision

[0006] Today, collision avoidance and separation provision is mechanized by air traffic controllers, pilots or the TCAS system. The basic feature in the TCAS system is the use of transponders and antennas. A very simplified explanation of the TCAS system is that it sends out a request from the transponder. If another aircraft is in the vicinity, an answer is sent back to the TCAS system which then knows the distance to the other aircraft (by measuring the time from the request to the received answer) and typically also in what direction the other aircraft is located (by using a directional antenna). The TCAS system then uses this information to issue warnings and suggested resolution manoeuvres if found necessary.
[0007] A drawback of today's TCAS systems is the uncertainties in the determined relative position (especially at large distances) due to the uncertainties in the directional antennas and the estimated distances to surrounding aircraft. These uncertainties may result in nuisance warnings from the system. The TCAS systems of today are therefore not considered to be suitable candidates for future collision avoidance and/or separation provision systems.
[0008] The ADS-B system and its possibility to automatically provide each aircraft with information relating to the surrounding traffic opens up for functionality such as automatic or semiautomatic separation provision and collision avoidance. These functions are particularly important in flight control of unmanned aerial vehicles (UAVs) but may also be important as a precautionary feature in piloted aircraft.
[0009] Considering the known shortcomings of TCAS, ADS-B seems a well suitable candidate for future systems for collision avoidance and separation provision using combinations of sensors such as, e.g., cameras, radar and ADS-B transponders. Aircraft-based aircraft surveillance systems for collision avoidance and separation provision are sometimes called Sense & Avoid systems.
[0010] Unfortunately, ADS-B systems of today suffer from a drawback. The position information received from surrounding air traffic has to be trusted to be correct. This is both a safety and security problem, safety in the sense that if the transmitting system emits an erroneous position it might cause a hazardous situation, and security in the sense that the system becomes prone to malicious use by emitting faked position reports.
[0011] For example, if an ADS-B message indicates an erroneous position of the aircraft from which it is transmitted, decisions made on the basis of that ADS-B message may have devastating consequences. An operator of an ATC system based on ADS-B data or a pilot/autopilot of an aircraft utilizing an ADS-B-based aircraft surveillance system, may be fooled to order/confirol an aircraft towards instead of away from the aircraft transmitting the erroneous ADS-B message.

Summary

[0012] it is an object of the present invention to provide a vehicle surveillance system that is less prone to errors and less sensitive to malicious use.

[0013] This object is achieved by a method for validating positional data in vehicle surveillance applications wherein vehicles transmit positional data indicating their own position to surrounding vehicles, such as an ADS-B-based aircraft surveillance application. The method involves the steps of:

receiving, with a radio direction finding antenna arrangement of a receiving unit, a signal carrying positional data indicating an alleged position of a vehicle, transmitted from a radio source;
estimating the bearing from the receiving unit to said radio source utilizing said radio direction finding antenna arrangement and the received signal;
estimating the distance between the receiving unit and the radio source based on the time of flight for a signal travelling there between at known speed;
calculating an estimated position of the radio source based on the estimated bearing and the estimated distance, and determining a deviation value indicating the deviation/coincidence between the alleged position of a vehicle according to the received positional data and the estimated position of the radio source.

[0014] By estimating the bearing and the distance to a radio source transmitting positional data relating to an alleged position of a vehicle, and by calculating an estimated position for said radio source based on the estimated bearing and distance, the above method provides for a way of determining whether the radio source really is located at the position given by the positional data that it transmits.

[0015] Since the method is used in a self-reporting vehicle surveillance system, meaning that each vehicle transmits positional data indicating its own position, a mismatch between the alleged position of a vehicle according to the received data and the estimated position of the radio source indicates that something is not right and that the received positional data cannot be indiscriminately relied upon.

[0016] The determined deviation value can hence be used as an indicator of the reliability of the received positional data.

[0017] The step of estimating the bearing from the receiving unit to the radio source is, according to one embodiment of the invention, performed by receiving the signal with a directional antenna connected to a transceiver circuitry which is adapted to determine the bearing to the radio source based on the output from the directional antenna.

[0018] The step of estimating the distance between the receiving unit and the radio source may be performed in different ways depending on e.g., the type of data link used for the transmission of the signal and the information carried by the signal.

[0019] When the signal carrying the positional data is transmitted over a time-synchronized data link, meaning that transmissions over that data link are initiated at points in time that are known by all users of the data link, the signal carrying the positional data can be used to estimate the distance between the radio source and the receiving unit. By determining the point in time at which the signal is received, the approximate time elapsed between transmission and reception of the signal can be determined by the receiving unit as the point in time at which transmission was initiated is known. This time corresponds to the time of flight for the signal and since the signal travels at known speed (the speed of light), the distance between the radio source and the receiving unit can be determined. An example of a time-synchronized data link to which this method is applicable is the STDMA data link used in ADS-B systems conforming to the VDL Mode 4 format.

[0020] If the signal carrying the positional data also carries information about its own transmission time, the distance between the radio source and the receiving unit can also be estimated using this signal alone. The receiving unit can use the transmission time information contained in the signal and the reception time of the signal to determine the signal time of flight, and hence the distance, between the radio source and the receiving unit. This method is applicable to, e.g., ADS-B systems based on UAT.

[0021] If it is not possible to estimate the distance to the radio source based on the signal carrying the positional data, the receiving unit can be equipped with additional distance measuring equipment, such as primary radar equipment, laser detection and ranging equipment, and/or secondary surveillance radar equipment. When a signal carrying positional data relating to an alleged position of a vehicle is received by the receiving unit, the additional distance equipment can be used to estimate the distance to the radio source from which the signal originated. Today, this method must be used in, e.g., ADS-B systems based on Mode S ES.

[0022] According to an aspect of the invention, the method is used to discard received positional data that is found unreliable. When the method is used in, e.g., an aircraft-based aircraft surveillance system or a ground-based ATC system, the suggested method ensures that navigational decisions are made based on correct information of surrounding traffic, which considerably increases the safety of such systems.

[0023] The object is also achieved by a vehicle surveillance system for validating positional data in vehicle surveillance applications wherein vehicles transmit positional data indicating their own position to surrounding vehicles, such as an ADS-B-based aircraft surveillance application. The vehicle surveillance system comprises:

bearing-estimation means adapted to receive a signal carrying positional data indicating an alleged position of a vehicle, transmitted from a radio source, said bearing-estimation means further being adapted to estimate the bearing to said radio source using said received signal;
distance-estimation means adapted to estimate the distance to the radio source based on the time of flight, TOF, for a signal received there from, which signal travels at known speed;
calculating means adapted to calculate an estimated position of the radio source based on the estimated bearing and the estimated distance, and
comparing means adapted to determine a deviation value indicating the deviation/coincidence between the alleged position of a vehicle according to the received positional data and the estimated position of the radio source.

[0024] The vehicle surveillance system according to the invention may be included in any type of receiving unit, such as a vehicle or stationary unit, for validating positional data that is transmitted from surrounding radio sources. For example, it can be included in aircraft or ships for use in separation provision and/or collision avoidance applications, or it can be included in ground-based ATC or VTS stations for monitoring air traffic or maritime traffic, respectively.

[0025] Besides the increased flight safety offered by the vehicle surveillance system according to the invention, aircraft comprising such systems and using them for automatic aircraft separation provision will lower their fuel consumption since their pre-programmed flight plan will not be altered due to erroneous ADS-B messages reported by surrounding radio sources.

Brief description of the drawings

[0026] The present invention will become more fully understood from the detailed description provided hereinafter and the accompanying drawings, which are not necessarily to scale, and are given by way of illustration only. In the different drawings, same reference numerals correspond to the same element.

Figs. 1A and 1B illustrate a typical operational environment of the invention.

Figs. 2A and 2B illustrate schematically the concept of the present invention.

Fig. 3 is a flowchart illustrating a method for validating received positional data according to the invention.

Figs. 4A and 4B illustrate a principle for determining the time of flight for an ADS-B VDL Mode 4 message between a radio source and a receiving unit.

Fig. 5 illustrates an embodiment of a vehicle surveillance system according to the invention.

Acronyms and abbreviations

[0027]

Acronym	Definition
ADS-B	Automatic Dependent Surveillance-Broadcast
AIS	Automatic Identification System
ATC	Air Traffic Control
LADAR	Laser Detection and Ranging
Mode S ES	Mode-S Extended Squitter
MSO	Message Start Opportunities
STDMA	Self-organizing Time Division Multiple Access
TCAS	Traffic alert and Collision Avoidance System
TDMA	Time Division Multiple Access
TOF	Time of Flight
UAT	Universal Access Transceiver
UAV	Unmanned Aerial Vehicle
UTC	Coordinated Universal Time
VDL	VHF Data Link
VTS	Vessel Traffic Service

Detailed description

[0028] An aircraft or an air traffic control (ATC) ground station utilizing an ADS-B-based vehicle surveillance system is completely dependent on that the information in ADS-B messages received from surrounding aircraft is correct. Specifically, positional data contained in the ADS-B messages from emitting aircraft have to be trusted to be correct. The flaw is that as long as the received messages conform to the correct format they will be interpreted as ADS-B messages and, as such, relied upon by the vehicle surveillance systems. This fact makes ADS-B-based vehicle surveillance systems extremely vulnerable to ADS-B transponder malfunction and malicious use by transmission of faked ADS-B data.

[0029] All three data link technologies (Mode S ES, VDL Mode 4 and UAT) used for ADS-B suffer from the same shortcoming; the receiver of a message does not have any means to check whether the contents of the message are valid. An erroneous report will not be detected as long as it conforms to the proper message format.

[0030] This flaw is considered to be both a safety and security problem and is considered to be a major obstacle for future use of ADS-B data in various vehicle surveillance systems, such as aircraft-based separation provision and/or collision avoidance systems, and stationary traffic surveillance systems, such as for example ATC systems used to monitor air traffic near airports.

[0031] The invention presented herein is a method and a system which greatly increases the safety of a vehicle surveillance system based on ADS-B by providing a possibility to validate the positional data contained in received ADS-B messages.

[0032] The proposed principles utilize the fact that the vehicle positions in an ADS-B-based vehicle surveillance system are self-reported, meaning that all vehicles in such a system broadcast state vectors indicating their own position. By providing a possibility to estimate the position of a radio source from which a received ADS-B message was transmitted, the invention allows for validity check of the positional data contained in the received message. In general term, this is achieved by checking whether the estimated position of the radio source from which the ADS-B message was transmitted coincides sufficiently well with the position stated in the message. Since the vehicle positions are supposed to be self-reported, a mismatch between the estimated and reported position indicates that the reported position cannot be indiscriminately relied upon.

[0033] This improvement will enhance the criticality of the positional data in vehicle surveillance systems based on ADS-B and thus enable use of the data in safety critical vehicle surveillance systems.

[0034] As will be understood, the principles described herein for validating positional data is relevant and applicable to any vehicles surveillance system receiving self-reported positional data from surrounding vehicles. However, it will hereinafter be described mainly in the context of ADS-B-based aircraft surveillance system for separation provision and/or collision avoidance applications, residing in an aircraft. Aircraft-based aircraft surveillance systems used for separation provision applications, collision avoidance applications, or both, are sometimes referred to as Sense & Avoid systems.

[0035] Figs. 1A and 1B illustrate airspace 1 in which a host aircraft 3 surrounded by a plurality of surrounding aircraft 5 are located. An ATC ground station 7 for supervising the air traffic in the airspace 1 is also shown.

[0036] Each aircraft 3, 5 comprises an ADS-B transponder 9 (only shown for host aircraft 1 for illustrative purposes) for broadcasting their state vectors to all nearby aircraft and ground stations, and for receiving and interpreting ADS-B messages 13 from surrounding aircraft. The ATC ground station 7 also comprises an ADS-B transponder for receiving and interpreting received messages. The ADS-B messages 13 comprise positional data relating to the positions of the aircraft from which they are transmitted. Typically, the ADS-B messages also comprise other aircraft specific status information, such as an aircraft identifier and the current speed of the aircraft.

[0037] In Fig. 1A the host aircraft 3 broadcasts its state vector to all nearby aircraft 5 and the ground station 7, and in Fig. 1B the surrounding aircraft 5 broadcast their state vectors to the host aircraft 3 and typically also to all other aircraft 5 as well as the ground station 7. In this way, each aircraft 3, 5 as well as the ground station 7 can have a complete picture of all aviation traffic in the monitored airspace 1.

[0038] The ADS-B transponder 9 onboard each aircraft 3, 5 may be any of the ADS-B transponder types currently under consideration, i.e. a Mode S ES transponder, a VDL Mode 4 transponder or a UAT transponder. However, the different types of ADS-B transponders conform to different message formats and are, as of today, unable to communicate with each other. Therefore, all aircraft 3, 5 should be equipped with the same type of ADS-B transponders 9, or at least compatible ADS-B transponders 9, and the aircraft surveillance system of the ATC ground station 7 should be designed to support reception and interpretation of messages sent over the airborne data link (Mode S ES, VDL Mode 4 or a UAT) defined by that particular type of ADS-B transponder 9.

[0039] Figs. 2A and 2B illustrate schematically the concept of the present invention.

[0040] In Fig. 2A, an aircraft 5 transmits an ADS-B message 13 carrying information indicating at least the position $P_{ADS\text{-}B(5)}$ of said aircraft 5. The alleged position $P_{ADS\text{-}B(5)}$ of a vehicle as stated in an ADS-B message 13 will hereinafter be referred to as the ADS-B position or reported position. The positional data contained in an ADS-B message is associated with a certain uncertainty and, therefore, the ADS-B position $P_{ADS-B(5)}$ of the aircraft 5 is illustrated with a dotted circle that is somewhat bigger than the actual aircraft. Typically, the positional data contained in an ADS-B message 13 is based on GPS information and is therefore associated with a well known uncertainty which, as well known in the art, for example depends on how many GPS satellites the aircraft has contact with when the position is determined. The host aircraft 3 picks up the ADS-B message 13 and registers the reported position $P_{ADS-B(5)}$ of the aircraft 5. However, instead of indiscriminately relying on the reported ADS-B position $P_{ADS-B(5)}$ and e.g. use said position as input parameters to a Sense & Avoid system of the host aircraft 3, the host aircraft 3 according to the invention comprises means for validating the received positional data. As mentioned above, this is in general terms achieved by estimating the position $P_{EST(5)}$ of the radio source 5 from which the ADS-B message 13 was transmitted and comparing said estimated position $P_{EST(5)}$ with the reported ADS-B position $P_{ADS-B(5)}$. By comparing the position $P_{ADS-B(5)}$ indicated by the positional data in the received ADS-B message 13 with the estimated position $P_{EST(5)}$, the host aircraft 3 and its Sense & Avoid system can take actions, such as refusing the received positional data to be used in flight safety critical applications, if the two positions $P_{ADS-B(5)}$, $P_{EST(5)}$ do not coincide sufficiently well. The way the estimated position $P_{EST(5)}$ of the radio source 5 transmitting the ADS-B message 13 is calculated will be described in more detail later on.

[0041] The estimated position $P_{EST(5)}$ is also associated with an uncertainty which, as illustrated by a circle that is somewhat bigger than the one illustrating the ADS-B position $P_{ADS-B(5)}$, typically is larger than the uncertainty associated with the reported ADS-B position $P_{ADS-B(5)}$. Although illustrated as circles for the sake of simplicity, it should be appreciated that both the ADS-B position $P_{ADS-B(5)}$ and the estimated position $P_{EST(5)}$ are associated with uncertainties in all space dimension and that the dotted lines hence should be construed as cross sections of three-dimensional bodies of which shape depend on the positional uncertainties in each space dimension. The uncertainties associated with the ADS-B position $P_{ADS-B(5)}$ and the estimated position $P_{EST(5)}$, respectively, are preferably accounted for when the two positions are compared.

[0042] While Fig. 2A illustrates a scenario in which the reported ADS-B position $P_{ADS-B(5)}$ of aircraft 5 coincides with its position $P_{EST(5)}$ as estimated by the host aircraft 3, indicating that the radio source from which the received ADS-B message 13 was transmitted most likely is located at said position $P_{ADS-B(5)}$ and that the positional data hence can be relied upon, an opposite scenario will now be described with reference to Fig. 2B.

[0043] In Fig. 2B, an aircraft 5' transmits an ADS-B message 13' which is received by the host aircraft 3. The host aircraft 3 retrieves the positional data contained in the ADS-B message 13' and registers the reported ADS-B position. In accordance with what is described above, the host aircraft 3 also calculates an estimated position $P_{EST(5')}$ of the radio source 5' from which the message 13' was transmitted, which position $P_{EST(5')}$ in this case is seen to deviate substantially from the position of the aircraft 5' as stated in the ADS-B message 13'. The deviation between the self-reported position $P_{ADS-B(5')}$ and the estimated position $P_{EST(5')}$ indicates to the host aircraft 3 that the positional data in the received ADS-B message 13'cannot be indiscriminately relied upon.

[0044] Since the ADS-B system is based on that each aircraft broadcasts its own state vector, a mismatch between the position of a nearby aircraft according to a received ADS-B message and the estimated position of the radio source transmitting said ADS-B message typically depends on one of two things: First, the ADS-B transponder, the GPS receiver, or any other vital system component of the transmitting aircraft may be malfunctioning. Secondly, the radio source transmitting the ADS-B message may be deliberately arranged to report another position than its own. It is a well-known weakness of the ADS-B system that "fake" ADS-B messages may be broadcasted deliberately with malicious intent in order to create confusion or even in order to take out the aircraft surveillance system of both aircraft and ground stations in a certain area by flooding that area with deceptive ADS-B messages.

[0045] The latter scenario is also illustrated in Fig. 2B where a malicious ADS-B message 13" is seen to be transmitted from an ADS transponder 15" located on the ground. The positional data contained in the ADS-B message 13", which is received and registered by the host aircraft 3, deceptively alleges that an aircraft is located at the position $P_{ADS-B(15")}$. However, when the host aircraft 3 (or any other unit receiving the message 13" and having an aircraft surveillance system utilizing the inventive concept disclosed herein) tries to validate the received positional data by estimating the position of the radio source 15" from which it received the message 13", it will find a mismatch between the position of the radio source 15" and the alleged position $P_{ACS-B(15")}$ of an aircraft and can hence discard the positional data contained in the received ADS-B message 15" as unreliable.

[0046] The method and means for validating received positional data will now be described in more detail.

[0047] In order to estimate the positions $P_{EST(5)}$, $P_{EST(5')}$ of the radio sources 5, 5', 15" broadcasting the ADS-B messages 13, 13', 13" in Figs. 2A and 2B, the host aircraft 3 comprises a radio direction finding antenna arrangement, such as a directional antenna arrangement, which can be used to determine the bearing to a radio source by analyzing a radio signal received there from. How such antenna arrangements are designed and used to determine the approximate bearing to a radio source from which a signal is received is well known in the art and need not further be described herein.

[0048] The distance from the host aircraft 3 to the radio source 5, 5', 15" broadcasting the ADS-B message 13, 13', 13" is estimated based on the time of flight (TOF) for a signal travelling at a known speed between the radio source and the host aircraft. Preferably, when possible, the distance is determined based on the TOF for the ADS-B message 13, 13', 13" carrying the positional data that is to be validated.

[0049] Fig. 3 is a flowchart illustrating a method for validating received positional data according to the invention. The method steps may be performed by any receiving unit receiving such data, such as a vehicle (e.g. an aircraft) or a stationary unit (e.g. an ATC ground station). When describing the method, simultaneous reference will, however, be made to the exemplary operational environment of the invention illustrated in Figs. 2A and 2B, in which the receiving unit is the host aircraft 3.

[0050] In step S1, a signal 13, 13', 13" originating from a radio source 5, 5', 15" is received by the host aircraft 3 by means of a radio direction finding antenna arrangement capable of estimating the bearing to the emitting radio source. The signal 13, 13', 13" carries positional data that indicates an alleged position $P_{ADS-B(5)}$, $P_{ADS-B(5')}$, $P_{ADS-B(15")}$ of an aircraft. "Alleged" here means that there may or may not be an aircraft at the position reported by the radio source. The invention is intended for a vehicle surveillance system in which each vehicle transmits its own position, and the case in which an aircraft is not at the position reported by the radio source hence indicates either system equipment malfunction or that the radio source is deliberately arranged to transmit deceptive positional data.

[0051] In step S2, the bearing to the radio source 5, 5', 15" transmitting the signal 13, 13', 13" that carries the positional data is estimated by the host aircraft 3 by analyzing the signal 13, 13', 13" received with the radio direction finding antenna arrangement in known ways.

[0052] In step S3, the host aircraft 3 estimates the distance to the radio source 5, 5', 15" based on the TOF for a signal travelling between the radio source and the host aircraft 3, and the propagation velocity (the speed of light) of the signal. Preferably, the distance is estimated based on the TOF for the signal 13, 13', 13' carrying the positional data that is to be validated. However, the distance may be estimated based on the TOF also for other signals transferred between the radio source and the host aircraft. The way the host aircraft 3 estimates the distance to the radio source may vary depending on, e.g., the type of data link used for the transmission and the information content of the signal and will be described in more detail below.

[0053] In step S4, the host aircraft 3 calculates an estimated position $P_{EST(5)}$, $P_{EST(5')}$, $P_{EST(15")}$ of the radio source 5, 5', 15" based on the bearing estimated in step S2 and the distance estimated in step S3.

[0054] In step S5, the host aircraft 3 determines a deviation value indicative of the deviation/coincidence between the aircraft position $P_{ADS-B(5)}$, $P_{ADS-B(5')}$, $P_{ADS-B(15")}$ as reported by the radio source 5, 5', 15" and the estimated position $P_{EST(5)}$, $P_{EST(5')}$, $P_{EST(15")}$ of the radio source 5, 5', 15" calculated in step S4. If the reported position $P_{ADS-B(5)}$, $P_{ADS-B(5')}$, $P_{ADS-B(15")}$ is an absolute position, the own position of the host aircraft 3 must be used when estimating the distance to the reported position. If, on the other hand, the reported position $P_{ADS-B(5)}$ $P_{ADS-B(5')}$, $P_{ADS-B(15")}$ is a relative position of an aircraft in relation to the host aircraft, knowledge about the host aircraft's own position is not needed. The determined deviation value is an indicator of the reliability of the received positional data and can be used as a basis for deciding whether the received positional data should be used or discarded by the receiving unit (in this exemplary case host aircraft 3).

[0055] Now, method step S3 will be described in more detail with simultaneous reference to Figs. 2A and 2B. As aforementioned, the estimated distance to the radio source 5, 5', 15" is based on the TOF for a signal travelling between the radio source and the host aircraft 3 at known speed, and the way the TOF determination is performed depends on the data link type over which the positional data is transmitted.

Distance estimation in VDL Mode 4

[0056] First, a concept for determining the TOF for an ADS-B message 13, 13', 13" conforming to the VDL Mode 4 format will be described.

[0057] VDL Mode 4 is based on STDMA which is a channel access method allowing several users to share the same frequency channel by dividing it into different slots based on time. Each ADS-B transponder conforming to the VDL Mode 4 format is required to transmit its state vector in specific timeslots. The start of each timeslot is determined by the VDL Mode 4 standard and based on UTC (GPS time). Each timeslot starts at a specific point in time and ends at a specific point in time (as defined by UTC), which points in time are globally defined and known by all VDL Mode 4 transponders. More detailed information about VDL Mode 4 and STDMA is found in, e.g., the document entitled "Self-organizing Time Division Multiple Access VDL Mode 4 - Standards and Recommended Practices", which is Appendix D of the Report on Agenda Item 5 of the fourth meeting of the Aeronautical Mobile Communications Panel (AMCP/4); Montreal, 25 March - 4 April 1996 (also found on the Internet at http://www.icao.int/anb/panels/acp/meetings/amcp4/item-5d.pdf, 2008-04-22).

[0058] The proposed principle for determining the TOF for a VDL Mode 4 message is to estimate the TOF based on the time between the start of the timeslot in which the message is received and the point in time at which the message is received.

[0059] This principle is illustrated in Figs. 3A and 3B which illustrate a frame 10 that is a part of a VDL Mode 4 data stream. The frame 10 is divided into a plurality of timeslots 12. Different timeslots are allocated to different VDL Mode

4 transponders. For example, the timeslot indicated by reference numeral 12 can be allocated to the aircraft indicated by reference numeral 5 in Fig. 2A. At the start 14 of the timeslot 12, the aircraft 5 broadcasts the VDL Mode 4 message 13 over the STDMA-based VDL Mode 4 data link.

[0060] Typically, the transmission of the VDL Mode 4 message 13 commences almost immediately upon the start 14 of the timeslot 12 allocated for that transmission. According to the VDL Mode 4 standard and recommended practice, transmission of a VDL Mode 4 message should commence no later than 1 microsecond after the start 14 of the timeslot 12 allocated for that transmission, which normally is a much longer time period than needed. The host aircraft 3, which also comprises a VDL Mode 4 transponder 9 and hence knows when each timeslot starts and ends, receives the message 13 at some point in time 16 within the timeslot 12 (the STDMA timeslots are long enough to ensure that at least the start of a VDL Mode 4 message is received within the same timeslot as it is broadcasted). The host aircraft 3 comprises means to determine the point in time 16 at which the message 13 arrives. Typically, the VDL Mode 4 transponder 9 itself comprises means for determining when a message 13 is received. Since the VDL Mode 4 transponder of the host aircraft knows exactly when the timeslot started, the elapsed time Δt between start of the timeslots and reception of the message can be determined. As this time Δt substantially corresponds to the TOF of the VDL Mode 4 message 13, and as the radio signal carrying the message 13 propagates at known speed (the speed of light), the host aircraft 3 can calculate an estimated distance $d_{EST(5)}$ to the aircraft 5 from which it received the VDL Mode 4 message 13. As the VDL Mode 4 standard permits a transponder to commence transmission up to 1 microsecond after the start of a timeslot, such a transmission delay is preferably accounted for by the receiving unit when determining the TOF for the signal. For example, the TOF may be estimated as the elapsed time Δt between start of the timeslot and reception of the signal minus 500 nanoseconds (half the allowable transmission delay).

[0061] The above described method for estimating a distance to a radio source from which a signal is received is applicable to all communications systems using STDMA-based radio links. Besides ADS-B VDL Mode 4 systems for air traffic surveillance, an example of such a system is the AIS system which is commonly used for maritime traffic surveillance. In both the ADS-B VDL Mode 4 system and the AIS system, the vehicles (aircraft and ships/vessels, respectively) transmit positional data indicating their own position to surrounding vehicles.

[0062] It should also be appreciated that the method described above is not limited to systems using STDMA-based radio links but is applicable in any communications system using time-synchronized data links over which transmissions are initiated at points in time that are known by all users of the data link.

Distance estimation in UAT

[0063] Now, a concept for determining the TOF for an ADS-B message conforming to the UAT format will be described.

[0064] Transmissions over the UAT data link are one of two general types; a ground uplink message or an ADS-B message. When the term "UAT message" is used hereinafter, it refers to the ADS-B message of a UAT transmission. Contrary to ADS-B messages conforming to the VDL Mode 4 format, UAT messages are broadcasted on pseudorandom basis. A UAT frame that has a length of 1 second typically comprises 3200 so called Message Start Opportunities (MSO), each associated with a well-defined point in time (UTC). The transmission of a UAT message occurs at a randomly chosen MSO within the UAT frame.

[0065] The information transmitted in a UAT message is referred to as the "Payload" and besides the state vector of the aircraft (comprising e.g. the positional data), a UAT message payload includes the MSO at which it was broadcasted. That is, a UAT message carries information of its own precise transmission time.

[0066] By determining the point in time at which a UAT message is received, and by establishing the point in time at which the message was transmitted based on the MSO information in the message, the elapsed time between transmission and reception, i.e. the TOF, of a UAT ADS-B message can be determined.

[0067] As in the case with VDL Mode 4 messages described above, an aircraft receiving a UAT message from a nearby aircraft can hence estimate the distance to that aircraft based on the TOF of the message.

Distance estimation in Mode S ES

[0068] Mode S ES messages, i.e. ADS-B messages conforming to the Mode S ES format, are randomly broadcasted and, unlike UAT messages, they carry no information about the point in time at which they were transmitted. Today, there are therefore no known ways of establishing the exact TOF for a Mode S ES message.

[0069] In order to calculate an estimated position of a radio source from which a Mode S ES message originates, the receiving unit needs to comprise additional distance measuring equipment. Such additional distance measuring equipment may be, e.g., primary radar equipment, laser detection and ranging (LADAR) equipment, or secondary surveillance radar equipment, all known in the art for utilizing signal TOF for estimating distances to surrounding objects.

[0070] That is, if for example the ADS-B message 13 broadcasted by aircraft 5 in Fig. 2A is a Mode S ES message 13, the host aircraft 3 must comprise additional distance measuring equipment in order to calculate an estimated position

$P_{EST(5)}$ of the aircraft 5. However, thanks to the radio direction finding antenna arrangement with which the Mode S ES message 13 is received according to the invention, the host aircraft 3 can still estimate a bearing to the transmitting aircraft 5. A measure of the bearing can be sufficient to establish that the reported Mode S ES position $P_{ADS\text{-}B(5)}$ is erroneous and cannot be relied upon.

[0071] If the host aircraft 3 comprises conventional radar or LADAR equipment, the TOF for the radar radio signal or LADAR laser pulse signal can be used for estimating a distance to the aircraft 5. An estimated position $P_{EST(5)}$ of the aircraft 5 can then be calculated based on the bearing estimated by means of the radio direction finding antenna arrangement receiving the Mode S ES message 13 and the distance estimated using the TOF of the reflected radar or LADAR signal.

[0072] Besides or instead of conventional radar and/or LADAR equipment, the host aircraft 3 may comprise a rapidly-steerable radar connected to control means and drive means which are arranged to steer the radar based on the positional data contained in received Mode S ES messages. As soon as a Mode S ES message 13 is received by the host aircraft 3, such a rapidly-steerable radar can be directed towards the position $P_{ADS\text{-}B(5)}$ stated in the Mode S ES message 13 to obtain a TOF of a radar signal reflected by the aircraft 5 that broadcasted the Mode S ES message. Thereby, an estimated position $P_{EST(5)}$ of the aircraft 5 can be calculated. The radar beam should of course be wide enough to allow for changes in aircraft position during alignment of the steerable radar. Such changes in aircraft position can also be accounted for by allowing a larger deviation between the reported Mode S ES position $P_{ADS\text{-}B(5)}$ and the estimated position $P_{EST(5)}$ without discarding the reported Mode S ES position as erroneous.

[0073] The host aircraft 3 may also comprise secondary surveillance radar equipment, such as e.g. a Mode S transponder and interrogator which are used in TCAS systems of today as described in the background portion. The interrogator, which in conventional secondary surveillance radar systems typically broadcasts general presence requests/ interrogations on a periodic basis, can be arranged to broadcast a presence request immediately upon reception of a Mode S ES message, such as the Mode S ES message 13 from the nearby aircraft 5. If the aircraft 5 comprises a transponder conforming to the same data format as the interrogator of the host aircraft 3, it will respond to the request. The interrogator of the host aircraft 3 can then determine the TOF for a radio signal travelling between the two aircraft 3, 5 based on the time elapsed between the transmission of the request/interrogation and the reception of the response (which time hence equals twice the signal TOF between the aircraft 3, 5 plus additional signal processing delays which can be accounted for).

[0074] It should also be appreciated that, as an increase in Mode S ES radio traffic is expected, future generations of Mode S ES may support globally or locally time synchronized broadcasting of Mode S ES messages to avoid interference-related issues. In such a case, it would probably be possible to estimate the distance to a radio source transmitting a Mode S ES message in a way similar to the above described way of estimating the distance to a radio source transmitting a VDL Mode 4 message. It is also possible that future generation of Mode S ES will allow for inclusion of transmission time information in the Mode S ES messages, in which case the method described above for estimating the distance to a radio source broadcasting a UAT message can be utilized for the distance estimation.

[0075] Fig. 5 illustrates an embodiment of a vehicle surveillance system 17 according to the invention. The vehicle surveillance system 17 comprises a subunit 18 which may be included in any type of receiving unit, such as a vehicle or stationary unit, for validating self-reported positional data. In this exemplary embodiment, however, the vehicle surveillance system subunit 18 is used in an ADS-B-based aircraft surveillance system 17 for aircraft separation provision and/or collision avoidance applications. It should be understood that the vehicle surveillance system 17 in Fig. 5 is associated with a host aircraft, such as the host aircraft 3 in Figs. 2A and 2B. The host aircraft comprising the aircraft surveillance system 17 may be a conventional manned aircraft or a UAV that is either manually but remotely piloted or that flies autonomously based on pre-programmed flight plans.

[0076] The aircraft surveillance system 17 comprises an antenna module 19 comprising a radio direction finding antenna arrangement. In this exemplary embodiment, the direction finding antenna arrangement comprises at least one directional antenna 21. Typically, the antenna module 19 comprises a plurality of antennas for various purposes and may, besides the directional antenna 21, for example comprise an omnidirectional antenna, a planar array antenna and a dipole antenna, illustrated in dotted lines. The antenna(s) are connected to transceiver circuitry 23 for processing signals transmitted and received by said antenna(s).

[0077] The aircraft surveillance system 17 further comprises a sensor module 25 which typically comprises a plurality of passive and active sensors for monitoring and communicating with the world around.

[0078] The sensor module 25 comprises an ADS-B functionality module 27, typically in form of a conventional ADS-B transponder, for generating and for processing ADS-B messages. The ADS-B transponder 27 may be any of a Mode S ES transponder, a VDL Mode 4 transponder or a UAT transponder. The ADS-B module 27 may also comprise two or all three of said ADS-B transponder types to ensure compatibility with ADS-B transponders of nearby aircraft. Future ADS-B systems are likely to use transponders supporting all three of the above mentioned data link formats. Such a transponder would be an obvious part of the ADS-B module 27. The ADS-B functionality module 27 is connected, via the transceiver circuitry 23, to the directional antenna 21 which is used at least for receiving incoming ADS-B messages.

[0079] The sensor module 25 further comprises a positioning functionality module 29 for selfi-location determination. Typically but not necessarily, the positioning functionality module 29 is a GPS receiver receiving GPS data enabling it to determine its own and thereby the host aircraft position, speed and direction of motion, as well as determining UTC time. The positioning module 29 may also use other navigational systems such as the Galileo positioning system or the GLONASS in order to determine its position in global coordinates. The positioning module 29 could also include an inertial navigation module keeping track of the host aircraft position without the need of external references. Additional functionality well known in the art for further increasing the accuracy in the positioning of a GPS receiver may also be included in the positioning module 29. The positioning functionality module 29 may also include sensors for measuring the atmospheric pressure, thus enabling the host aircraft elevation to be determined without the need of external references as well known in the art. The positioning module 29 may comprise one or several built-in antennas and/or use one or several antennas in the antenna module 19 for receiving signals, e.g, from GPS satellites, enabling self-location determination. The positioning module 29 is connected to the ADS-B module 27 for providing the ADS-B module 27 with information relating to the position of the host aircraft in which the aircraft surveillance system 17 resides, which information then may be included in ADS-B messages transmitted by the host aircraft. The positioning module 29 may also form an integral part of the ADS-B functionality module 27.

[0080] The sensor module 25 may further comprise various distance measuring sensors 31, 33, 35, 37, 39 for measuring the distance to nearby aircraft.

[0081] For example, the sensor module 25 may also comprise a conventional primary radar module 31. The primary radar module 31 is coupled to one or several antennas in the antenna module 19 for transmitting and receiving radio waves. As described above, the primary radar module 31 can then be used to estimate the distance to a nearby aircraft by determining the time elapsed between transmission and reception of said radio waves when reflected by the nearby aircraft. The primary radar module 31 can also comprise control means and drive means which are arranged to steer one or several rapidly-steerable radar antennas in the antenna module 19 based on positional data contained in received ADS-B messages. This functionality is particularly intended for estimating the distance to radio sources broadcasting Mode S ES messages, as described above. The primary radar module 31 is typically connected to differently designed antennas in the antenna module 19 to provide for both short range and long range radar functionality.

[0082] The sensor module 25 may further comprise a laser detection and ranging (LADAR) module 33. The LADAR module 33 uses the same principle as primary radar systems for estimating the distance to a remote object, i.e. measuring the time delay between transmission of a signal and detection of the reflected signal. However, instead of using radio waves, LADAR devices uses laser light. To implement this functionality, the LADAR module 33 typically comprises a laser source, a laser light detector, optical transceiver circuitry and signal processing logic (not shown).

[0083] The sensor module 25 may also comprise a secondary surveillance radar module 35. The secondary surveillance radar module 35 comprises a transponder 37 and an interrogator 39. The secondary surveillance radar module 35 is coupled to one or several antennas in the antenna module 19 to broadcast presence request/interrogations and receive responses to said requests/responses as described above. The secondary surveillance radar module 35 can be arranged to transmit presence request/interrogations on a periodic basis but may also be arranged to transmit presence request/interrogations as soon as an ADS-message is received. This functionality is particularly intended for estimating the distance to radio sources broadcasting Mode S ES messages, as described above. The secondary surveillance radar module 35 is arranged to estimate the distance to nearby objects responding to a broadcasted presence request/interrogation by determining the time elapsed between the transmission of the request/interrogation and the reception of the response.

[0084] The transponder 37 may for example be a Mode S, Mode A or Mode B transponder but may conform to any known data link format which offers the same functionality. It should be appreciated that the signal transmitted by a transponder as response to a request from an interrogator does not need to carry any information and that the requirements of the data link format therefore is low. The secondary surveillance radar module 35 may use the directional antenna 21 or any other antenna in the antenna module 19 for transmission and reception of requests and responses.

[0085] Typically, the positioning module 29 is connected to each sensor 27, 31, 33, 35 in the sensor module 25 to allow the various sensors to use GPS time (UTC) and self-location data when estimating the distance to a radio source from which an ADS-B message is received. The sensors 27, 31, 33, 35 may also be connected to each other in order to use each others measurements so as to optimize their own functionality. So for example the primary 31 and secondary 35 radar modules may be connected to the ADS-B module 27 in order to adjust the steering of steerable radar antennas and the transmission of presence requests/interrogations based on the positional data contained in received ADS-B messages, and the time of reception of ADS-B messages, respectively. The various sensors 27, 31, 33, 35 may also comprise built-in clocks for determining the point in time for transmission and reception of signals.

[0086] When the directional antenna 21 receives an ADS-B message from a nearby radio source, the transceiver circuitry 23 estimates the bearing to said radio source. Depending on what format the ADS-B message conforms to, the ADS-B module 27 or some of the distance measuring sensors 31, 33, 35 estimate the distance to the radio source as previously described. The ADS-B module 27 also extracts the ADS-B position reported in the received ADS-B message, which position allegedly is the position of a nearby aircraft. Furthermore, the positioning module 29 is arranged to establish the self-location of the host aircraft when an ADS-B message is received. The estimated bearing and distance to the radio source, as well as the received ADS-B position and the established self-location of the host aircraft are then sent to a position validation unit 41.

[0087] The position validation unit 41 comprises a calculation unit 43 which is arranged to take the estimated bearing and distance to the radio source as well as the self-location of the host aircraft as input parameters and calculate an estimated position of the radio source from which the ADS-B message was received. The estimated position of the radio source and the reported ADS-B position are then provided to a comparator 45. The comparator 45 is arranged to compare the estimated position with the reported ADS-B position and determine a deviation value indicating the deviation/coincidence between the two positions. The deviation value and at least the reported ADS-B position are then sent to a discriminator 47. The discriminator 47 is arranged to process the reported ADS-B position data in different ways based on the deviation value that is determined by the comparator 45 and hence indicative of the reliability of the currently processed ADS-B position data. Preferably, the discriminator 47 is arranged to take the uncertainties associated with the reported ADS-B position and the estimated position, respectively, into account when determining how to process the received ADS-B position data. These uncertainties can be either pre-programmed into the discriminator 47 or provided to the discriminator 47 by the antenna module 19 and the sensor module 25 if the components responsible for retrieving the reported ADS-B position and estimate the position of the radio source are capable of determining the uncertainties associated therewith.

[0088] In this exemplary aircraft surveillance system 17, the discriminator 47 is communicatively connected to an information module 49 and a decision and manoeuvring unit 51 to which it forwards the received ADS-B positions of nearby aircraft, at least when found reliable.

[0089] In a conventional, manned aircraft, the information module 49 is located in the aircraft cockpit and serves to inform the pilot about the surrounding air traffic. The ADS-B positions of the nearby aircraft are typically displayed on a graphical navigational display 53. The information module 49 is also seen to comprise a speaker 55 for providing audible warnings to the pilot in case a nearby aircraft is getting too close to the host aircraft. The host aircraft position is typically provided to the information module 49 by the positioning module 29 of the aircraft surveillance system 17. In case the host aircraft with which the aircraft surveillance system 17 is associated is a UAV, the information module 49 may reside in a ground station at which a pilot is situated to remotely control and/or supervise the UAV. In that case, data, such as the host aircraft position and the ADS-B positions of nearby aircraft received by the directional antenna 21 of the UAV, is typically broadcasted to the ground-based information module 49 over a radio link.

[0090] The decision and manoeuvring unit 51 comprises control means 57 for manoeuvring the host aircraft, and a manoeuvring logic module 59 for continuously determining the optimal flight route for the host aircraft. The manoeuvring logic module 59 is arranged to take navigation-critical data as input parameters, analyze said data and determine an optimal speed and flight direction for the host aircraft based on the result of the analysis. One such navigation-critical parameter is the reported ADS-B positions of nearby aircraft. Other may be, e.g., a pre-programmed flight plan, the current speed, position and flight direction of the host aircraft, and the current speed and flight direction of the nearby aircraft. If the host aircraft is an autonomously controlled UAV or a piloted aircraft (manned aircraft or remotely piloted UAV) currently on autopilot, the manoeuvring logic module 59 may continuously or periodically provide the control means 57 with information on the (momentarily) optimal speed and flight direction in order for the control means 57 to manoeuvre the host aircraft accordingly. If, on the other hand, the host aircraft is manually piloted from cockpit, or remotely piloted from a ground station, the optimal speed and flight direction of the host aircraft as determined by the manoeuvring logic module 59 can be provided to the pilot and used for decision-making support.

[0091] According to one aspect of the invention, the discriminator 47 of the position validation module 41 in the aircraft surveillance system 17 is arranged to discard a received ADS-B position if the deviation value indicating the deviation between said ADS-B position and the estimated position exceeds a certain threshold value. Here "discard" means that the discriminator 47 prevents the ADS-B position from reaching the information module 49 and the decision and manoeuvring unit 51. Thereby, a reported ADS-B position of a nearby aircraft that cannot be validated by the aircraft surveillance system 17 will never be presented to the aircraft pilot and/or used as a basis for automatic aircraft control.

[0092] According to another aspect of the invention, the discriminator 47 does not discard a reported ADS-B position even though it deviates substantially from the estimated position of the radio source transmitting it. Instead, when the deviation value established by the comparator 45 exceeds a certain threshold value, the discriminator 47 is arranged to add a flag indicating that the received ADS-B position may not be trustworthy to the ADS-B data before forwarding the data to the information module 49 and the decision and manoeuvring unit 51. Thereby, the information module 49 and the decision and manoeuvring unit 51 can recognize unreliable ADS-B data and act accordingly.

[0093] The information module 49 can in this case be arranged to visually or audibly alert a pilot of the host aircraft that an unreliable ADS-B position of a nearby aircraft has been received and, e.g., indicate the alleged position of the nearby aircraft on the navigation display 53. The manoeuvring logic module 59 of the decision and manoeuvring unit 51 may, upon detection of such a flag indicating an unreliable ADS-B position, be arranged to ignore the ADS-B position and not use it in the determination of the (momentarily) optimal speed and direction of flight for the host aircraft.

[0094] According to yet another aspect of the invention, a large deviation value between an ADS-B position reported by a radio source and an estimated position of that radio source can be used as an indicator for initiating an additional aircraft position validation process. If the deviation value determined by the comparator 45 exceeds a predetermined threshold value, the discriminator 47 can be arranged to ask other sensors in the aircraft surveillance system 17, such as e.g. the primary radar 31 or the LADAR 33, whether they are able to detect an aircraft at the given ADS-B position. If they are, the ADS-B position can be forwarded to and used by the information module 49 and the decision and manoeuvring unit 51 as described above. If, on the other hand, the sensors of the aircraft surveillance system 17 are unable to confirm the presence of an aircraft at the alleged ADS-B position, the discriminator 47 either discards the ADS-B positional data or sets a flag indicating that it is found unreliable before forwarding it, as also described above.

[0095] Although the functionality implementing the inventive concept has been described herein as residing in separate functional modules, such as the antenna module 19, the sensor module 25 and the position validation unit 41, it should be appreciated that this is made only to facilitate description of the aircraft surveillance system 17 and that the functionality may be implemented in many other ways without departing from the scope of the invention.

[0096] It should also be appreciated that the self-location of the host aircraft would not be a required parameter in the process of validating received positional data if the received positional data indicate the relative position of the transmitting aircraft in relation to the host aircraft instead of the absolute position of the transmitting aircraft. If, for example, a first aircraft in an airspace monitored by a ground-based ATC station receives a relative position of a second aircraft from the ATC station, this relative position could be validated by the second aircraft if transmitted to said second aircraft in a message from said first aircraft. In this case, the second aircraft does not need to know its own position in order to validate the received positional data.

[0097] The principle proposed in this document for validating received positional data ensures that navigational decisions are made based on correct information of surrounding traffic. The above described vehicle surveillance system may be included in aircraft and ground-based ATC stations as well as ships and land-based VTS stations to increase air and maritime traffic safety.

[0098] In particular, the suggested principle for validating received ADS-B positional data relating to the positions of nearby vehicles enhances the safety and security of an aircraft surveillance system which uses ADS-B data as at least one source of information. Thereby, an ADS-B-based aircraft surveillance system according to the invention can be advantageously used for both separation provision and collision avoidance applications due to the increased reliability of the data on which decisions are made.

[0099] Besides the increased flight safety offered by the vehicle surveillance system 17 according to the invention, aircraft comprising such a system and using it for automatic aircraft separation provision will lower their fuel consumption since their pre-programmed flight plan will not be altered due to erroneous ADS-B messages reported by surrounding aircraft.

[0100] As well known in the art, ADS-B transponders transmit ADS-B messages periodically at regular intervals. The proposed principle of validating positional data contained in ADS-B messages can be used to validate each and every one of the ADS-B messages received from a particular radio source, but it may also be used to validate, e.g., every tenth received ADS-B message. Once a particular radio source has been found reliable, there may not be a need to validate every single ADS-B message received there from. Thus, it should be understood that a vehicle surveillance system according to the invention can be adapted to validate positional data in received ADS-B messages continuously or periodically, or even by order of the system operator (e.g. a pilot of an aircraft equipped with the system).

[0101] It should be understood that although particularly intended for validation of ADS-B data, the inventive concept disclosed herein may be used to validate any positional data relating to the position of a vehicle from which the data allegedly is transmitted.

[0102] Although the invention has been described with reference to specific embodiments, these descriptions are not meant to be construed in a limiting sense. Various modifications of the disclosed embodiments, as well as alternative embodiments of the invention will become apparent to persons skilled in the art upon reference to the description of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiments disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the scope of the invention as set forth in the appended claims.

[0103] It is therefore contemplated that the claims will cover any such modifications or embodiments that fall within the true scope of the invention.

Claims

1. A method for validating received positional data in vehicle surveillance applications wherein vehicles transmit po-

sitional data indicating their own position to surrounding vehicles (3, 5; 5'), **characterized in** comprising the steps of:

receiving (S1), with a radio direction finding antenna arrangement (21, 23) of a receiving unit (3), a signal (13; 13', 13") carrying positional data indicating an alleged position ($P_{ADS-B(5)}$; $P_{ADS-B(5')}$, $P_{ADS-B(15")}$) of a vehicle, transmitted from a radio source (5; 5', 15");
estimating (S2) the bearing from the receiving unit (3) to said radio source (5; 5', 15") utilizing said radio direction finding antenna arrangement (21, 23) and the received signal (13; 13', 13");
estimating (S3) the distance between the receiving unit (3) and the radio source (5; 5', 15") based on the time of flight, TOF, for a signal travelling there between at known speed;
calculating (S4) an estimated position ($P_{EST(5)}$; $P_{EST(5')}$, $P_{EST(15")}$) of the radio source (5; 5', 15") based on the estimated bearing and the estimated distance, and
determining (S5) a deviation value indicating the deviation/coincidence between the alleged position ($P_{ADS-B(5)}$; $P_{ADS-B(5')}$, $P_{ADS-B(15")}$) of a vehicle according to the received positional data and the estimated position ($_{PEST(5)}$; $P_{EST(5')}$, $P_{EST(15")}$) of the radio source (5; 5', 15").

2. A method according to claim 1, wherein said deviation value is used as an indicator of the reliability of the received positional data.

3. A method according to claim 1 or 2, wherein the signal (13; 13', 13") carrying the positional data is transmitted using a data link over which a transmission is initiated at a given transmission point in time (14) that is known by all users of said data link, and wherein the step of estimating (S3) the distance between the receiving unit (3) and the radio source (5; 5', 15") is performed by:

determining the time of flight, TOF, for the signal carrying the positional data based on the time (Δt) elapsed from the transmission point in time (14) of said signal to the time of reception (16) of at least a first part of the signal; and
estimating said distance based on said TOF and the propagation velocity of said signal (13; 13', 13").

4. A method according to claim 3, wherein the signal (13; 13', 13") is an ADS-B message (13; 13', 13") conforming to the VDL Mode 4 format and the data link is a TDMA-based data link, such as a STDMA data link.

5. A method according to claim 1 or 2, wherein the signal (13; 13', 13") carrying the positional data further comprises transmission time information indicating the point in time at which it was transmitted, and wherein the step of estimating (S3) the distance between the receiving unit (3) and the radio source (5; 5', 15") comprises the steps of:

determining, by using the transmission time information in the received signal (13; 13', 13"), the time elapsed from the point in time at which said signal was transmitted to the point in time at which said signal was received, and estimating said distance based on said determined time and the propagation velocity of said signal (13; 13', 13").

6. A method according to claim 5, wherein said signal (13; 13', 13") is an ADS-B message (13; 13', 13") conforming to the UAT format.

7. A method according to claim 1 or 2, wherein the step of estimating (S3) the distance between the receiving unit (3) and the radio source (5; 5', 15") is performed by using primary radar equipment (19, 31), laser detection and ranging [LADAR] equipment (33), and/or secondary surveillance radar equipment (19, 35) comprised in the receiving unit (3).

8. A method according to claim 7, wherein said signal (13; 13', 13") is an ADS-B message (13; 13', 13") conforming to the Mode S ES format.

9. A vehicle surveillance system (17) for vehicle surveillance applications wherein vehicles (3, 5; 5') transmit positional data indicating their own position to surrounding vehicles (3, 5; 5'), **characterized in** comprising:

bearing-estimation means (21, 23) adapted to receive a signal (13; 13', 13") carrying positional data indicating an alleged position ($P_{ADS-B(5)}$; $P_{ADS-B(5')}$, $P_{ADS-B(15")}$) of a vehicle, transmitted from a radio source (5; 5', 15"), said bearing-estimation means (21, 23) further being adapted to estimate (S1) the bearing to said radio source (5; 5'; 15") using said received signal (13; 13', 13");
distance-estimation means (25) adapted to estimate (S2) the distance to the radio source (5; 5', 15") based on

the time of flight, TOF, for a signal received there from, which signal travels at known speed;
calculating means (43) adapted to calculate (S4) an estimated position ($P_{EST(5)}$; $P_{EST(5')}$, $P_{EST(15")}$) of the radio source (5; 5', 15") based on the estimated bearing and the estimated distance, and
comparing means (45) adapted to determine (S5) a deviation value indicating the deviation/coincidence between the alleged position ($P_{ADS-B(5)}$; $P_{ADS-B(5')}$, $P_{ADS-B(15")}$) of a vehicle according to the received positional data and the estimated position ($P_{EST(5)}$; $P_{EST(5')}$, $P_{EST(15")}$) of the radio source (5; 5', 15").

10. A vehicle surveillance system (17) according to claim 9, further comprising discriminating means (47) connected to an information module (49) for informing a system user of surrounding vehicle traffic and/or to a decision and manoeuvring unit (51) for controlling a vehicle in which the system (17) is included, said discriminating means (47) being adapted to discard positional data indicating an alleged position ($P_{ADS-B(5)}$; $P_{ADS-B(5')}$, $P_{ADs-B(15")}$) of a vehicle which, according to the deviation value determined by the comparing means (45), deviates substantially from the estimated position ($P_{EST(5)}$; $P_{EST(5')}$, $P_{EST(15")}$) of the radio source (5; 5', 15") from which the positional data was received.

11. A vehicle surveillance system (17) according to claim 9 or 10, wherein said bearing-estimation means (19) comprises at least one directional antenna (21) for receiving the signals (13; 13', 13") carrying the positional data and a transceiver circuitry (23) connected to said directional antenna (21) for estimating the bearing to the radio sources (5; 5'; 15") from which the signals (13; 13', 13") are received.

12. A vehicle surveillance system (17) according to any of the claims 9 to 11, wherein said signal (13; 13', 13") is an ADS-B message (13; 13', 13").

13. A vehicle surveillance system (17) according to any of the claims 9 to 12, wherein said vehicle surveillance system (17) is located in an aircraft (3) and used in an aircraft surveillance system (17) for separation provision and/or collision avoidance applications.

14. A vehicle (3, 5; 3, 5'), **characterized in** comprising a vehicle surveillance system (17) according to any of the claims 9 to13.

15. A ground-based air traffic control [ATC] station (7) for air traffic surveillance, **characterized in** comprising a vehicle surveillance system (17) according to any of the claims 9 to 13.

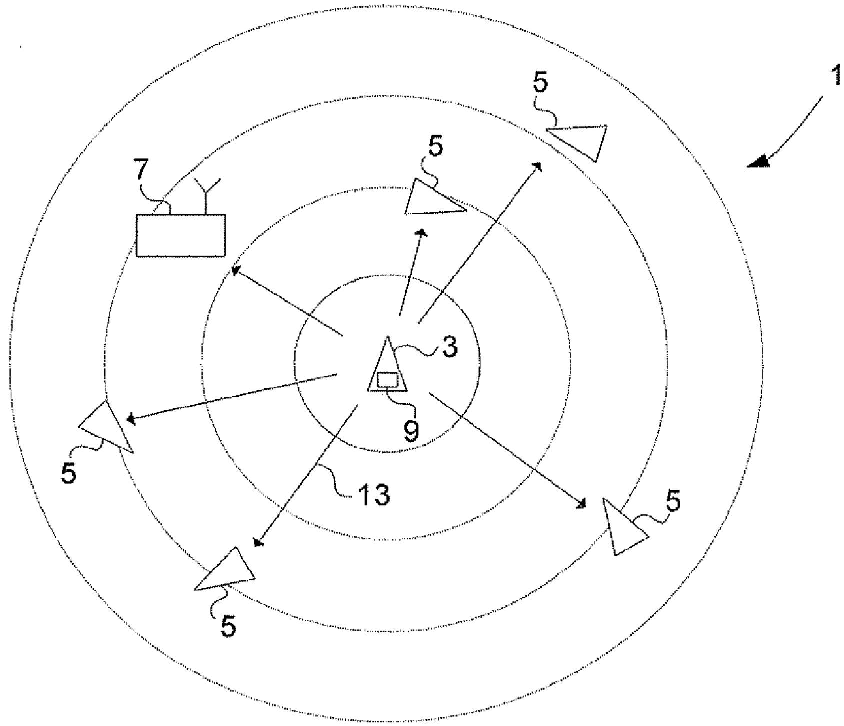


Fig. 1A

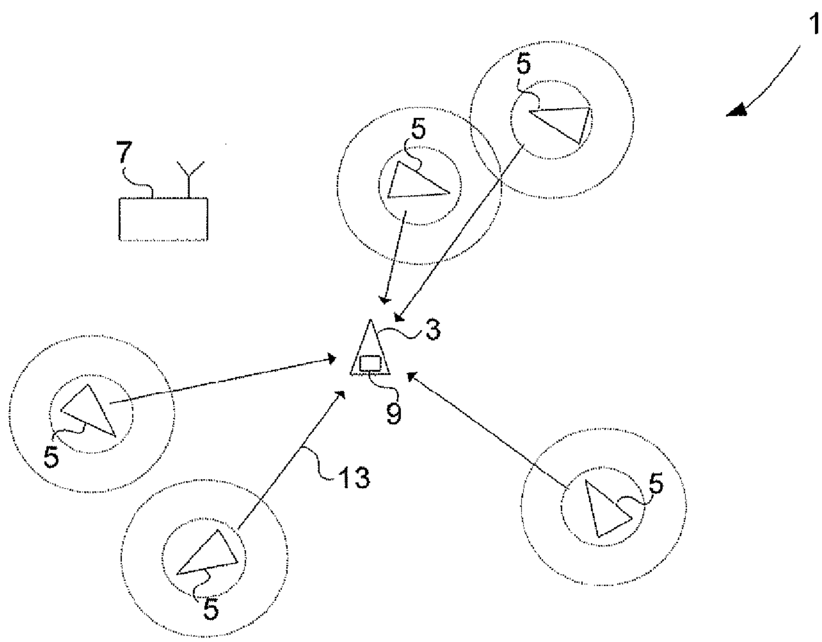


Fig. 1B

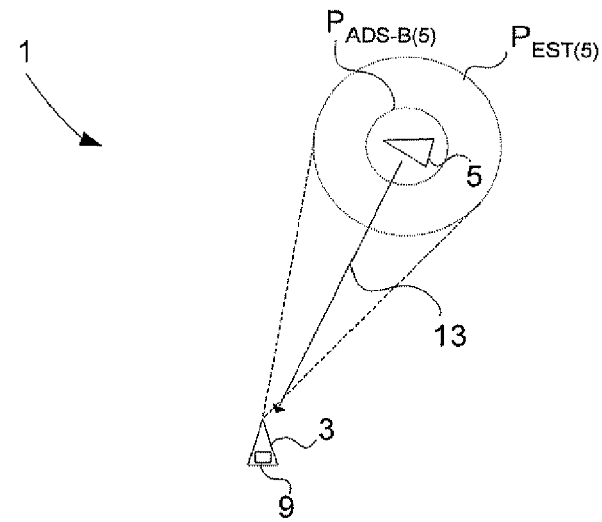

1
$P_{ADS-B(5)}$
$P_{EST(5)}$
5
13
3
9

Fig. 2A

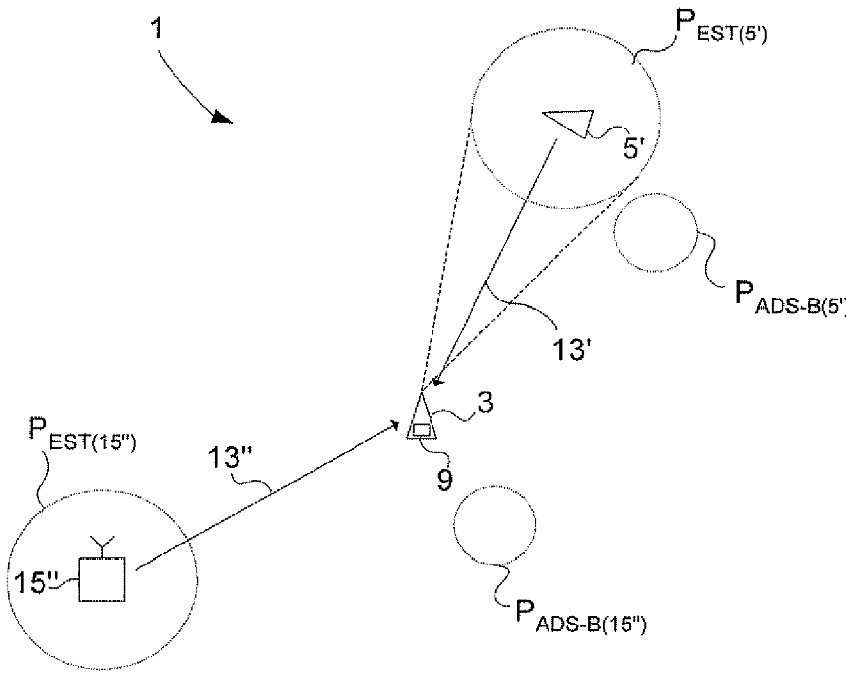

1
$P_{EST(5')}$
5'
$P_{ADS-B(5')}$
13'
3
9
$P_{EST(15'')}$
13''
15''
$P_{ADS-B(15'')}$

Fig. 2B

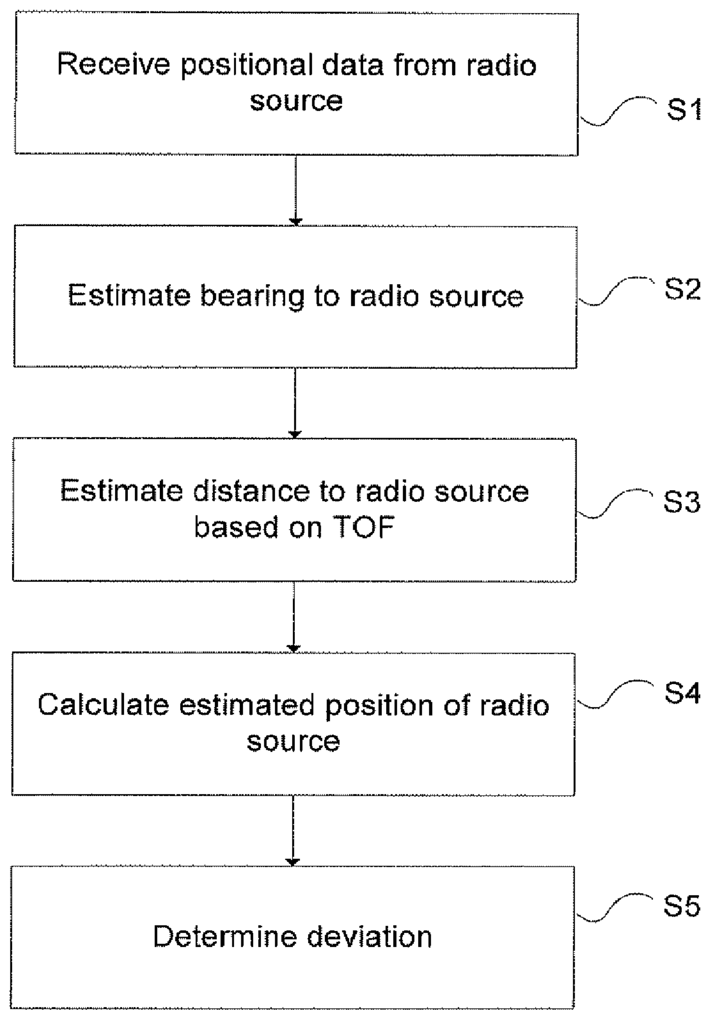

Receive positional data from radio source
S1
Estimate bearing to radio source
S2
Estimate distance to radio source based on TOF
S3
Calculate estimated position of radio source
S4
Determine deviation
S5

Fig. 3

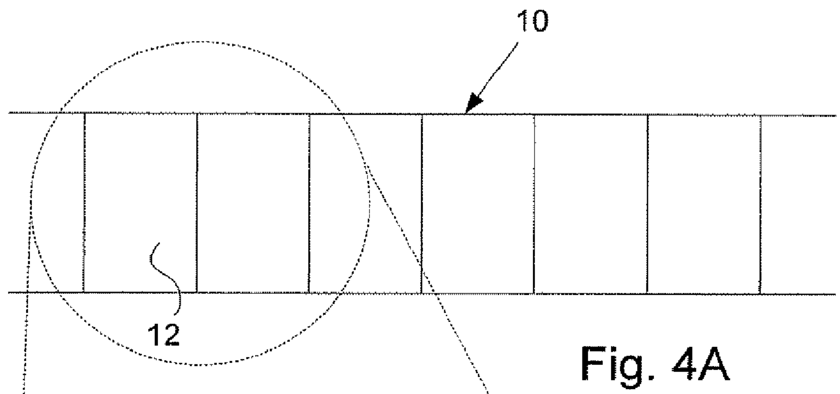


Fig. 4A

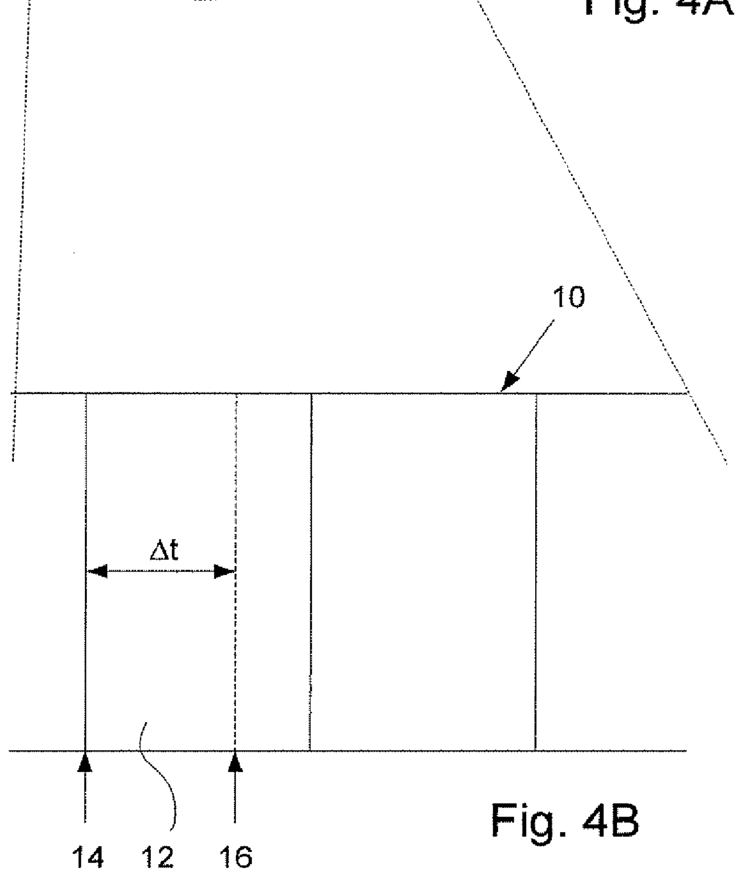


Fig. 4B

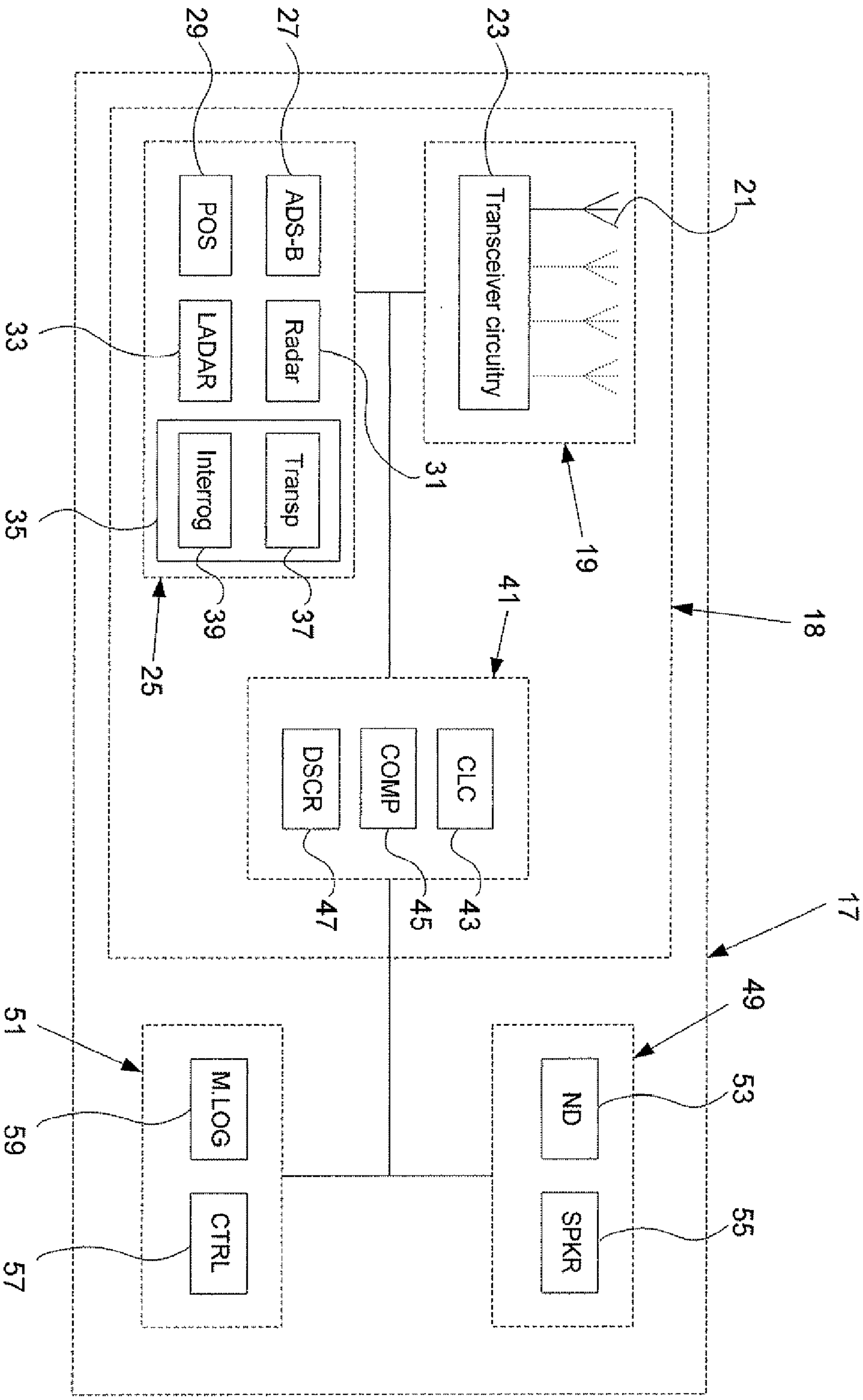

Transceiver circuitry
ADS-B
POS
Radar
LADAR
Transp
Interrog
CLC
COMP
DSCR
ND
SPKR
M.LOG
CTRL
17
18
19
21
23
25
27
29
31
33
35
37
39
41
43
45
47
49
51
53
55
57
59

Fig. 5

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 08 15 8503

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 7 116 266 B1 (VESEL ANDREW M [US] ET AL) 3 October 2006 (2006-10-03) * figures 3,4 * * column 2, lines 5-15 * * column 8, lines 9-45 * -----	1-15	INV. G01S13/76 ADD. G08G5/04
A	SPITZER, CARY R.: "Digital Avionics Handbook second edition (ISBN:0849384389)" 2007, CRC PRESS , FLORIDA USA , XP002504906 * pages 21-1, paragraph 21.2 * -----	1-15	
A	STEAD R P ET AL: "Traffic Alert and Collision Avoidance System (TCAS) transition program (TTP): a status update" DIGITAL AVIONICS SYSTEMS CONFERENCE, 1995., 14TH DASC CAMBRIDGE, MA, USA 5-9 NOV. 1995, NEW YORK, NY, USA,IEEE, US, 5 November 1995 (1995-11-05), pages 135-139, XP010154171 ISBN: 978-0-7803-3050-4 * page 135, column 1, paragraph 1 * -----	1-15	TECHNICAL FIELDS SEARCHED (IPC) G01S

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	27 November 2008	Coffa, Andrew

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 15 8503

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-11-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7116266 B1	03-10-2006	NONE	

EPC FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Electronic Code of Federal Regulations
e-CFR™

e-CFR Data is current as of October 1, 2009

Title 14: Aeronautics and Space

PART 91—GENERAL OPERATING AND FLIGHT RULES
Subpart B—Flight Rules
General

Browse Previous | Browse Next

§ 91.113 Right-of-way rules: Except water operations.

(a) *Inapplicability.* This section does not apply to the operation of an aircraft on water.

(b) *General.* When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft. When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and may not pass over, under, or ahead of it unless well clear.

(c) *In distress.* An aircraft in distress has the right-of-way over all other air traffic.

(d) *Converging.* When aircraft of the same category are converging at approximately the same altitude (except head-on, or nearly so), the aircraft to the other's right has the right-of-way. If the aircraft are of different categories—

(1) A balloon has the right-of-way over any other category of aircraft;

(2) A glider has the right-of-way over an airship, powered parachute, weight-shift-control aircraft, airplane, or rotorcraft.

(3) An airship has the right-of-way over a powered parachute, weight-shift-control aircraft, airplane, or rotorcraft.

However, an aircraft towing or refueling other aircraft has the right-of-way over all other engine-driven aircraft.

(e) *Approaching head-on.* When aircraft are approaching each other head-on, or nearly so, each pilot of each aircraft shall alter course to the right.

(f) *Overtaking.* Each aircraft that is being overtaken has the right-of-way and each pilot of an overtaking aircraft shall alter course to the right to pass well clear.

(g) *Landing.* Aircraft, while on final approach to land or while landing, have the right-of-way over other aircraft in flight or operating on the surface, except that they shall not take advantage of this rule to force an aircraft off the runway surface which has already landed and is attempting to make way for an aircraft on final approach. When two or more aircraft are approaching an airport for the purpose of landing, the aircraft at the lower altitude has the right-of-way, but it shall not take advantage of this rule to cut in front of another which is on final approach to land or to overtake that aircraft.

[Doc. No. 18334, 54 FR 34294, Aug. 18, 1989, as amended by Amdt. 91-282, 69 FR 44880, July 27, 2004]

Browse Previous | Browse Next

Electronic Code of Federal Regulations
e-CFR ™

e-CFR Data is current as of October 1, 2009

Title 14: Aeronautics and Space

PART 91—GENERAL OPERATING AND FLIGHT RULES
Subpart B—Flight Rules
General

Browse Previous | Browse Next

§ 91.115 Right-of-way rules: Water operations.

(a) *General.* Each person operating an aircraft on the water shall, insofar as possible, keep clear of all vessels and avoid impeding their navigation, and shall give way to any vessel or other aircraft that is given the right-of-way by any rule of this section.

(b) *Crossing.* When aircraft, or an aircraft and a vessel, are on crossing courses, the aircraft or vessel to the other's right has the right-of-way.

(c) *Approaching head-on.* When aircraft, or an aircraft and a vessel, are approaching head-on, or nearly so, each shall alter its course to the right to keep well clear.

(d) *Overtaking.* Each aircraft or vessel that is being overtaken has the right-of-way, and the one overtaking shall alter course to keep well clear.

(e) *Special circumstances.* When aircraft, or an aircraft and a vessel, approach so as to involve risk of collision, each aircraft or vessel shall proceed with careful regard to existing circumstances, including the limitations of the respective craft.

Browse Previous | Browse Next

Heli-Expo 2007

Gulf of Mexico Helo Ops Ready for ADS-B

Aviation Week & Space Technology
02/26/2007, page 56
Frances Fiorino
Washington

HAI members and FAA work to adapt next-gen 'backbone' in Gulf of Mexico

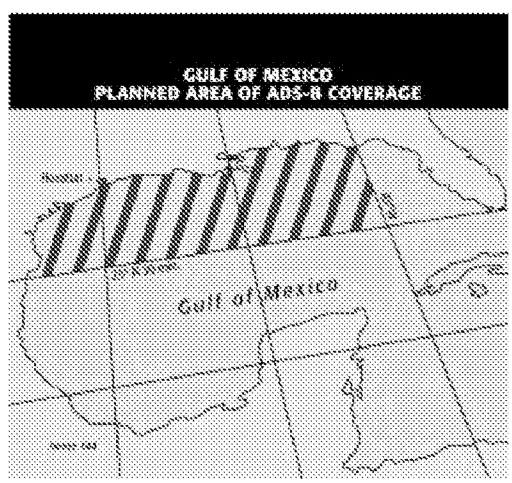
Printed headline: **Helo Ops Ready for ADS-B**

Helicopter operators are moving closer to reaping the benefits of ADS-B--a system that will "take the National Air Space and extend it out over the Gulf of Mexico."

At least that's how Vincent Capezzuto likes to describe the capability of Automatic Dependent Surveillance-Broadcast, which the FAA calls "the backbone" of the Next-Generation Air Transportation System. Capezzuto is FAA program manager for the FAA's national ADS-B office. For Gulf of Mexico operators, ADS-B means real-time ATC surveillance, communications and weather data--which, in effect, translate to conducting safe, low-altitude IFR operations in the gulf.

That's in sharp contrast to current operating conditions in the region, an area roughly 994 mi. (1,600 km.) east to west and 559 mi. from north to south, with a surface area spanning 579,153 sq. mi. Thousands of rigs offshore mine oil and gas riches round-the-clock in water with an average depth of 1,615 meters.

Approximately 650 helicopters and 2,000 pilots operate 7,500 shore-to-platform trips daily to fulfill their primary mission of ferrying personnel and equipment to thousands of platforms located about 150-200 mi. out from the Texas, Louisiana, Mississippi coastline. And all of this is accomplished while flying below 5,000 ft.



Once the flights leave the shore, "They operate in an environment devoid of the normal infrastructure found over land," says Helicopter Assn. International President Matt Zuccaro.

Radars cannot be installed on oil platforms, Capezzuto says. "It's a very harsh environment. Electromechanical devices don't like the salt water."

And Houston Center, which provides coverage of what is now classified as Oceanic airspace, can't see or talk to the helicopter operators--and as a result cannot provide direct surveillance, adds Zuccaro. Nor can pilots obtain real-time weather services.

But that will change. Under a May 2006 Memorandum of Agreement (MOA) with the FAA, the Gulf region, Louisville, Ky., Juneau, Alaska, and Philadelphia were selected to participate in "Segment One" ADS-B implementation. This involves initial installation of ground infrastructure that will support the system--and for which the FAA requested $80 million in the Fiscal 2007 budget.

Implementation committees are now assessing ground infrastructure and equipment and fielding of services. Zuccaro says the first platform site, conducted this month, was successful. Certain oil platforms will house ADS-B receivers. Under ADS-B , satellites provide GPS information to the aircraft avionics, which emit the data to ground-based receivers. Then these would couple the information to shore--in this case, Houston Center controller automation platforms. Eventually, weather-sensing devices will be installed on the platforms.

By the end of 2010, FAA expects to have the ADS-B system tested and operationally acceptable for the NAS, with Houston Center providing services in the Gulf region. By 2013, all of the U.S. is scheduled to be covered with ground infrastructure.

The avionics installation will take longer, says Capezzuto, because we will be dealing with a larger aircraft population--20,000 or more general aircraft and about 35,000 transport aircraft, all of which will have to be retro- or forward-fitted with ADS-B equipment (AW&ST Feb. 17, 2006, p. 52).

Subsequent program phases include HAI members voluntarily equipping aircraft with traffic display capability so pilots can self-separate from other aircraft. This ability, according to Capezzuto, leads to shared pilot-controller situational awareness, and therefore enhanced safety.

"The Gulf is probably the perfect implementation area for ADS-B. It's a clean slate. There's nothing down there," says Zuccaro. "Segment One is 'the true test' of ADS-B implementation in an area without support or infrastructure."

The Gulf of Mexico's area of coverage will extend to 25 deg. N. Lat. in the Gulf (see map). In about 5-10 years, it will extend to 26 deg. N. Lat., based on planned expansion of oil platform infrastructure, according to the FAA.

Zuccaro says that in the next decade activities in the gulf are expected to grow 25%, move into deeper water and extend toward the Florida coastline.

"This is a win-win situation for all stakeholders," says Capezzuto. "The operators not only get [ADS-B] service, [they also] provide FAA with data required to validate the service and get it certified."

ADS-B's precision is also seen as a way to improve capacity in the future NAS via streamlining separation standards. "Today's established standards--3 mi. to terminal and 5 mi. en route--are based on the traditional radars' infrastructure," says Capezzuto. "The reality is, everyone puts a little buffer around it . . . and the FAA is interested in removing those buffers. Its hope is to project forward as air traffic increases and start looking at reducing those separation standards," he says.

To accomplish that wouldn't require more air traffic controllers, Capezzuto says. Rather, ADS-B would increase situational awareness of pilots by putting information in the cockpit, and controllers can then shift more toward air traffic management function.

The nation's more crowded airspace of the future could and would be kept safe under current infrastructure, but ATC would not be able to accommodate traffic at the times airlines want to fly, says Capezzuto. And the Next-Gen system must be able to handle future growth.

Under the MOA, the FAA will fund, install and operate the ADS-B network in the gulf. The helicopter industry and platform operators will prove platform space for installation of system equipment. HAI's efforts in a 20-year period to provide transportation of personnel to the platform, along with power and telecommunications as well as the voluntary installation of the avionics equipment for their IFR fleet, is valued at more than $100 million.

The minimum equipment required on the aircraft would be a transmitter, which would allow ATC to "see" and control the aircraft. The next upgrade, the display unit, would open up available uplink data so pilots can visually monitor traffic on the panel and self-separate. When that will occur will depend on the completion of the evaluation of transmitters and equipment operation.

Louisville, Philadelphia and Juneau were selected for Segment One because they all pose a unique set of problems. Each Tracon or Center has different computer interfaces with the NAS, which would require the FAA to build and test new infrastructure to interface with various automation platforms.

The challenge at Philadelphia, a UPS hub, is in validating ADS-B within terminal airspace that has a high RF interference environment. The New York-Philadelphia region is rife with various types of radars and other devices that emit RF energy, says Capezzuto.

Louisville, UPS's main hub, is a "petri dish" in which the FAA will validate separation standards involving a large number of UPS aircraft operating within certain timeframes, similar to most major hubs.

Juneau offers the challenge of a mixture of equipment including multiple types of transponder devices, not to mention robust mountainous areas where radars are especially challenged.

Some general aviation sectors are exercising caution in fully embracing ADS-B. The National Business Aviation Assn. is in support of the system, but wants the FAA to set a firm plan for certification of equipment. The Aircraft Owners and Pilots Assn. also supports implementation of ADS-B, but is concerned about the affordability of equipment.

Sensing Requirements for Unmanned Air Vehicles

Engineers develop requirements and metrics to ensure integration of future autonomous unmanned aircraft into manned airspace.

AFRL's Air Vehicles Directorate, Control Sciences Division, Systems Development Branch, Wright-Patterson AFB OH

Engineers from the Air Vehicles Directorate transferred unmanned air vehicle (UAV) sensing system requirements for airspace operations to civilian UAV users and developers. These requirements represent design goals on which to base future sensing subsystem designs, filling an omission in UAV technology planning. Directorate engineers are continuing to develop the technologies that will enable future UAVs to coexist with manned aircraft in both military and civilian airspace. Incorporating these requirements will ensure that engineers design future UAVs to detect possible conflicts, such as midair collisions or runway incursions, and take action to avoid them.

Present UAVs cannot detect manned aircraft and conflict situations and, therefore, they cannot share airspace with manned aircraft. To overcome this obstacle, UAVs need to sense the presence of other aircraft in their operating environment (see figure on next page). In other words, UAVs need to at least replicate a human pilot' s ability to see and avoid problems before they will be accepted into the national air space (NAS). Since some aircraft do not have air traffic transponders, UAVs must use onboard sensors to detect aircraft and coordinate that information with available transponder information. With this level of capability, UAVs and operators will have the situational awareness of the airspace around the vehicle to ensure safety at the same level as manned aircraft.

With this goal in mind, directorate engineers worked with Northrop Grumman Corporation (NGC) engineers to establish, iterate, and finalize sensing system performance requirements for the broad range of future Air Force missions. During this collaborative process, directorate engineers noted that many mission elements were similar to civilian airspace operations tasks, and that the requirements they were developing were directly applicable to civilian UAV technology. They also found no report that defined and expressed these requirements for nonmilitary use. To help fill this void, directorate engineers coordinated their research results with the American Institute for Aeronautics and Astronautics UAV airspace operations' focal point, North Atlantic Treaty Organization' s Standards Committees, the National Aeronautics and Space Administration, and industry organizations working the same topics from the civilian side. Incorporation of the directorate' s technology into civilian requirements' definitions and standards will directly impact airspace operations' sensing systems for current and future UAVs.

The coordinated effort of directorate and NGC engineers that resulted in the sensing system requirements represents the first stage of work on the Autonomous Flight Control Sensing Technology (AFCST) program. This program' s long-term goal is to develop the upfront portion of the UAV virtual pilot capability. During this first phase, NGC engineers analyzed midair and near-midair collision data, along with runway incursion data, to generate lessons learned. Then, the NGC engineers combined the lessons learned from aircraft mishap data with sensing performance specifications and good engineering judgment to establish conventions for operating aircraft in the NAS. Next, they examined airspace tasks for operation in NAS and grouped them into deconfliction, collision avoidance, autonomous landing, and ground operations. The UAV functional requirements resulting from this effort are shown in the table.

As shown in the table, the threshold values represent the nearterm requirements (year 2007), while objective values are far-term requirements (year 2013). Engineers consider the forward vision threshold values equivalent to or slightly better than human performance. Federal Aviation Administration data indicates the dominant cause for midair collision is when an aircraft is overtaken by a faster aircraft because a pilot' s position in the cockpit limits rear visibility. In the UAV, rear visibility is not restricted because designers can locate sensors anywhere on the aircraft. Objective values contain UAV rear vision capability to improve safety in this scenario.

Directorate and NGC engineers are currently working on the second phase of AFCST– the preliminary design of the sensor hardware architecture. The AFCST design strategy for all UAV situational awareness functions is to minimize hardware and software quantity and maximize use of multifunction sensors and common image processing software components. Most of the design efforts are completed satisfactorily. NGC engineers are continuing detailed sensor reliability analyses, capturing the individual and combined effects of sensor field-of-view coverage, sensor failure rates, and exposure rates.

During the final stage of the AFCST program, engineers will run simulations emphasizing landing and collision avoidance-tasks with demanding sensing and processing requirements. The engineers will develop landing and see-and-avoid strategies of operation as well as a detailed software architecture design. The simulations should determine if the preferred electrooptic/ infrared and radar sensors meet the specifications identified in the first phase of the AFCST program and the number of false alarms and false negatives that will be encountered. The engineers will also compare various image-processing solutions to determine the most reliable. The ideal system design will be free of nuisance faults caused by system error and will include software designed to minimize such faults. Reliability analysis studies will eventually combine software reliabilities with hardware reliabilities to meet the overall UAV system reliability.

In the near future, directorate and NGC engineers plan to publish the results of the detailed sensor reliability analysis. Program managers are also planning a follow-on hardware-in-the-loop simulation effort to address and demonstrate the integrated system design. In this realistic simulation, engineers will study concepts such as the integration of AFCST sensors with instrument flight rules avionics for see-and-avoid maneuvers, landing, and automated traffic collision avoidance. Real-time simulation will stress the detailed sensor architecture design, allowing the engineers to assess its adequacy and determine its readiness for technology transition to flight test. These efforts will ensure the safe incorporation of UAVs into the NAS.

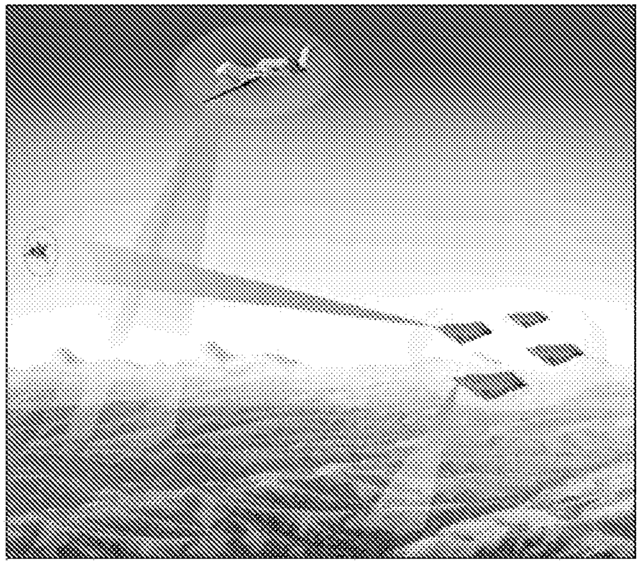


Figure. UAV senses presence of other aircraft

AIRSPACE OPERATIONS SENSING REQUIREMENTS FOR UAVs		
Functional Requirements	Threshold Values	Objective Values
Field of View	Azimuth: 60° Elevation: 30°	4 π steradians
Field of Regard	Azimuth: +/-100° Elevation: +30°, -90°	4 π steradians
Ranging	0.5 ft CEP* @ 100 ft 700 ft CEP* @ 6 nm	0.25 ft CEP* @ 100 ft 770 ft CEP* @ 13.2 nm
Imaging	Varies from 30 ft to 3 nm	Varies from 30 ft to 13.2 nm
Data Rate	30 Hz	60 Hz
Weather Capability	Visual Meteorological Capability	Visual and Instrument Meteorological Capability
Criticality	Safety Critical	Safety Critical
Emission Constraints	Various Federal Aviation Administration Limitations	Various Federal Aviation Administration Limitations
	*CEP = circular error probability	

Table. Near- and far-term UAV sensing requirement

Mr. Tom Molnar and Mr. Bruce Clough, of the Air Force Research Laborator y' s Air Vehicles Directorate, and Mr. Won-Zon Chen, of Northrop Grumman Corporation, wrote this article. For more information contact TECH CONNECT at (800) 203-6451 or place a request at http://www.afrl.af.mil/techconn/index.htm. Reference document VA-03-06

DISTRIBUTION A
PUBLIC RELEASE

Developing Sense & Avoid Requirements for Meeting an Equivalent Level of Safety

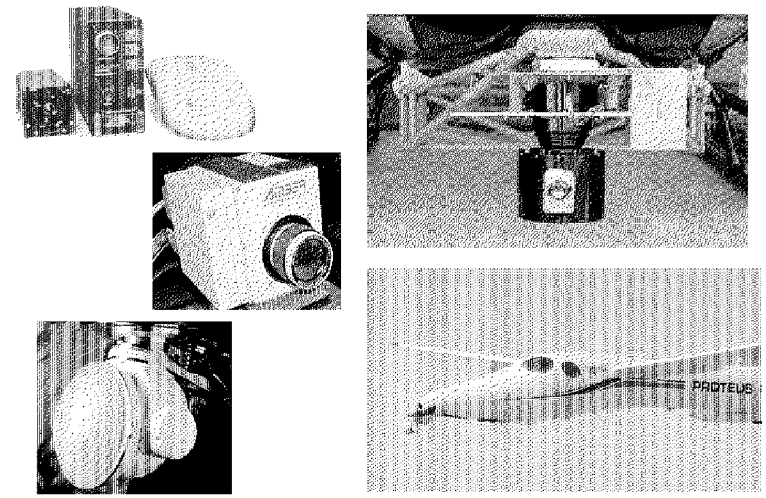
UVS Tech 2006
Salon-de-Provence, France
17-19 January 2006

Presenter: Russell Wolfe
Access 5 Technology IPT Lead
Modern Technology Solutions, Inc

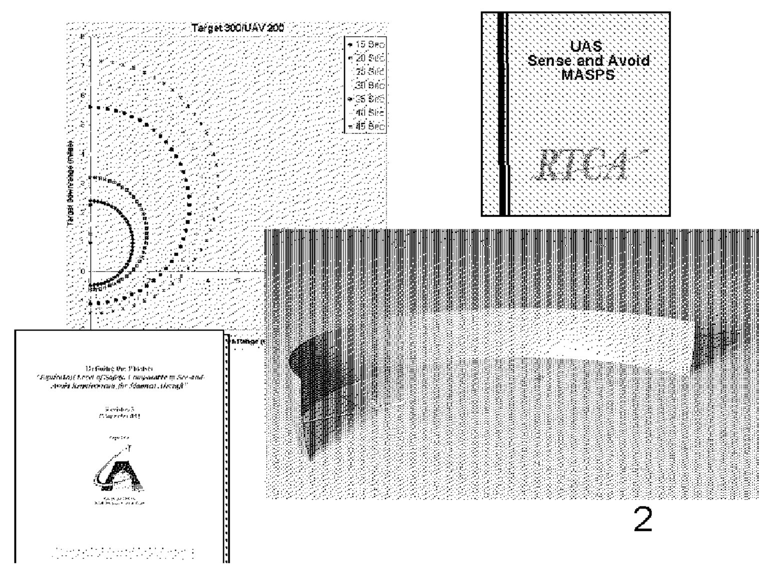
UAS Collision Avoidance Initiatives

NASA Dryden Flight Research Center

- ERAST: 1993 - 2003
  - Sensor Requirements
  - Sensor Concept Development
  - Flight Test Demonstrations
    - Cooperative
    - EO / IR
    - Radar

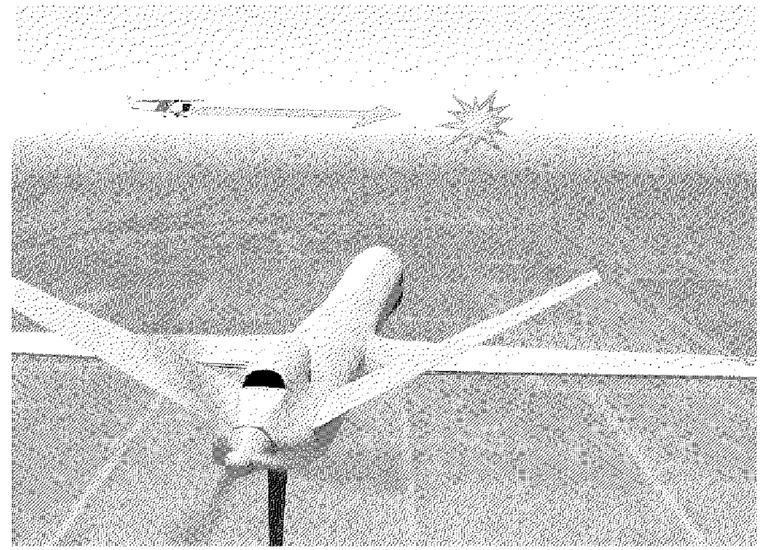


- ACCESS 5: 2004 - present
  - Requirements Development
  - Safety Analysis
  - Simulation Tools
  - Flight Test Demonstrations
  - Standards Development



ACCESS 5
Collision Avoidance Work Package

- Work Package Objectives:
  - Define Equivalent Level of Safety (ELOS) for Sense and Avoid.
  - Develop collision avoidance (CA) requirements for Unmanned Aircraft Systems (UAS); validated through analysis, simulation, and flight demonstration.
  - Provide inputs to the FAA and RTCA Special Committee 203 "Unmanned Aircraft Systems"

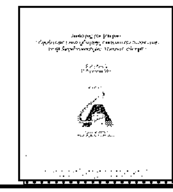


- Team Members:
  - NASA Dryden & Langley
  - Northrop Grumman
  - Lockheed Martin (Ft. Worth)
  - MITRE
  - Modern Technology Solutions
  - Aurora Flight Sciences
  - Federal Aviation Administration

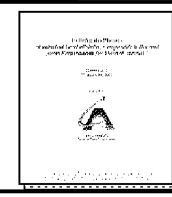
ACCESS 5 Collision Avoidance Work Package

5 Major Task Areas

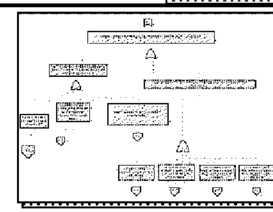
– CA Task 1: **Define ELOS for See & Avoid**



– CA Task 2: **Develop CA Requirements**

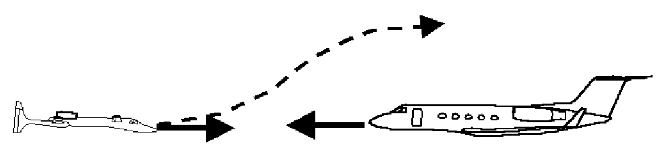


– CA Task 3: **Perform CA Safety Analysis**



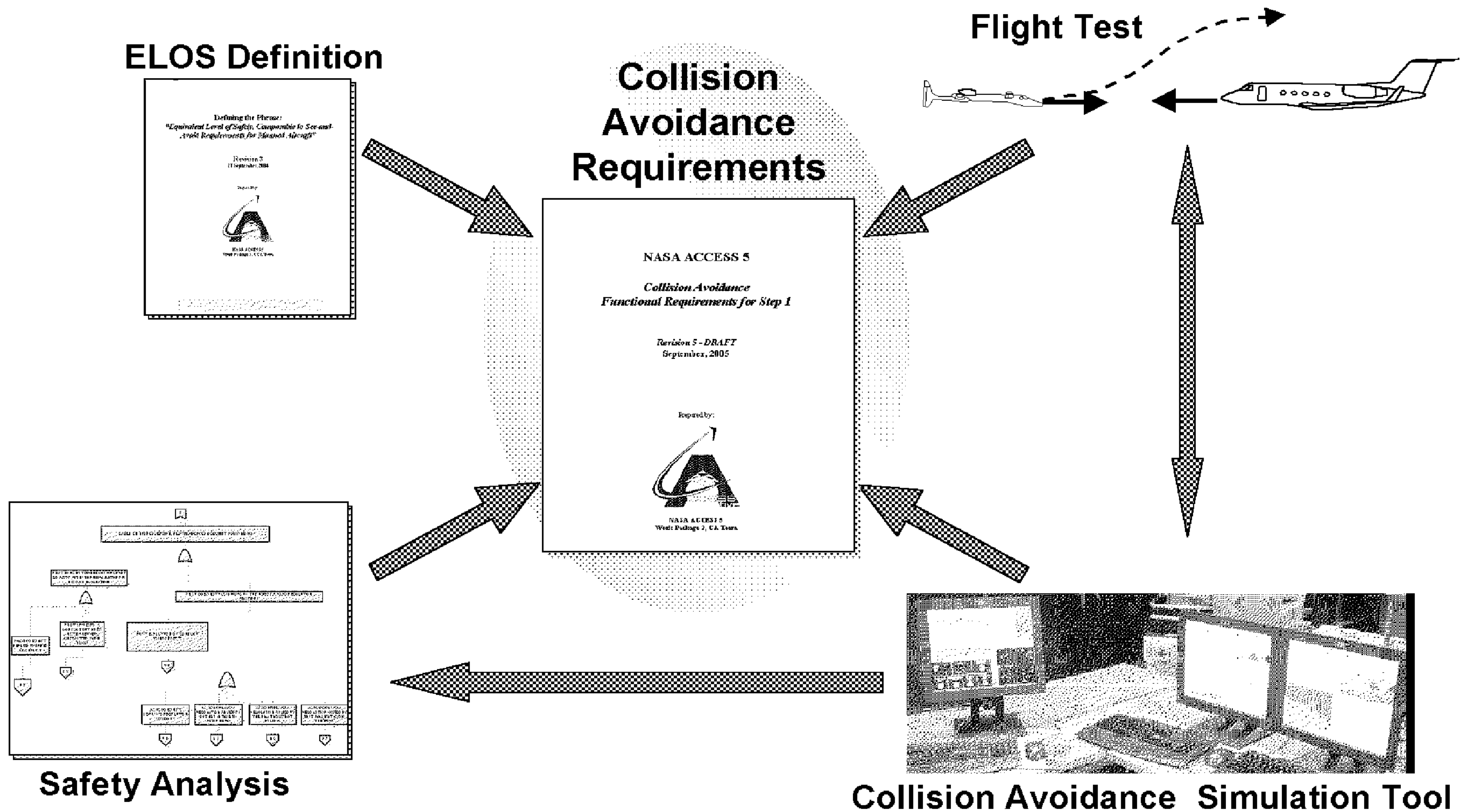
– CA Task 4: **Develop CA Simulation Tool**

– CA Task 5: **Perform CA Flight Test**



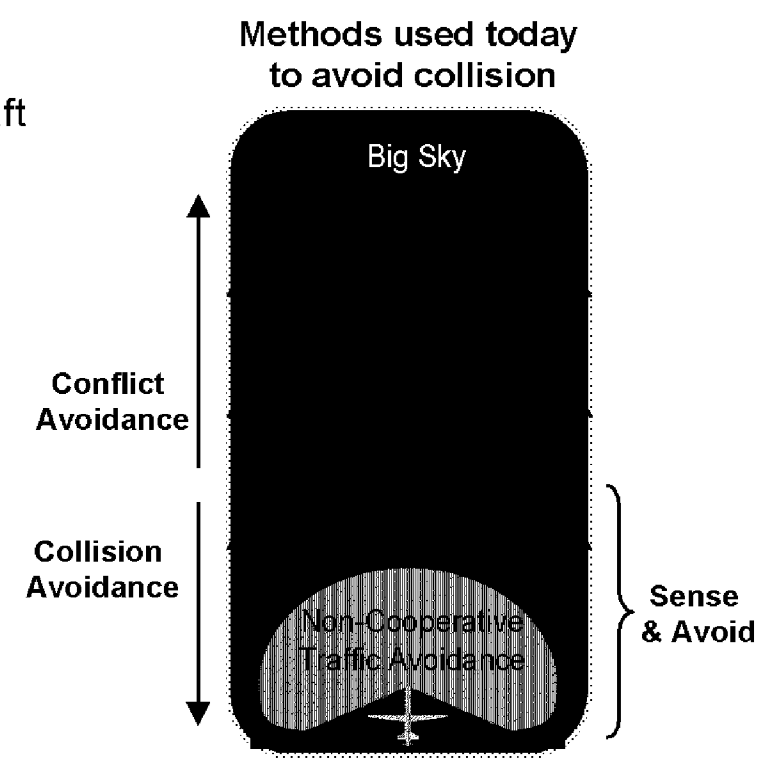
Collision Avoidance Work Package

Task Relationships



Task 1: ELOS Definition Document

- Objective: To present a recommended approach for defining an equivalent level of safety, as it pertains to see and avoid.
- Deliverable Content:
  - Current regulatory / operational environment
    - 14 CFR 91.113(b), Right of Way Rules
    - 14 CFR 91.111, Operating near other aircraft
  - Basis for having to meet an Equivalent Level of Safety
    - 14 CFR 21.21(b), Certification Procedures
    - FAA Order 8110.4C, Equivalent Level of Safety Findings
  - Potential Approaches & Methodologies for defining ELOS
    - 1) Statistical Approach
    - 2) Performance / Rule Based Approach
  - Recommended Definition and Measures of Performance for Sense and Avoid ELOS



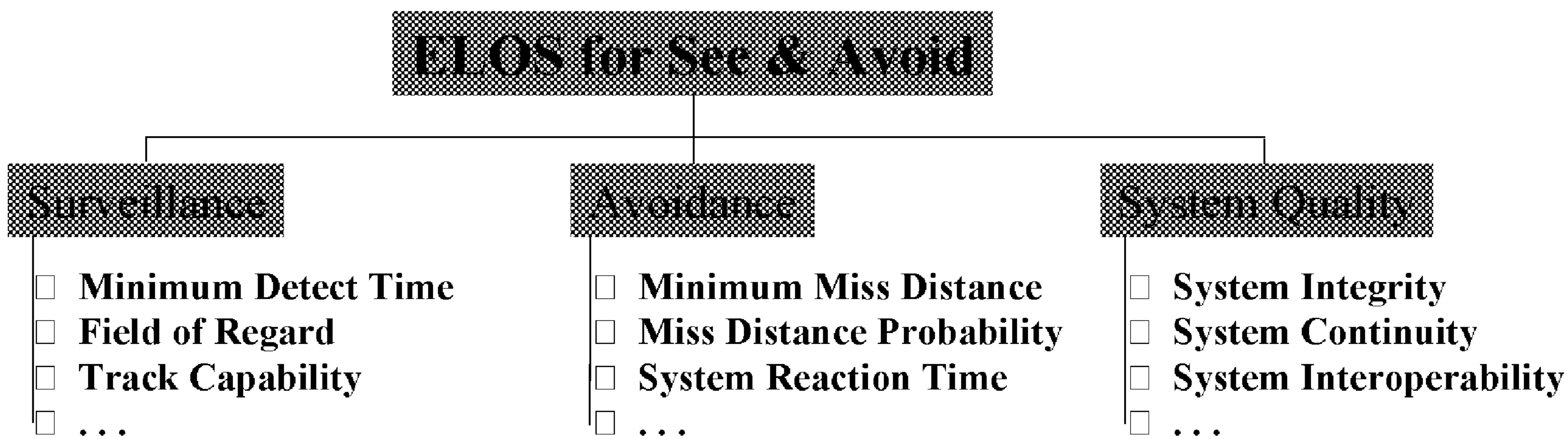
- Status: Delivered to FAA on 23 Nov 2004

Task 1: ELOS Definition Document

Definition and Measures of Performance

- Definition: *"Equivalent level of safety to manned aircraft see-and-avoid" is the capability to provide situational awareness with adequate time to detect conflicting traffic and the ability to take the appropriate action necessary to avoid collisions."*

- Measures of Performance:



Task 2: Develop Collision Avoidance Reqmts

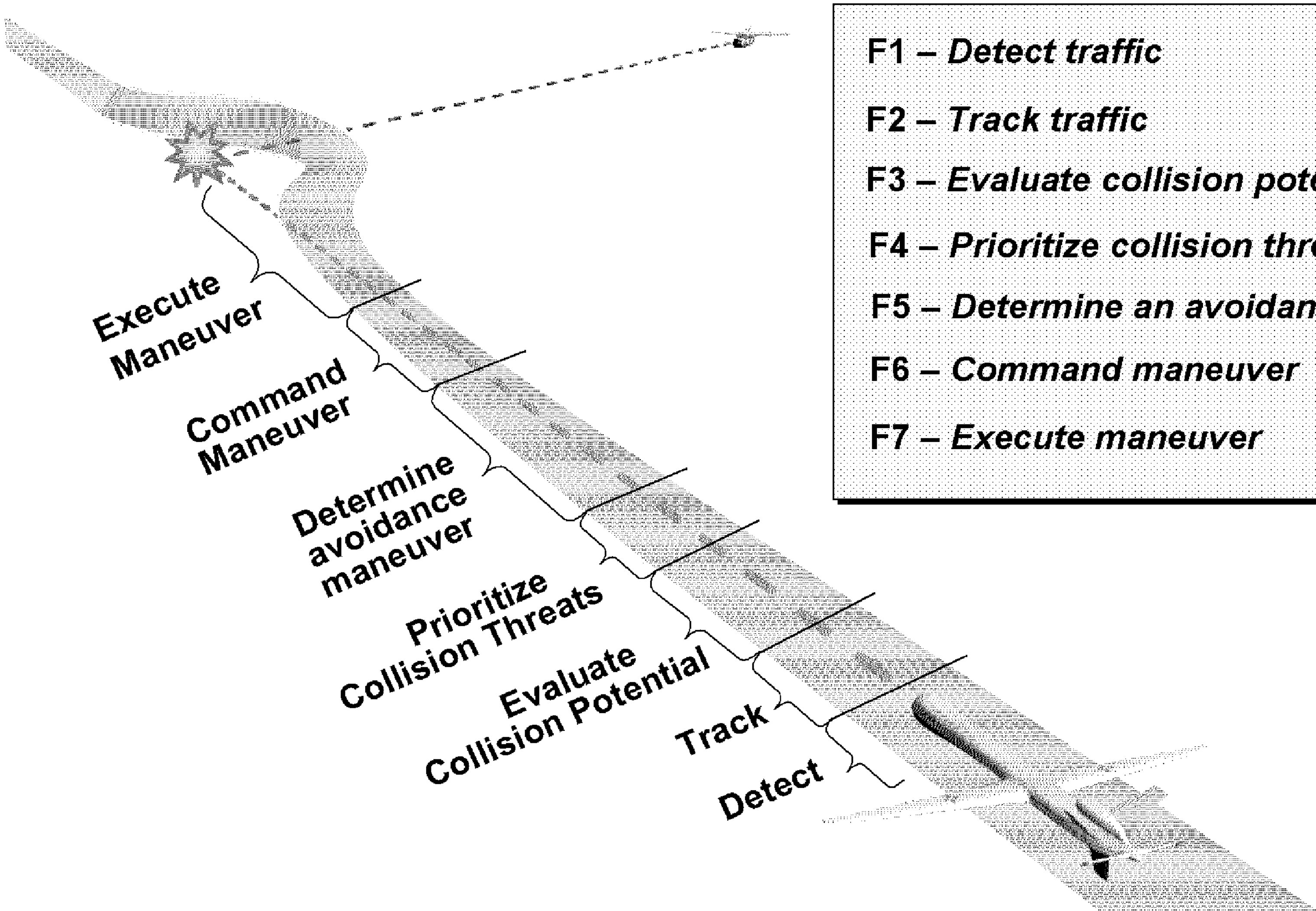
- Objective: To develop the collision avoidance operational, functional, and performance requirements for HALE UAS.

- Deliverable Content:
  - Notional CA Subsystem Description
    - Subsystem Architecture
    - Interfaces
  - Operational Requirements
  - Functional Analysis
    - List of Collision Avoidance Functions
    - Functional Flow Block Diagram
    - Functional Requirements
  - Performance Requirements
    - Design Guidelines
    - Performance Trade-offs
  - Verification Method (Analysis, Inspection, Simulation/Modeling, Demo, Test)

- Status: Intend to release Revision 6.0 in February 2006
  (All previous revisions have included FAA input and review)

Task 2: Develop Collision Avoidance Reqmts

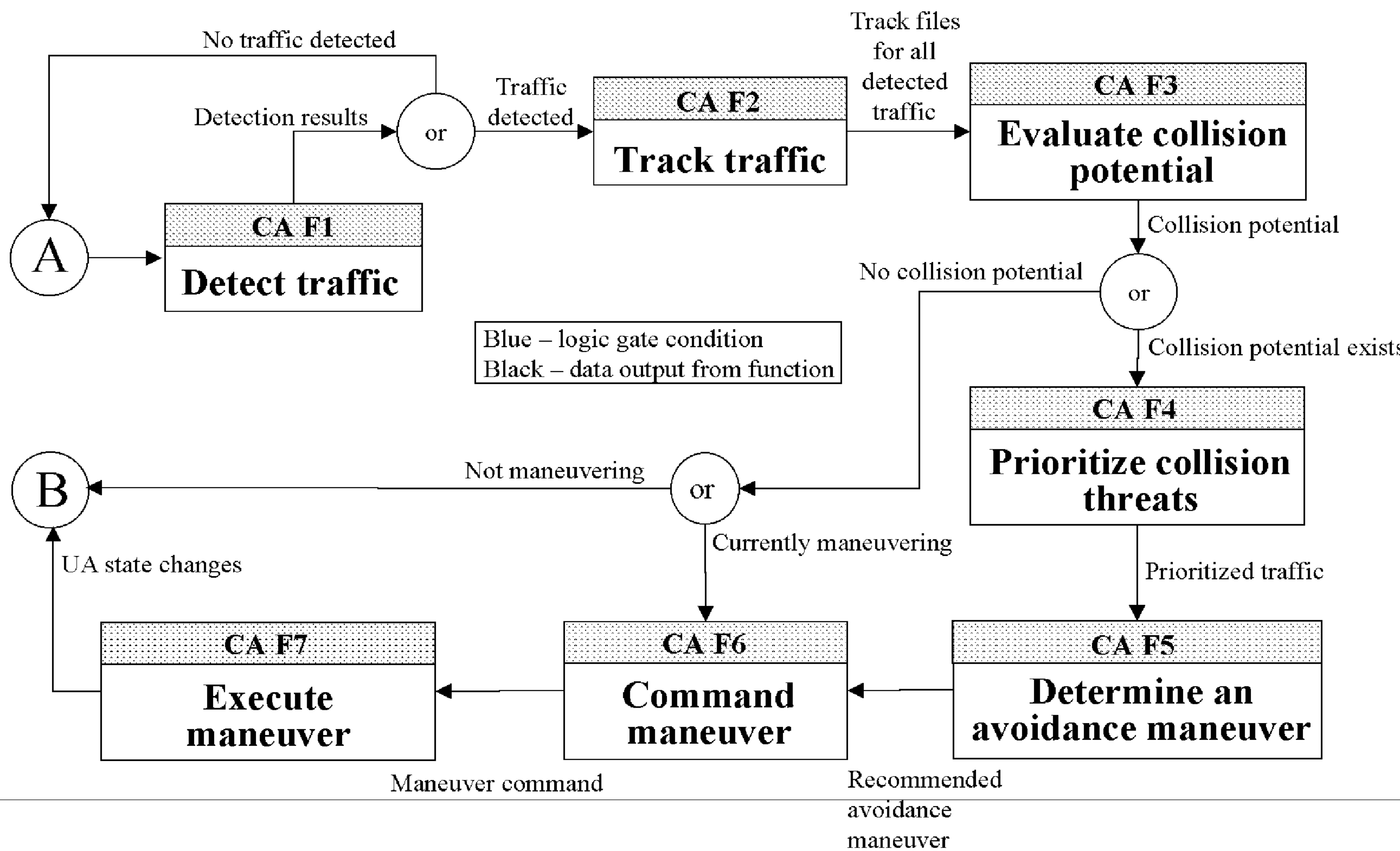
Collision Avoidance Functions



- F1 – ***Detect traffic***
- F2 – ***Track traffic***
- F3 – ***Evaluate collision potential***
- F4 – ***Prioritize collision threats***
- F5 – ***Determine an avoidance maneuver***
- F6 – ***Command maneuver***
- F7 – ***Execute maneuver***

Task 2: Develop Collision Avoidance Reqmts

Functional Flow Block Diagram



Task 2: Develop Collision Avoidance Reqmts

Function 1: Detect Traffic Requirements (Example)

- **F1: Detect Traffic - The UAS shall detect traffic within its surveillance volume.**
  - **F1.1: Minimum Detect Time** - The CAS shall detect traffic with sufficient time remaining for successful performance of all required collision avoidance functions.
  - **F1.2: Detection Range** - The CAS shall detect cooperative traffic at a range of at least xx nautical miles. (*see Table F1.2*)
  - **F1.3: Azimuth Field of Regard** - The CAS shall detect cooperative traffic within an azimuth FOR of at least +/-110° referenced from the flight path of the UA.
  - **F1.4: Elevation Field of Regard** - The CAS shall detect cooperative traffic within an elevation FOR of at least +/-15° referenced from the flight path of the UA.
  - **F1.5: Detection Probability** - The CAS shall detect cooperative traffic in the surveillance volume at a rate that supports the track probability guideline (*see F2.3*).
  - **F1.6: Detection Rate** - The average CAS detection rate shall be equal to or greater than xx hertz. (*see Table F1.6*)
  - **F1.7: Detection Accuracy** - The CAS shall detect cooperative traffic with an accuracy of TBD ft for range determinations, and TBD ft for altitude determinations
  - **F1.8: False Detection/Nuisance** - False detections shall account for less than TBD% of all detected traffic.

Task 3: Perform Safety Analysis

- Objective: To develop a method for evaluating the safety of collision avoidance for UAS.
  - Establish equivalent level of safety to manned aircraft using event/fault trees and logic risk ratios

$$\text{Risk Ratio} = \frac{P(\text{collision UAS})}{P(\text{collision manned AC})} \leq 1$$

- Accomplishments:
  - Developed visual acquisition model based on Lincoln Lab's SEE1 model
  - Developed surveillance error models for GPS/ADS-B
  - Performed multiple assessments using results from the CA simulation tool for the primary event tree probabilities.
  - Supported requirements development in the areas of Surveillance, Effectiveness, Detection Accuracies, Detection times, Reaction times, Maneuver times, etc.

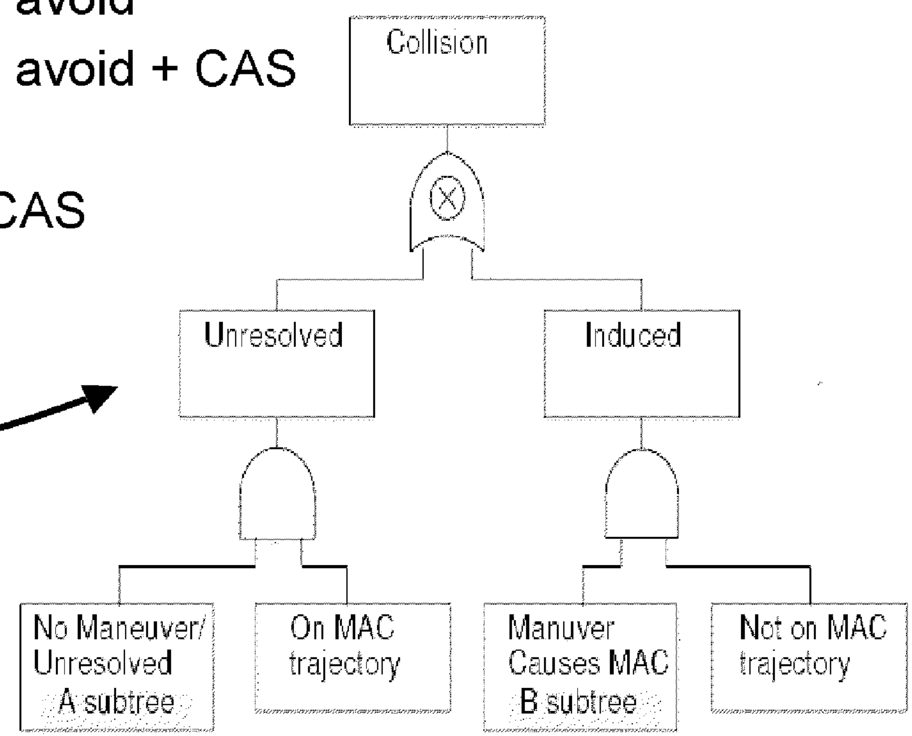
- Status: Currently finalizing final report and lessons learned

Task 3: Perform Safety Analysis

Generic Event/Fault Tree for Collision Probability Estimation

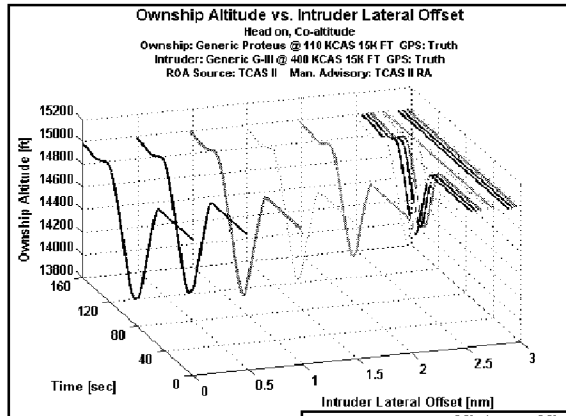
- Generic Event/Fault Tree established to provide a consistent basis for comparison:
  - 1. Manned aircraft using see & avoid
  - 2. Manned aircraft using see & avoid + CAS
  - 3. UAS with Sense & Avoid
  - 4. UAS with Sense & Avoid + CAS

Simplified Fault Tree
(actual tree is several pages long)

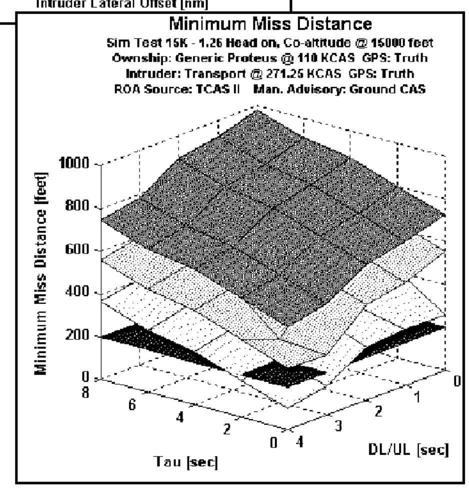


Task 4: Develop CA Simulation Tool

- Objective: To assess the validity of the proposed CA Functional Requirements via Simulation as well as support the CA Flight Test activities.
  - Allows characterization of:
    - Ownship Vehicle Dynamics
    - CA Equipment and Software
    - Encounter Scenarios



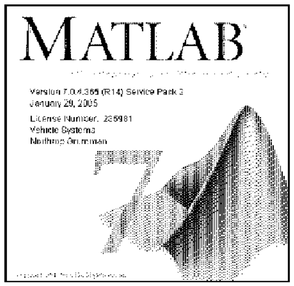
- Accomplishments:
  - Duplicated Tech Demo Scenarios
    - Flight Test Risk Reduction
    - Improve Probability of Obtaining Useful Data
  - Validated Against the System Integration Lab (SIL)
    - Flight Test Risk Reduction
    - CCA Component Models
  - Sensitivity Analyses performed



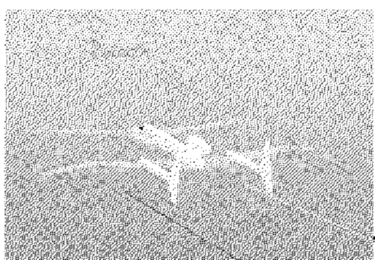
- Status: Currently analyzing flight test data and validating the CA simulation tool.

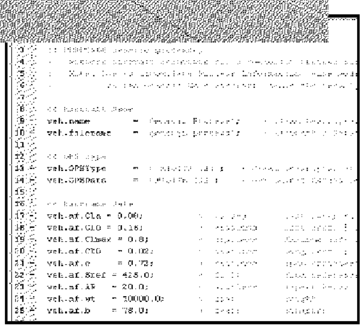
Task 4: Develop CA Simulation Tool

Simulation Features



- MATLAB™/Simulink® Simulation Environment
- Multi-Vehicle Simulation (4 Aircraft Max)
- Generic Aircraft Models Represent Any Fixed Wing Aircraft
  - Each Aircraft = 1 Parameter File
  - Scripts Trim & Initialize Aircraft to Any Encounter Geometry



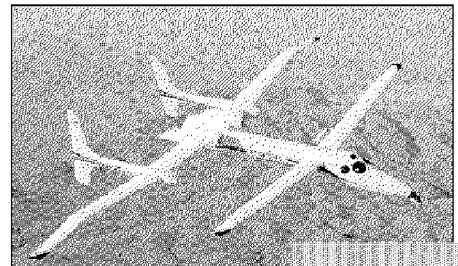


- Modular Components
  - Blocks Can be Copied and/or Swapped Out for Software Upgrades (e.g. CA Sensors, Maneuver Advisory)
- Capable of Batch Runs for Parametric Variation Studies
  - Uses Microsoft Excel Input Dataset
  - Multiple Plot Outputs Available
- PC Portable (< 37 MB)
- Can Run in Both Fast Sim-Time & Soft Real-Time

Task 5: Perform CA Flight Test

- Objective: To collect cooperative collision avoidance data to validate the CA simulation tool

OPV - Proteus



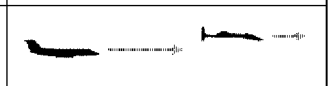
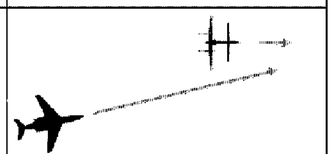
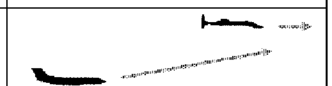
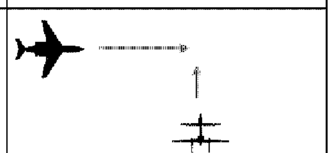
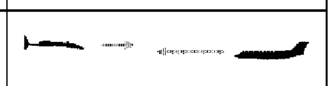
Intruder – Gulfstream III

- Accomplishments:
  - Developed Interface Control Document
  - Developed System Integration Lab (SIL)
  - Developed CA algorithms
  - Developed CA software and human interface tool
  - Procured CA sensors and integrated them onto Proteus platform
  - Developed CA scenarios and test cards
  - Post-processed flight data and prepared for data analysis effort

- Status: Successfully completed over 50 collision scenarios during the last two weeks of September 2005.

Task 5: Perform CA Flight Test

Test Scenarios

	HOST	INTRUDER		PICTORIAL
Scenario #	Climb Rate (fpm)	Δψ (degrees)	Climb Rate (fpm)	
1	0	0	0	
2	0	10	0	
3	0	0	500	
4	0	-90	0	
5	0	180	0	
6	-500	180	0	

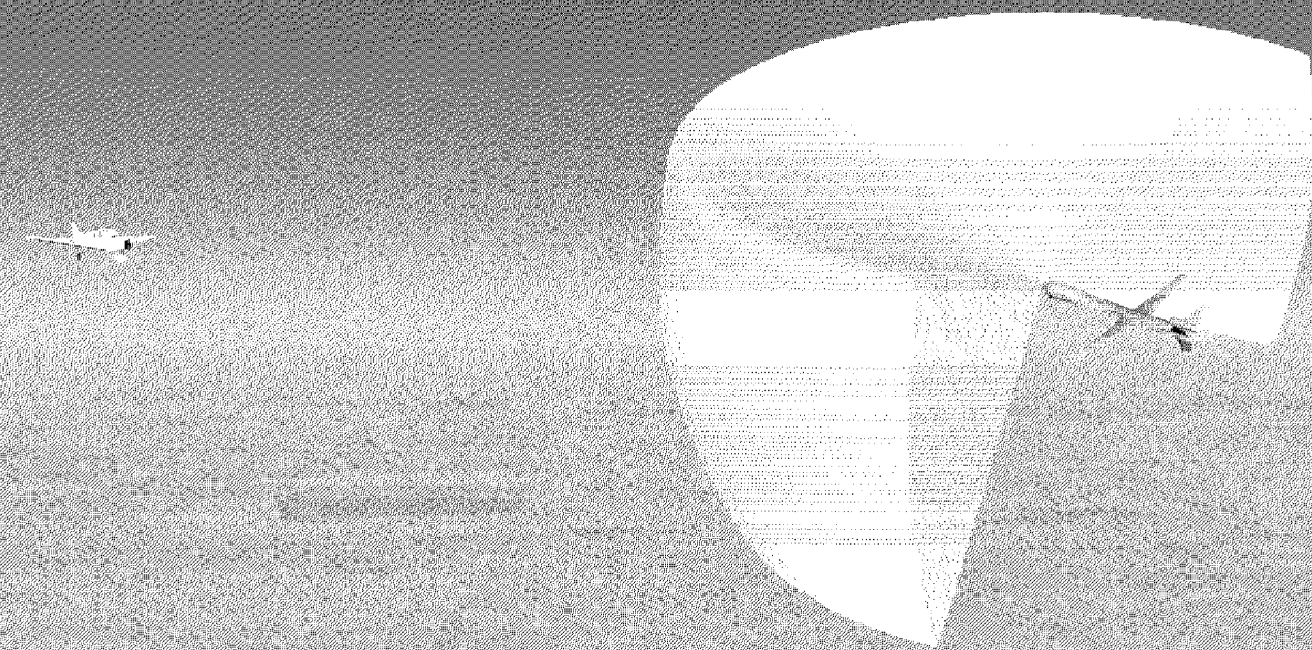
- Test scenarios included multiple collision geometries:
  - Co heading, Intruder overtaking
  - Low aspect, co-altitude
  - Co heading, Intruder climbing
  - Abeam, co-altitude
  - Head-on, co-altitude
  - Head-on, descending

	Configuration						
	TGC & AGA					TRT	
Buffer	6	4	2	0	4	0	0
Link Delay	0	0	0	0	2	0	2
Scenario							
1. Co-Heading, Co-Alt, Intruder Overtaking				1		2	
2. Low Aspect, Co-Alt				1		2	
3. Co-Heading, Intruder Climbing				1		2	
4. Abeam, Co-Alt	1	1	1	2	1	1	1
5. Head-On, Co-Alt	1	1	1	2	1	1	1
6. Head-On, Descending	1	1	1	2	1	1	1

Next Steps

- Document the results and lessons learned from the Safety Analysis and Flight Test Activities
- Complete validating the CA Simulation tool
- Derive practical values/ranges for the TBDs in the performance requirements
  - Utilize the validated CA Simulation tool
  - Utilize the safety analysis results
- Begin Non-cooperative Collision Avoidance Activities
  - Derive unique Non-cooperative performance requirements
  - Perform Trade Studies and Concept Assessments
  - Conduct Non-cooperative Simulation Runs and Flight Demos
- Support RTCA SC-203 on developing the Sense & Avoid Minimum Aviation System Performance Standards (MASPS)

QUESTIONS ?



MTSI

Russell Wolfe
Modern Technology Solutions, Inc.
Russell.C.Wolfe @mtsi-va.com
(703) 212-8870 x126

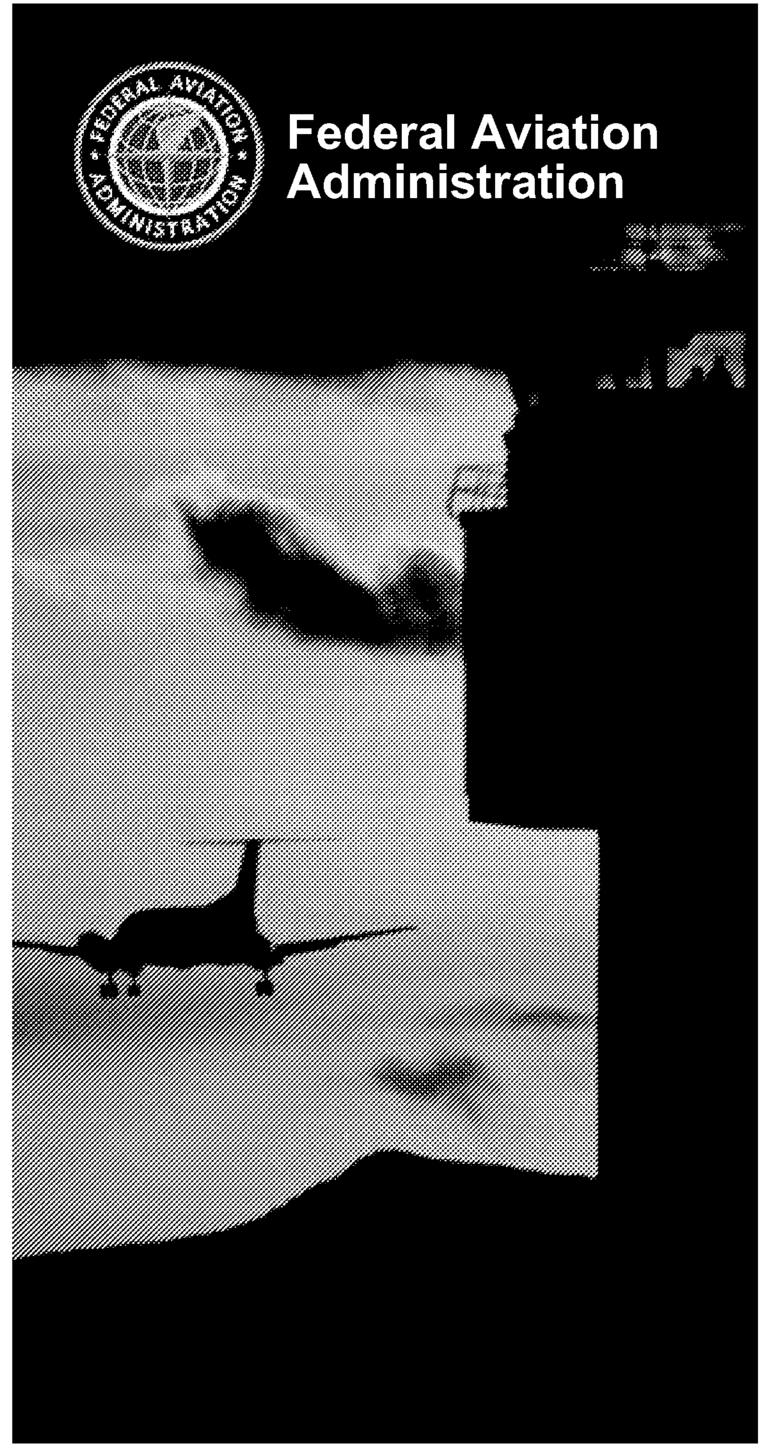
Unmanned Aircraft Systems

Integration into the National Airspace System (NAS)

Presented to: Access5

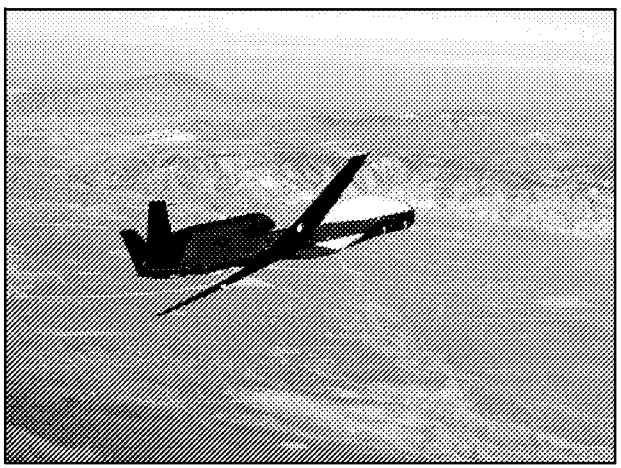
By: John Timmerman

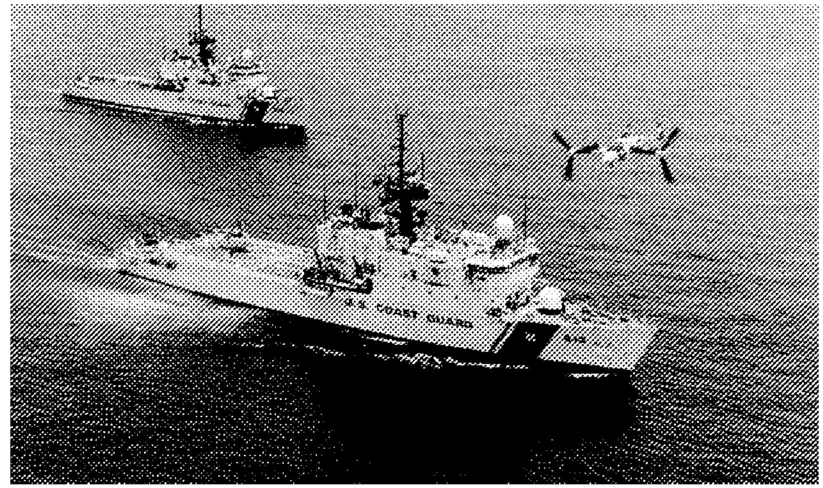
Date: July 12, 2005

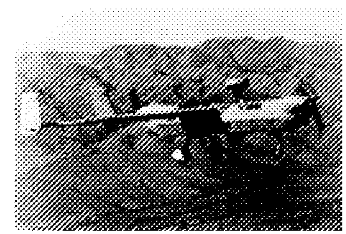


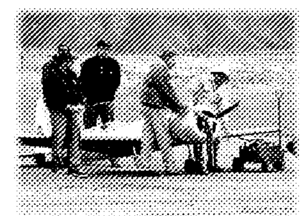
What is UAS?

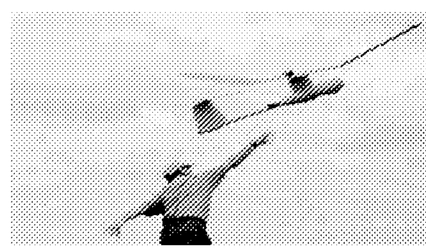
- Unmanned Aircraft Systems (UAS) historically called by various terms:
  - Drone/ROA/RPV/UAV/Model/R-C
- Includes:
  - Unmanned Aircraft (UA)
  - Aircraft Control Station
  - Command & Control Link/s
- Operated or flown by a "pilot"

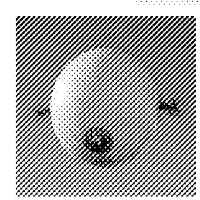


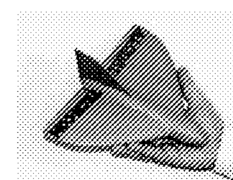












Current UAS Operations in the NAS

- Within "segregated" airspace
  - Includes Special Use Airspace (SUA) & Air Traffic Control Assigned Airspace (ATCAA)
  - Primarily by DOD
- In non-segregated airspace
  - "Public" UAS – through Certificate of Authorization (COA) process
    - Includes initial "trials" in support of DHS
  - "Civil" UAS – using experimental / type certification process
  - "Model" aircraft – with guidance from AC 91-57, dated June 1981
  - Variety of other operations believed to be occurring by both the public and private sector
    - Some based on interpretations of "model" aircraft guidance
    - Others with a lack of knowledge of aviation environment requirements
- While ensuring "no harm" to other NAS customers and public

Expected Changes - Next 5-10 years

- Many UAS's transitioning from R&D to operational status
  - Routine UAS flight - both VFR and IFR and in all airspace classes
- Wider scale development and uses for UAS
  - R&D activities in public and civil sectors continue to grow
  - New uses and applications – innovative customers and providers
- Increased demands on the NAS
  - Greater numbers and diversity of requests to operate in the NAS
  - UAS operations "mushrooming" in an increasingly busy NAS
  - Additional airspace and access requested for UAS flight
    - Including security and surveillance
      - Border and harbor patrol
      - Broad spectrum of law enforcement activities
  - Pressure for quicker access - "file and fly"
  - Conflicting interests among aviation stakeholders
- International efforts to "harmonize out of the box"

2015 and Beyond

- UAS operations dominate some aviation sectors
  - Particularly those “dirty, dull or dangerous”
- Commercial UAS applications steadily grow
  - Driven by “business cases” for reduced costs
- Consumers becoming increasingly receptive to reduced human presence in aircraft cockpits
  - Passenger flights with a single “supervisory” pilot
  - Cargo operations without an on-board pilot
- Increased “cooperation” needed between aviation segments to efficiently manage finite airspace resources
- Increased expectations for higher levels of safety

GOAL

&

RESPONSIBILITY!

A Safe NAS for All

www.ato.faa.gov

Zone Ready for Drone

(from FAA Air Traffic Organization Employees web site)

April 7 – The desolate landscape of the southwestern U.S. border with Mexico is widely known for illegal and unseen nocturnal activity. Now, the Department of Homeland Security is keeping watch from restricted airspace between 14,000 and 16,000 feet that extends from Organ Pipe Cactus National Monument in Arizona to New Mexico's Potrillo Mountains. Their unprecedented vantage point is the result of close cooperation with the FAA and the controllers who will keep the sky clear for a remote roving eye.

Since March 29, a temporary flight restriction (view the pdf) has limited access to the airspace along almost 350 miles of the border, expanding an earlier TFR near Nogales. The restriction is in effect nightly from 6 p.m. to 9 a.m., although that time can be expanded by issuance of a Notice to Airmen. Aircraft wishing to fly in the TFR when it is active must receive authorization from air traffic control prior to entry. Once in, pilots are required to maintain two-way communication with ATC and transmit a discrete transponder code.

Though not stated outright in the NOTAM that created the restriction, the reason behind the TFR is no secret. For some time both the White House and the Department of Homeland Security have advocated the use of unmanned aerial systems to increase the Secure Border Initiative's surveillance capability. The TFR makes it possible to fit the operation of those UASs into airspace traditionally occupied by manned military and civilian aircraft.

Predator-B, UAS. Photo: General Atomics Aeronautical Systems

"This is an extreme situation that has been presented to us," states Stephen Glowacki, a Systems Safety and Procedures specialist with the FAA's Air Traffic Organization, stressing the nation's security. "We have been working with U.S. Customs and Border Protection to try and answer this situation."

Inserting UASs into the National Airspace System is not a simple feat. According to Glowacki, the technology and certification that will permit unmanned aircraft to "see and avoid" other air traffic is still eight to ten years away. In the mean time, a carefully controlled environment is needed.

Until the advent of this TFR and its smaller forerunner, border surveillance using UASs was limited to airspace in restricted military areas. Tests conducted there helped develop the procedures now being used to safely conduct flights within the TFRs in New Mexico and Arizona.

Keeping a Homeland Security UAS separated from manned aircraft not participating in its mission requires positive control of aircraft movement within the restricted airspace. In the weeks leading up to the original TFR's issuance, ATC personnel at Albuquerque ARTCC and Tucson ATCT were briefed on procedures for handling UAS operations in airspace that includes non-participating aircraft. IFR control standards are applied and no change in separation minima is involved.

Controllers maintain communication with all manned aircraft operating in the TFR, while simultaneously monitoring the path of the UAS and talking to its ground-based pilot. The controllers' focus is on keeping non-participating aircraft away from the UAS, which flies under an IFR clearance within the TFR boundaries. Should the need arise to temporarily re-direct the UAS, the directions are delivered through secure communication with its pilot.

Although the TFR's Notice to Airmen states that ATC may provide flight advisories concerning UAS operation in the TFR, doing so is neither desired nor expected to be necessary. Only aircraft with ATC permission are allowed to enter the TFR, making it possible to control non-participating aircraft in ways that eliminate the need for such an advisory.

The TFR was not created without opposition. Even though the impact of its presence is expected to be minimal, the Aircraft Owners and Pilots Association feels that long-term operations are inappropriate for temporary restrictions. The TFR is in effect until Feb. 28, 2007. At the local level, airport management at Nogales International Airport reported a drop in business after the first, smaller TFR was created in January. However, because the restrictions are at an altitude well above that flown by aircraft using the airport, pilots may have been avoiding the area out of fear based on misunderstanding the restriction's boundaries.

ATO's Glowacki points out that the TFR was designed to cause the least amount of impact to pilots. The restricted airspace is relatively narrow vertically and is active primarily at night. Aircraft that operate at night are required to have all the equipment needed to communicate with ATC and transmit a discrete beacon code. All that is required for a pilot to enter the airspace, beyond that equipment, is permission from ATC. By flying above or below the restricted altitudes, pilots don't have to worry about what's going on in the TFR.

"It has been an amazing and ingenious way of temporarily resolving an incredible situation," Glowacki says. "Airspace studies and known aviation operations were reviewed and balanced against national security needs."

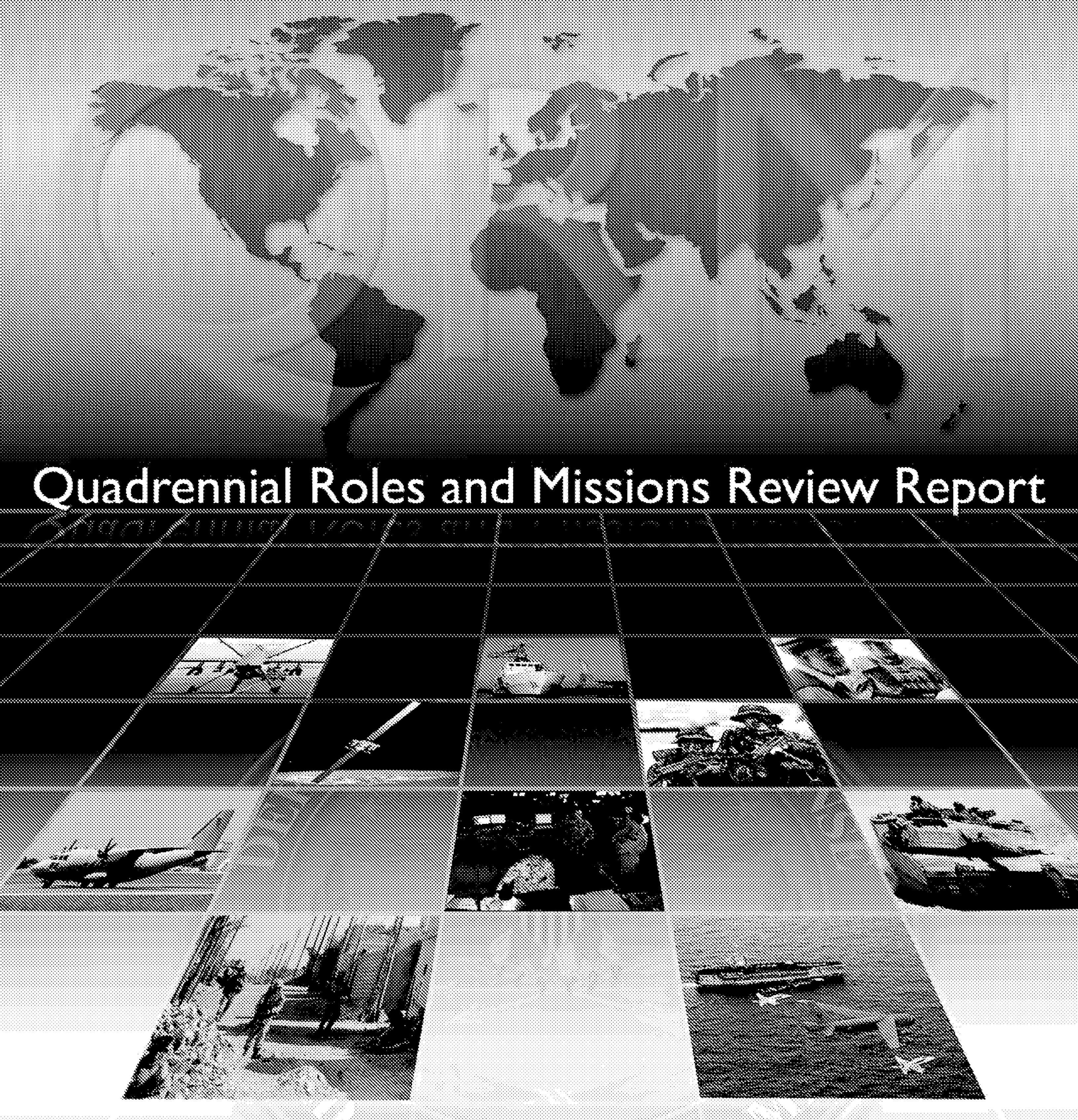
Now the challenge is to ensure safety while a relatively new technology is introduced to the NAS. Long-term TFRs like those along the southern border allow DHS time to carefully plan missions, without interruption or unexpected changes to the rules that govern them. However, fine tuning may be needed as the program continues. TFRs are flexible enough to be changed quickly based on anything new that is learned, unlike more rigid airspace restrictions such as Air Defense Identification Zones.

As Glowacki says, "the TFR is the best tool to fit the situation."

Related Information:

- Temporary Flight Restriction (PDF)

Quadrennial Roles and Missions Review Report



Department of Defense
January 2009

Quadrennial Roles and Missions

Review Report

January, 2009

Front Cover Image Credits

Top Row
#1 A fully armed MQ-9 Reaper taxis before a mission in Afghanistan.
U.S. Air Force photo by Staff Sergeant Brian Ferguson

#2 U.S. Coast Guard Cutter Bainbridge Island stands watch over the Statue of Liberty in New York Harbor.
U.S. Coast Guard photo by Petty Officer Mike Lutz

#3 An Afghan engineer talks with a member of the Nangarhar Provincial Reconstruction Team in the Nangarhar province of Afghanistan.
Photo by Staff Sergeant Joshua T. Jasper, U.S. Air Force

Second Row
#4 Wideband Global SATCOM satellite.
Air Force Image

#5 SEALs in from the water.
U.S. Navy SEALs Photo

Third Row
#6 The first Joint Cargo Aircraft presented to the U.S. Army.
L3, Alenia North America, Global Military Aircraft Systems

#7 Operations center in Qatar.
U.S. Air Force photo by SrA Brian Ferguson

#8 Soldiers in their M1A1 Abrams tank in Iraq.
Photo by Pvt. Brandi Marshall

Bottom Row
#9 Marines conduct a security patrol in Husaybah, Iraq.
AP Photo/ U.S Marine Corps, Cpl Michael R McMaugh, 1st Marine Division Combat Camera, HO

#10 A B-52 Stratofortress flies past the USS Nimitz with two U.S. Navy F/A-18 Hornets.
U.S. Navy photo

TABLE OF CONTENTS

FOREWORD

Since September 2001, our Nation has been engaged in a multi-theater, long-term conflict against militant extremists who seek to erode the strength and will of the United States, our partners, and our allies through irregular and asymmetric means. As the Department of Defense continues to engage in ongoing operations, we must also prepare for our future challenges by learning from the past, building on the present, and taking advantage of opportunities to increase the effectiveness and efficiency of our institution. During the inaugural Quadrennial Roles and Missions Review, we have leveraged previous defense reviews and lessons from recent operations to determine how we should change to better meet our institutional responsibilities and improve support to our national security partners.

In accordance with section 941 of the National Defense Authorization Act for Fiscal Year 2008, this report identifies the Department's Core Mission Areas and Core Competencies. Additionally, this report describes how the Department's civilian and military leadership reviewed the rapidly-evolving roles, missions, and capabilities associated with irregular warfare, cyberspace operations, unmanned aircraft systems, and intratheater airlift. Together, we have concluded the Department must improve how we organize, train, and equip our forces for these areas.

Of course, the Department of Defense cannot address our Nation's complex security challenges alone. One of the most important lessons from recent operations is that military success does not equate to victory. As a result, during the Quadrennial Roles and Missions Review we considered opportunities that will help strike a better balance between our Nation's hard and soft power capabilities. The Quadrennial Roles and Missions Review concludes we must improve our soft power: our national ability to promote economic development, institution-building and the rule of law, internal reconciliation, good governance, training and equipping indigenous military and police forces, strategic communications, and more. Doing so requires exploring whole-of-government approaches for meeting complex security challenges.

While the Quadrennial Roles and Missions Review lays a foundation for understanding the Department's roles and responsibilities in today's complex security environment, there is still much work to be done. As we move toward the Quadrennial Defense Review, we must continue initiatives that establish the right balance between winning today's wars and preventing tomorrow's conflicts while improving our whole of government ability to promote stability and security at home and aboard.

Robert M. Gates
Secretary of Defense

I. INTRODUCTION

Quadrennial Roles and Missions Review Objectives. The Quadrennial Roles and Missions Review (QRM) offered a unique opportunity for the Defense Department to further our strategic priorities by assessing responsibilities of individual components and evaluating improvements to the way we do business across our enterprise. Completed toward the end of the 2006 QDR implementation cycle, the 2009 QRM capitalized on changes the Department has made to its responsibilities, processes, and capabilities since 2006 and direction for the future established in our latest strategic guidance documents, including the 2008 *National Defense Strategy.*

From the onset of the Review, teams of senior civilian and military leaders from the Military Services, Joint Staff, Combatant Commands, and Office of the Secretary of Defense worked together to develop a framework that defines and links the Department's Core Mission Areas with its Core Competencies and Functions of the Armed Forces. Additionally, teams of civilian and military experts worked together to assess high-interest issue areas and propose actions to achieve the Department's primary objectives for this inaugural QRM:

- Increase synergy across the Department's Components.
- Improve the effectiveness of joint and interagency operations.
- Ensure the Department continues to efficiently invest the Nation's defense resources to meet the asymmetric challenges of the 21st Century.

This approach stems from our understanding that dealing with long-term security challenges requires the Department to operate with unity, agility, creativity, and in concert with our partners across the U.S. Government.

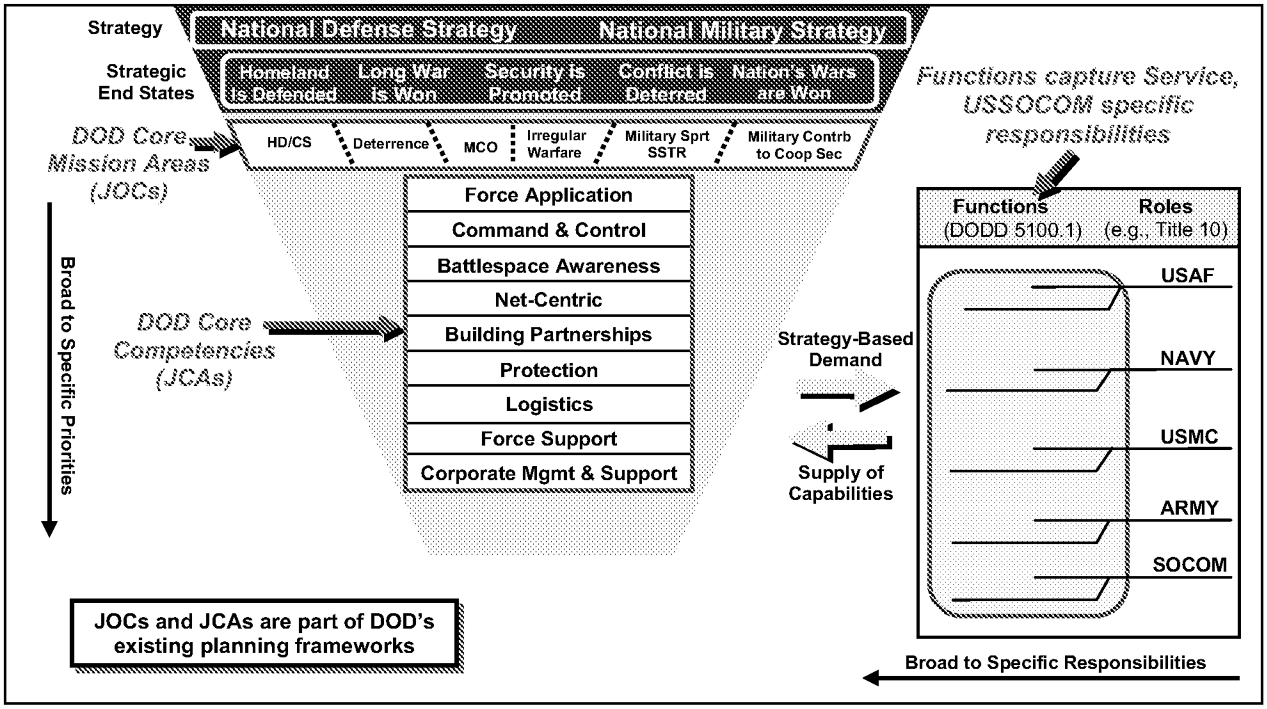
QRM Report Overview. Section II of this report describes a framework developed by the Department for assessing potential future roles and missions changes. This framework, which integrates traditional missions with new and emerging military activities, is the first of its kind developed during a defense review. Section III defines the Department's Core Mission Areas and Core Competencies, as required by section 941 of the 2008 National Defense Authorization Act. Section IV summarizes the Department's insights and initiatives for four specific roles and missions focus areas: Irregular Warfare; Cyberspace; Intratheater Airlift; and Unmanned Air Systems / Intelligence, Surveillance, Reconnaissance. Section V addresses the need for increased emphasis on effective interagency operations to address complex national security challenges.

During the QRM, the cohesive efforts of our civilian and military leaders and their desire to address security challenges from a Departmental perspective provided a solid foundation for continued cooperation in these and other roles and missions issue areas. While this report captures 2009 QRM results, they should not be viewed as the final solution for roles and missions challenges the Department and its partners face in today's dynamic security environment. Continued progress will depend on the capacity of the Department and its partners to take advantage of real-word lessons learned and our ability to work together to better integrate all instruments of national power.

II. ROLES AND MISSIONS FRAMEWORK

The framework in Figure 1 summarizes results of the Department's efforts to define its Core Mission Areas and Core Competencies. As the framework illustrates, Core Mission Areas and Core Competencies provide guidance to the Services and U.S. Special Operations Command on the appropriate mix and scope of roles and functions to meet priorities of the *National Defense Strategy* and *National Military Strategy*:

Figure 1: Department of Defense Framework for the QRM



Core Mission Areas are broad Department of Defense military activities required to achieve strategic objectives of the *National Defense Strategy* and *National Military Strategy*. A Core Mission Area is a mission for which the Department is uniquely responsible, provides the preponderance of U.S. Government capabilities, or is the U.S. Government lead for achieving end states defined in national strategy documents.

- Each of the Department's Core Mission Areas is underpinned by a Joint Operating Concept (see Section III) that identifies desired effects necessary to achieve operational objectives, essential capabilities to achieve these objectives, and relevant conditions under which capabilities must be applied. Joint Operating Concepts (JOCs) are a visualization of future operations. They describe how a commander, using military art and science, might employ capabilities necessary to meet future military challenges. In practice, JOCs establish context for the Department's force development planning and resourcing activities. This helps the Department identify military problems and develop innovative solutions that go beyond merely improving the ability to execute missions under existing standards of performance.

- Although JOCs underpin the Department's Core Mission Areas, they are not entirely Department-centric. For example, the Department informally coordinates with the Department of State and other agencies on concepts for irregular warfare, cooperative security, and stability operations. As we continue to evolve JOCs, there will be additional opportunities for interagency cooperation.

Core Competencies are groupings of functionally-organized capabilities associated with the performance of, or support for, a Department of Defense Core Mission Area. The Department's Components perform tasks and activities that supply these functionally-organized capabilities.

- The QRM determined the Department's Core Competencies correspond to the nine Joint Capability Areas (see Section III) established following the 2006 QDR. Joint Capability Areas (JCAs) are groupings of related capabilities that support strategic decision-making, capability portfolio management, and joint analyses of capability gaps, excesses, and major tradeoff opportunities. JCAs also provide a common capabilities language for use across the Department's activities and processes.

Functions are the appropriate or assigned duties, responsibilities, missions, or tasks of an individual, office, or organization as defined in the National Security Act of 1947, including responsibilities of the Armed Forces as amended. The term "function" includes purpose, powers, and duties. Specific Functions of the Services and U.S. Special Operations Command are captured in Department of Defense Directives.

Roles are the broad and enduring purposes for which the Services and U. S. Special Operations Command were established by law.

III. DEPARTMENT OF DEFENSE CORE MISSION AREAS, CORE COMPETENCIES, AND FUNCTIONS

A. Core Mission Areas

The QRM defined five key attributes for the Department's Core Mission Areas: they represent relatively enduring missions; they are necessary for achieving strategic end states derived from the 2008 *National Defense Strategy;* they constitute a broad military activity; they describe a unique Department of Defense capability and capacity; or they identify a mission for which the Defense Department is the U.S. Government lead and/or provides the preponderance of U.S. Government capabilities. In compliance with section 941 of the 2008 National Defense Authorization Act, the Department has established six Core Mission Areas:

1. **Homeland Defense and Civil Support (HD/CS)** operations help ensure the integrity and security of the homeland by detecting, deterring, preventing, or, if necessary, defeating threats and aggression against the United States as early and as far from its borders as possible so as to minimize their effects on U.S. society and interests. The Department also may be directed to assist civilian authorities in order to save lives, protect property, enhance public health and safety, or to lessen or avert the threat of a catastrophe. The Department provides many unique capabilities that can be used to mitigate and manage the consequences of natural and man-made disasters and must be prepared to provide support to federal, state, and local authorities.

Two UH-60 Black Hawk helicopters from 2nd Battalion, 227th Aviation Regiment, 1st Air Cavalry Brigade, 1st Cavalry Division, fly the commanding general of U.S. Northern Command General Victor Renuart Jr. and his staff over Galveston, Texas and surrounding areas during an aerial assessment of damage left in the wake of Hurricane Ike.

Photo by Sgt. Nathan D. Hoskins, 1st ACB, 1st Cav. Div. Public Affairs

2. **Deterrence Operations** are integrated, systematic efforts to exercise decisive influence over adversaries' decision-making calculus in peacetime, crisis, and war to achieve deterrence.

3. **Major Combat Operations (MCOs)** are the conduct of synergistic, high-tempo actions in multiple operating domains, including cyberspace, to shatter the coherence of the adversary's plans and dispositions and render him unable or unwilling to militarily oppose the achievement of U.S. strategic objectives.

4. **Irregular Warfare** encompasses operations in which the joint force conducts protracted regional and global campaigns against state and non-state adversaries to subvert, coerce, attrite, and exhaust adversaries rather than defeat them through direct conventional military confrontation. Irregular warfare emphasizes winning the support of the relevant populations, promoting friendly political authority, and eroding adversary control, influence, and support.

5. **Military Support to Stabilization Security, Transition, and Reconstruction Operations** is assistance to severely stressed governments to avoid failure or recover

from a devastating natural disaster, or assist an emerging host nation government in building a new domestic order following internal collapse or defeat in war.

6. **Military Contribution to Cooperative Security** describes how Joint Force Commanders mobilize and sustain cooperation, working in partnership with domestic and foreign interested parties, to achieve common security goals that prevent the rise of security threats and promote constructive regional security environments.

B. Core Competencies

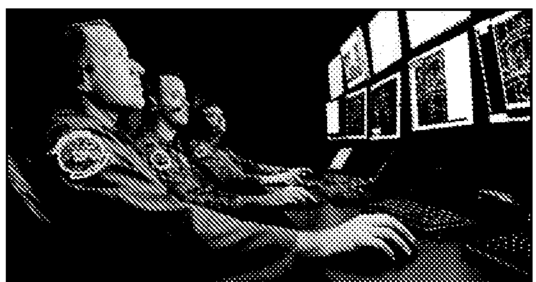
The Department's Core Competencies, expressed as Joint Capability Areas, establish the link between the operational perspectives of our Core Mission Areas and the Department's capabilities development processes. In practice, Joint Capability Areas translate current and future operational needs to capability priorities, and form the functional structure used to prioritize, assess, develop, and manage capabilities across all the Department's Components. In compliance with section 941 of the National Defense Authorization Act for 2008, the Department has defined nine Core Competencies:

1. **Force Application** – The ability to integrate the use of maneuver and engagement in all environments to create effects necessary to achieve mission objectives.

2. **Command and Control** – The ability to exercise authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission.

3. **Battlespace Awareness** – The ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making.

4. **Net Centric** – The ability to provide a framework for full human and technical connectivity and interoperability that allows all Defense Department users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.



Electronic warfare officers monitor a simulated test in the Central Control Facility (CCF) at Eglin Air Force Base, Florida. The Air Force uses the CCF to oversee electronic warfare flight testing.

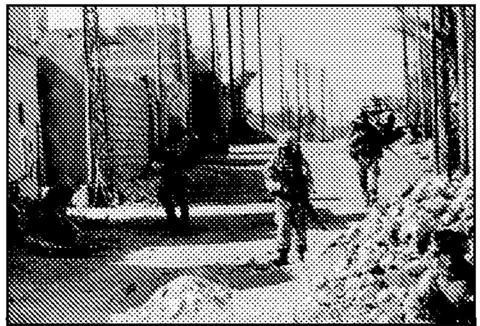
U.S. Air Force photo by Capt. Carrie Kessler, 53rd Wing Public Affairs

5. **Building Partnerships** – The ability to set the conditions for interaction with partner, competitor or adversary leaders, military forces, or relevant populations by developing and presenting information and conducting activities to affect their perceptions, will, behavior, and capabilities.

6. **Protection** – The ability to prevent/mitigate adverse effects of attacks on combatant and non-combatant personnel and physical assets of the United States, our allies, and friends.

7. **Logistics** – The ability to project and sustain a logistically-ready joint force through the deliberate sharing of national and multi-national resources to effectively support operations, extend operational reach, and provide joint force commanders the freedom of action necessary to meet mission objectives.

8. **Force Support** – The ability to establish, develop, maintain and manage a mission-ready Total Force, and provide, operate, and maintain capable installation assets across the Total Force to ensure needed capabilities are available to support national security.



Marines with 1st Platoon, Echo Company, 2nd Battalion, 1st Marine Regiment conduct a security patrol in Husaybah, Iraq, during Operation Steel Curtain.

9. **Corporate Management and Support** – The ability to provide strategic senior level, enterprise-wide leadership, direction, coordination, and oversight through a chief management officer function.

C. Integrating Core Mission Areas & Core Competencies into DOD Processes

As described in the 2006 QDR Report, the Department has expanded its use of integrated capability portfolios to balance risk and conduct strategic-level capability trade-offs. Accordingly, the Department has organized its governance structure for managing its capability portfolios around the nine Core Competencies/Joint Capability Areas. A pilot program started during the Fiscal Year 2009 budget process validated using JCAs as part of an integrated portfolio management framework. The current defense budget development cycle considered all nine JCAs, with specific program elements mapped to appropriate lead and supporting JCA portfolios. Additionally, the Department has assigned oversight responsibility for each of the JCAs to a Senate confirmed official paired with a senior military co-lead. The Core Competencies/Joint Capability Areas structure is now a significant part of the Department's requirements process. For example, the Joint Capability Integration Development System will direct all requirements documents to be associated with appropriate JCAs. As the Department fully integrates the Core Competencies/Joint Capability Areas structure, it will be able to better illustrate capability investments across the Department.

D. Functions of the Services and U.S. Special Operations Command

The QRM examined responsibilities assigned by U.S. Code and the Secretary of Defense to the Services and other Department Components. A major aspect of this assessment was a thorough review of Department of Defense Directive 5100.1, "Functions of the Department of Defense and Its Major Components." This document was modified to ensure functions are identified and assigned to appropriate organizations. These modifications stress the Department's continued emphasis on joint warfighting, and incorporate recent and emerging responsibilities in such areas as special operations and cyberspace operations.

IV. ROLES AND MISSIONS FOCUS AREAS

During the Quadrennial Roles and Missions Review, the Department of Defense assembled teams of experts to address specific roles and missions issues in the areas of Irregular Warfare; Cyberspace; Intratheater Airlift; and Unmanned Aircraft Systems / Intelligence, Surveillance, Reconnaissance.[1] The following sections capture the Department's common vision for each area and initiatives underway to increase synergy across the Department's Components; improve effectiveness of joint and interagency operations; and ensure the Department continues to efficiently invest our Nation's defense resources to meet the asymmetric challenges of the 21st Century.

A. Irregular Warfare

Executive Summary. The Department currently defines irregular warfare as a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will.[2] The Department continues to make steady progress toward incorporating irregular warfare into its force planning construct, influencing the size of the force and the capabilities needed to ensure the joint force is as effective in irregular warfare as it is in conventional warfare. Both the 2008 *National Defense Strategy* and the 2006 QDR codified this commitment to irregular warfare. The Department will continue to inculcate irregular warfare priorities into policy, doctrine, training, and education at all levels, while developing and sustaining a balanced investment strategy to field needed capabilities and capacity. General Purpose Forces (GPF) and Special Operations Forces (SOF) each have roles and responsibilities for irregular warfare missions, with the force composition mix depending largely on the risk and character of the operational environment. To support maturation of our national ability to conduct irregular warfare, the Department, in collaboration with other U.S. Government departments and agencies, will explore alternatives that promote interagency cooperation, and improve the efficiency, flexibility, and responsiveness of funding lines and legislative authorities.

The Department's vision is to shape the future joint force to be as effective in irregular warfare as it is in conventional warfare.

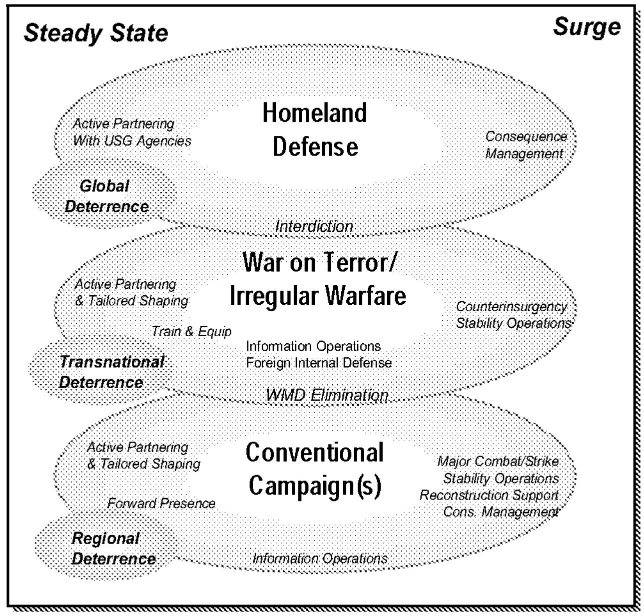
Irregular Warfare Challenges. Historically, the Department has focused its efforts on the ability to defeat a state adversary's conventional military forces. However, the 2006 QDR assessed that while conventional threats will remain and U.S. Armed Forces must maintain the capacity to defeat them, current and future adversaries are more likely to pose irregular and asymmetric threats. The Department therefore developed a force planning construct (Figure 2) that recognizes the need to maintain capabilities to defend the homeland and prevail in conventional campaigns while concurrently developing a mastery of irregular warfare comparable to that which our armed forces have achieved for conventional warfare. This

[1] The Defense Department's leadership and members of the 2008 U.S. House Armed Services Committee Roles and Missions Panel identified these areas as high interest.

[2] In this definition, the term "violent" refers to the nature of the conflict and is not necessarily the prescription for a U.S. response.

assumes added importance, especially during an era when the character of warfare is blurring and military forces are likely to engage adversaries who use hybrid warfare which simultaneously blends conventional and irregular methods. Given this likelihood, the Department must determine the most efficient and effective balance between homeland defense, irregular warfare, and conventional warfare priorities.

Figure 2: DoD Force Planning Construct



The primary irregular warfare activities addressed by this report – foreign internal defense, counterinsurgency, counter-terrorism, unconventional warfare, and stability operations – occur across the spectrum of irregular and conventional warfare operations. None of these activities are new to the Department of Defense. Many of the capabilities required to execute them are resident in some parts of the joint force, but may not exist in sufficient capacity to meet expected demand. In other cases, the Department needs to develop new capabilities, such as foreign language and cross-cultural communication skills, to address emerging and future challenges.

During the QRM, an Irregular Warfare Issue Team led by U.S. Special Operations Command and the Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities addressed initiatives to improve effectiveness of joint operations and create opportunities for efficient investment of resources for irregular warfare. The team examined irregular warfare roles and missions across Special Operations Forces and General Purpose Forces; the balance of responsibilities across the Active and Reserve Components; identified mechanisms to further institutionalize irregular warfare across the Department; and how to better integrate defense capabilities with those of our interagency partners and allies.

Graduates of the first Ministry of Interior National Police Command Special Forces platoon perform a demonstration during their graduation ceremony at the Iraqi Police Academy in Kirkuk, Iraq. Irregular warfare increases demand for capabilities to organize, train, and equip foreign security forces.

Background. DOD has achieved some success in institutionalizing irregular warfare across the Department in recent years. The Department has established irregular warfare as one of its six Core Mission Areas, and completed a formal Irregular Warfare Joint Operating Concept describing how joint commanders might employ capabilities to meet future irregular warfare operational challenges. The Irregular Warfare Joint Operating Concept recognizes the protracted nature of irregular conflict and how it can occur in both steady-state and surge scenarios, just as partner capacity building can occur in both. At the component level, all Services and several Combatant Commanders have established irregular warfare-related training and education centers. The Office of the Secretary of Defense has initiatives underway to institutionalize irregular warfare in the joint force, working with the Services, Joint Staff and several interagency partners. The Department is currently conducting a study of irregular warfare-relevant requirements in the steady-state, as well as in counterinsurgency and unconventional warfare surge scenarios used for defense planning. Study results will allow the Department to identify and institute additional long-term changes to address irregular warfare capabilities and capacity priorities, resulting in a force that is better trained, equipped, and educated to handle the full range of missions across the spectrum of operations.

While these efforts reflect progress, the Department acknowledges it has more to do to achieve its irregular warfare vision. Gaps still exist in institutionalizing irregular warfare concepts and capabilities needed for future joint operations, and for operating in concert with our interagency partners. The Department will continue to develop a resource investment strategy that achieves the right balance of capabilities to meet future challenges across the spectrum of operations. While more remains to be done, institutional transformation requires time and appropriate resources. With the continued support of Congress, the Department will steadily improve critical irregular warfare capabilities to meet the challenges of a rapidly evolving security environment.

Vision: Responsibilities for Irregular Warfare and Continued Institutionalization. The Department's irregular warfare vision is to equip the joint force with capabilities, doctrine, organization, training, leadership, and operating concepts needed to make it as proficient in irregular warfare as it is in conventional warfare. The Defense Department's goals for the future joint force include two main elements:

1. A Department with increased and balanced capability and capacity to address all future security challenges, including irregular warfare; and

2. A Department that can better integrate with interagency partners to leverage all elements of national power to meet national security objectives.

A 7th Special Forces Group Soldier instructs his Colombian counterparts in urban-warfare techniques. DOD will continue to institutionalize irregular warfare capabilities in SOF and General Purpose Forces.

Decisions and Initiatives.

<u>SOF and GPF Roles and Missions for Irregular Warfare</u>. The Department reviewed the roles and missions for SOF and GPF and concluded each has significant responsibilities for irregular warfare. As a result, the Department is continuing to define how Services develop and apply capabilities in different environments. For example, U.S. Special Operations Command, acting as the Department's joint proponent for security force assistance, is collaborating with the Chairman of the Joint Chiefs of Staff, U.S. Joint Forces Command, Services, and Geographic Combatant Commanders to develop global joint sourcing solutions that recommend the most appropriate forces for validated security force assistance requirements.

- As noted in the 2006 QDR, General Purpose Forces will continue to support and play a leading role in stability operations and counterinsurgency, and a greater role in foreign internal defense. For steady-state operations, GPF will have an increased role in training, advising, and equipping foreign security forces, deploying and engaging with foreign partner security forces, supporting civil-military teams in stability operations, and conducting integrated irregular warfare operations with SOF. To do this effectively, General Purpose Forces will need a greater degree of language and cultural instruction to train and advise indigenous forces.

- The SOF and GPF force mix for conducting future operations will largely depend on the risk and character of the operational environment, not simply by the task at hand. For example, when operational environments dictate that the joint force presence remains unobtrusive, SOF will play a leading role. General Purpose Forces will continue to play a leading role in operational environments where a large-scale presence is warranted to provide security to a population.

<u>Balancing Active and Reserve Components for Irregular Warfare</u>. The global, protracted nature of irregular warfare will continue to place more demands on the Department's Active Component, Reserve Component, and civilian Total Force. To address this challenge, the QRM assessed the appropriate Active/Reserve Component balance to meet future irregular warfare-related operational demand. The Department concluded that persistent presence and sustainment of irregular warfare activities require increasing specific capabilities across the Total Force, including civil affairs and psychological operations capabilities in the Active Component force.

<u>Key Mechanisms to Institutionalize Irregular Warfare</u>.

- Oversight. The Department's Components have matured their understanding and execution of irregular warfare. While the Department assessed the need to designate a lead component for oversight of institutionalizing irregular warfare, we have determined it is more advantageous to use existing oversight structures and mechanisms for institutionalizing irregular warfare across the joint force rather than create new ones.

- Guidance. Despite gains achieved since the 2006 QDR, the Department has determined efforts to transform capabilities are not uniform across all of its elements. As a result, the Department has finalized a Directive that provides a policy framework and designates responsibilities for irregular warfare. This Directive will help lay the foundation for investments that will continue to build capabilities needed to balance near-term risk and long-term force development goals.

- Component Responsibilities. The Department is revising DOD Directive 5100.1, Functions of the Department of Defense and its Major Components, to incorporate irregular warfare responsibilities.

- Planning Construct. In order to further ingrain irregular warfare key elements into planning for the range of military operations, the Department will assess revisions to its current campaign planning construct[3] to account for complexities of the environment and incorporate irregular warfare concepts for influencing relevant populations.

Mechanisms to Integrate with Interagency Partners. Meeting challenges of current and future security environments requires the concerted effort of all instruments of U.S. national power. Achieving unity of effort within the U.S. Government is often complicated by organizational "stove-piping," crisis-driven planning, and divergent organizational processes and cultures. These differences have certain benefits, but are not well-suited for addressing the range of irregular challenges that cut across organizational expertise of different U.S. Government entities. Additionally, many interagency processes are oriented toward responding to crises, or surge scenarios, rather than supporting steady-state activities.

A soldier from the 502nd Infantry Regiment, 2nd Brigade Combat Team, 101st Airborne Division speaks with an Iraqi man while visiting a home for the elderly in Kadhimiya, Iraq. Earning the trust of the local population is critical to successful counter-insurgency operations.

Photo by Staff Sergeant Manuel J. Martinez, U.S. Air Force

- The Department will continue to promote and participate in efforts to institutionalize irregular warfare in interagency planning. Initiatives currently underway include development of the Interagency Management System for Reconstruction and Stabilization led by the Department of State Coordinator for Reconstruction and Stabilization, and the National Counter Terrorism Center's efforts to lead interagency steady-state and surge planning for the war on terrorism.

Looking Forward. While significant progress is being made today toward achieving the Department's vision for irregular warfare, there are still challenges to overcome. The Department must continue to address related issues with the interagency outlined in the "Interagency Opportunities" section of this report. With the continued support of Congress, the Department will achieve its objective of ensuring irregular warfare capabilities are firmly integrated into all aspects of the Department's future force.

[3] The Department's planning construct consists of six phases: Shape; Deter; Seize Initiative; Dominate; Stabilize; and Enable Civil Authority.

B. Cyberspace

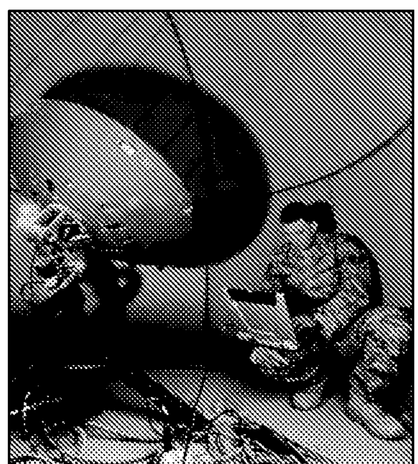
Executive Summary. Cyberspace is a decentralized domain characterized by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously, inexpensively, and anonymously. Amidst the rush of technological advancement, the Department seeks cyberspace capabilities that maintain our freedom of action and that of our allies and partners while ensuring superiority over potential adversaries in militarily-relevant portions of the domain. This environment presents enormous challenges and unprecedented opportunities to forces charged with defending national interests and advancing U.S. policy.

The Department's vision is to develop cyberspace capability that provides global situational awareness of cyberspace, U.S. freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and, when called upon, provide cyberspace support to civil authorities.

The Department is continuing to transform to meet the challenges of this dynamic domain. As part of the 2009 QRM, the Department set out to define its roles, missions, and objectives in cyberspace through the year 2030. In particular, the 2009 QRM focused on the Department's roles and missions related to:

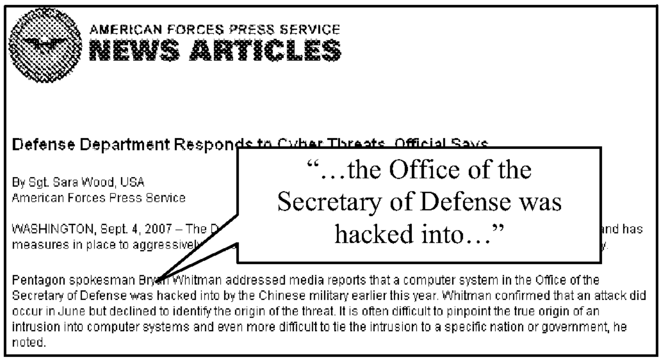
- Developing capable forces, equipped with requisite skills, training, education, and experience.
- Structuring forces and associated processes and procedures to effectively and efficiently execute Defense Department policies and priorities in cyberspace.
- Employing those forces to achieve desired effects across the full range of military operations.

The Department has determined it is appropriate for each Service to develop capabilities to conduct cyberspace operations. Improvements are needed in training and education to field a professional force, and in command and control for cyberspace operations. Initiatives described in this report represent current Defense Department responsibilities and challenges in this evolving domain. More remains to be done before the Department is able to fully meet its vision. Accordingly, decisions and initiatives reported in this section should be considered as waypoints to chart the Department's progress toward achieving our cyberspace vision.


A U.S. Air Force network systems technician reacquires the Global Broadcast System, which is part of keeping an uninterrupted flow of information streaming to a Combined Air Operations Center.

U.S. Air Force photo by Staff Sergeant Christine Seyer, 36th SW

Cyberspace Challenges. Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. The expanding use of cyberspace places United States' interests at greater risk from cyber threats and vulnerabilities. Cyber actors can operate globally, within our own borders, and within the borders of our allies and adversaries. The complexity and amount of activity in this evolving domain make it difficult to detect, interdict, and attribute malicious activities.


AMERICAN FORCES PRESS SERVICE
NEWS ARTICLES

Defense Department Respon[ds to Cyber Threats, Official Says]

By Sgt. Sara Wood, USA
American Forces Press Service

WASHINGTON, Sept. 4, 2007 – The D ... nd has measures in place to aggressive ...

Pentagon spokesman Bryan Whitman addressed media reports that a computer system in the Office of the Secretary of Defense was hacked into by the Chinese military earlier this year. Whitman confirmed that an attack did occur in June but declined to identify the origin of the threat. It is often difficult to pinpoint the true origin of an intrusion into computer systems and even more difficult to tie the intrusion to a specific nation or government, he noted.

"…the Office of the Secretary of Defense was hacked into…"

Although cyberspace presents unique challenges to military operations, the Department has made significant progress in defining its roles, missions, and objectives in cyberspace. Additionally, cyberspace offers the U.S. military unprecedented opportunities to shape and control the battlespace to achieve national objectives. Because adversaries operate in the same shared environment, U.S. forces have the ability to use non-kinetic options with new levels of global reach and immediacy against a variety of targets.

Background. The Department has officially defined cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Experience from recent operations and global cyberspace incidents underscore the critical role cyberspace capabilities play in preventing conflict when possible, and supporting full-spectrum military operations when necessary. The Department has made significant progress in operations in support of Combatant Commands and in working cyberspace issues collaboratively within the U.S. Government. Interagency forums allow the Department to leverage authorities in an integrated fashion and to understand equities in the earliest stages of planning. These operations are governed by U.S. domestic and international law. Additionally, our understanding of threats to the Global Information Grid and the development of defensive measures has progressed.

The findings of the 2006 Quadrennial Defense Review and the 2006 *National Military Strategy for Cyberspace Operations* (NMS-CO) laid the groundwork for many areas where the Department has made significant progress on cyberspace challenges.

- The 2006 QDR highlighted the Department's ability to operate effectively in cyberspace as a critical facet of our long-term strategy. The QDR set out several imperatives for the Department, including: capabilities to locate, tag, and track terrorists in cyberspace; capabilities to shape and defend cyberspace; and the strengthening of coordination of defensive and offensive missions in cyberspace across the Department.

- The NMS-CO and associated Implementation Plan provide a comprehensive strategy for the U.S. military to achieve military superiority in cyberspace. Combatant Commanders, Military Departments, Defense Agencies, and other Department Components use the NMS-CO as a reference for planning, resourcing, and executing cyberspace operations.

Outside the Department, we continue to work with other U.S. Government departments and agencies to better delineate roles and missions and enhance the Nation's ability to protect and advance national security objectives both in cyberspace and using cyberspace tools. The Comprehensive National Cyber Security Initiative (CNCI) provides an important framework for U.S. Government cooperation and division of labor.

Vision. U.S. national power and security depend on our ability to access and use the global commons. As such, the Department seeks the ability to achieve superiority in military-relevant portions of cyberspace. In an environment characterized by uncertainty, complexity, rapid technological change, vulnerability, and minimal barriers to entry, the Department seeks strategic, operational, and tactical cyberspace capabilities that provide:

- U.S. freedom of action in cyberspace, to include freedom from unwanted intrusions and the ability to deny an adversary's freedom of action in cyberspace.

- Global situational awareness of cyberspace.

- The ability to provide warfighting effects within and through the cyberspace domain that are synergistic with effects within other domains.

- The ability, when called upon, to provide cyberspace support to civil authorities.

Decisions and Initiatives. During the QRM, a Cyber Issue Team co-led by the Office of the Under Secretary of Defense for Policy and U.S. Strategic Command addressed cyberspace issues related to developing, structuring, and employing the cyberspace force. To achieve the desired end states of our cyberspace vision, the Department has decided to pursue the following initiatives.

<u>Developing the Cyberspace Force</u>.

- The Department has decided to develop a professional cyberspace force able to influence and execute cyberspace operations with the same rigor and confidence as traditional Department operations in other domains.

- To mature this force, the Defense Department intends to learn from the new, innovative capabilities and experiences of our counterparts across the U.S. Government, in the private sector, and internationally.

- Internally, the Department is changing its Joint Professional Military Education curricula to include more classes and information on cyberspace to improve knowledge of this domain throughout the force and among civilian employees.

- For Computer Network Operations (CNO) specialists, the Department is increasing basic training capacity in the coming years. Our goal is to double the capacity of Department CNO training facilities to 1,000 students per year.

Employing the Cyberspace Force.

- Internally, the Department is establishing adaptable, agile, and responsive organizational structures and processes that ensure resource coherence, integration of core functions, and optimization of cyberspace capabilities, while preserving Services' ability to field tactical CNO elements into their force structure.

- Externally, the Department will continue its robust cooperation with a broad range of cyberspace stakeholders. Consistent with the objectives of preserving U.S. freedom of action in cyberspace and denying an adversary's freedom of action in the domain, the Department seeks to build stronger partnerships with Congress, Federal Government departments and agencies, alliance and coalition partners, industry, academia, and other non-government organizations. Greater integration of cyber policies, operations and activities into exercises, discussions with allies and partners, within the U.S. Government and with industry is necessary to better understand the requirements and effects of military operations in this domain. The Department has much to build on within the framework of the CNCI and from ongoing international efforts.

Partnerships are a vital component to successful cyberspace operations.

Developing Cyberspace Capabilities.

- The Department has determined its acquisition processes for cyberspace capabilities should be more responsive to warfighter requirements. While we have continuously sought to increase capabilities and capacity for achieving effects in and through cyberspace, we will continue to seek new ideas through diverse venues and forums, including combatant commander senior warfighting forums and experimentation, to define future opportunities and develop creative solutions for warfighters' needs.

Looking Forward. In a cyberspace environment of constant change, the Department must continually review its posture. It is clear we cannot accomplish all we desire in this evolving domain without significant assistance from a broad range of partners from academia, industry, and other governments. Collectively, with the support of Congress, the Department will:

- Continually assess emerging threats and existing vulnerabilities.

- Exercise our abilities to anticipate, predict, prevent and respond to cyberspace attacks.

- Build capacity and capability to take advantage of the opportunities and limit challenges inherent to cyberspace.

- Organize ourselves, within the U.S. Government, to defend national interests and advance national policy through cyberspace.

Thanks to a strong basis for private sector, interagency and international cooperation, the Department's roles and missions in cyberspace will continue to mature. As the U.S., our alliance and coalition partners, and our adversaries learn to employ these capabilities in all phases of collaboration, cooperation, and conflict, we anticipate that the demand for effects in and through cyberspace will grow. This will require corresponding growth of the technical Defense Department workforce, expansion of our scientific and technological capabilities, and potential shifts in our traditional culture. Our approach to cyberspace must remain flexible as our understanding of the domain continues to mature, and as U.S., alliance, coalition partners, and adversary capabilities to operate in cyberspace increase. The Department remains steadfast in our commitment to achieve superiority in the military-relevant portions of cyberspace.


Department of Defense photo by R. D. Ward

Estonian Minister of Defense Jaak Aaviksoo, left, talks about how he views the threat of cyber terrorism during discussions with Secretary of Defense Robert M. Gates in the Pentagon.

C. Intratheater Airlift

Executive Summary. The 2009 QRM assessed alignment of Service responsibilities for conducting intratheater airlift operations. Airlift operations performed within a theater span the traditional division between "general support," which is normally provided for the joint force by an Air Force component commander through a common-user airlift service, and "direct support" conducted by all Service component commanders employing their Services' organic airlift assets. At the conclusion of the QRM, the Department determined Service responsibilities for intratheater airlift operations are appropriately aligned, and the option that provided the most value to the joint force was to assign the C-27J to both the Air Force and Army. However, based on lessons learned from recent operations, there are areas for improvement. By changing internal policy, updating doctrine, and maturing concepts of operations to better reflect our intratheater airlift vision, we will improve effectiveness, increase joint synergy and minimize duplication of effort for this mission

The Department's vision is to provide both general and direct support intratheater airlift by maximizing the use of aircraft that have significant multi-use capabilities and are able to alternate between these missions.

Intratheater Airlift Challenges. Responsibilities for the intratheater airlift mission have evolved over time to respond to the changing operating environment and fielding of enhanced capabilities. Most recently, lessons learned from airlift support to Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF) have reshaped our intratheater airlift vision. During the QRM, an Intratheater Airlift Issue Team co-led by the Office of the Under Secretary for Acquisition, Technology, and Logistics, and U.S. Transportation Command addressed all fixed-wing airlifters with significant theater capabilities, including the C-27J Joint Cargo Aircraft being acquired by the Air Force and Army through a joint program.[4] The team's objective was to identify potential changes to responsibilities, policies, doctrine, and concepts of operation to improve effectiveness, address current and future challenges, increase joint synergy, and minimize duplication of effort between the Services for the intratheater airlift mission.

U.S. Air Force photo by Staff Sgt. Ricky A. Bloom

Airmen finish signing forms after conducting a preflight inspection on a C-5 at Balad Air Base, Iraq. Strategic airlift aircraft effectively support intratheater movements for OIF and OEF.

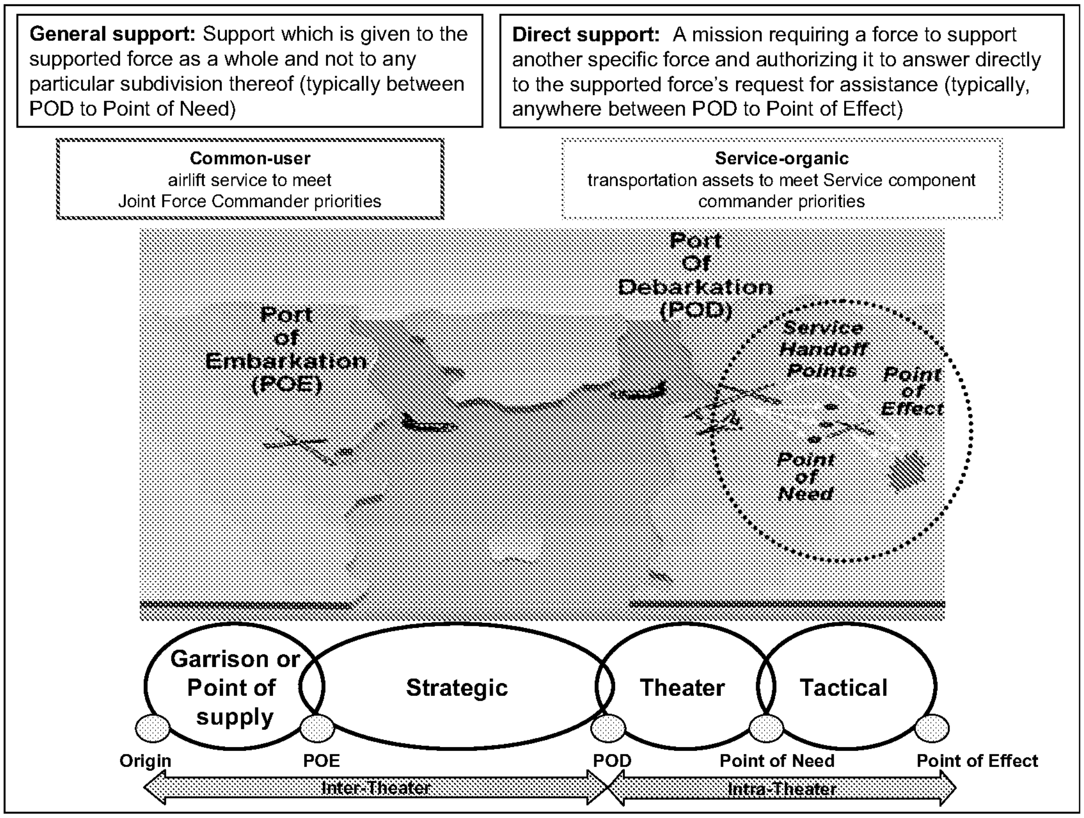
Background.

General and Direct Support Airlift. Intratheater airlift operations span the traditional division between general support, normally provided by an Air Force component commander using a

[4] The QRM assessed intratheater airlift operations conducted under Title 10, including Reserve Component forces operating as gained Title 10 forces. Traditional missions that are clearly organic to a Service component were not addressed (i.e., helicopter or small fixed-wing aircraft operations in direct support of a Service component in a "combat zone").

centrally-managed common-user airlift service, and direct support conducted by Service component commanders usually using Service component organic airlift transportation assets (see Figure 3).

Figure 3: General Support and Direct Support Airlift



Evolution of Airlift Responsibilities. The Army and Air Force first reached agreement on airlift responsibilities in the early 1950s. A series of memoranda removed restrictions on Army helicopter development and allowed the Army to conduct air operations for transport of Army supplies, equipment, and small units within the combat zone. In 1966, the Army and Air Force agreed the Army should fully develop helicopter capabilities, but barred the Service from major fixed-wing airlift roles. In 1986, another Army-Air Force agreement identified the Army as the executive Service for aircraft in units organic to the land force and employed within the land component's area of operations. The Air Force continued as the executive Service for aircraft that are most effective when organized under centralized control for theater-wide employment. Today, Service responsibilities for intratheater airlift missions generally remain aligned along the tenets of the 1986 agreement, as reaffirmed by an Army and Air Force Joint Cargo Aircraft Memorandum of Agreement signed in 2006.

OIF and OEF Observations. Recent operations in OIF and OEF highlighted three airlift issues of relevance to the QRM:

- The operational agility achieved by using airlift aircraft that alternate between intertheater and intratheater missions is a true transformation in airlift employment concepts. This flexibility is achieved by improving the visibility of requirements and exploiting previously untapped capacity gained through arrangements with U.S. Transportation Command to support theater airlift operations as needed. This new, combat-tested approach is a model for improving intratheater airlift across the full range of general and direct support operations.

- Increasing distances in a more dispersed and non-contiguous operational environment challenge our ability to supply distributed forces. While this evolving operational environment challenges the capabilities of helicopters to provide direct support to ground forces, the need for direct support remains unchanged. As a result, the Department has determined it must look for new ways to employ time sensitive/mission critical airlift in theater.

- Starting with U.S. Central Command in 2004, the Department has been integrating a Joint Deployment Distribution Operations Center (JDDOC) into every Combatant Command's operating structure to coordinate and synchronize logistical movements and ensure greater effectiveness and efficiency of intratheater airlift operations. A success story from the U.S. Central Command's JDDOC is the ability to meld commercially contracted intratheater airlift options into the mix of airlift capabilities. Commercial contracts/tenders offer a flexible means to quickly expand and reduce capacity to meet the ebb and flow of movement requirements in theater. Commercial contract and tender options range from short-takeoff and landing aircraft for moving small loads and servicing outlying airfields, to large transport aircraft moving palletized cargo and rolling stock. In collaboration with the Air Force, the U.S. Central Command's JDDOC provides the means to manage airlift requirements and funnel demand to military or commercial lift providers based on expected capacity.[5]

Vision for Future Intratheater Airlift Operations. Future joint operations will continue to require robust general and direct support intratheater airlift. The Air Force, through a common-user airlift service, will provide intratheater general support, while each Service will provide its own direct support using their "organic" transportation assets. The evolving operational environment, characterized by increasingly distributed operations and longer lines of communication, requires a suitable fixed-wing aircraft for intratheater airlift roles traditionally performed by helicopters. Mission-capable fixed-wing aircraft in a direct support role will complement other airlift assets and allow the entire intratheater airlift fleet to be employed more efficiently. Conducting simultaneous general and direct support missions using a fleet of cross-Service airlift capabilities will


L3, Alenia North America, Global Military Aircraft Systems

The first Joint Cargo Aircraft was presented to the U.S. Army on September 25, 2008. The C-27J offers significant utility to provide both general and direct support to warfighters.

[5] USTRANSCOM provides the contracting oversight for commercial contracts/tenders to ensure compliance with contracting requirements.

take full advantage of aircraft with significant multi-use capabilities. Some fixed-wing direct support aircraft, like the C-23B Sherpa, have limited payload and range and cannot support common-user airlift operations theater-wide. The C-27J, which is replacing the C-23B, has significantly greater capability and will be employed to maximize the overall utility for the joint force in either role.

Decisions and Initiatives. The QRM Intratheater Airlift assessment determined that Service responsibilities for intratheater airlift capabilities are appropriately aligned. However, there are opportunities to improve effectiveness, increase joint synergy and minimize duplication of effort between the Services for this evolving mission.

Supporting Time Sensitive/Mission Critical (TS/MC) Movement Requirements. The Department has determined theater TS/MC movement requirements will continue to drive a need for Service-organic aircraft to conduct direct support missions. These requirements reflect supported commanders' immediate priorities for delivery of equipment, supplies, and personnel. In support of the QRM, the intratheater airlift issue team created a definition of TS/MC movement requirements (see Glossary) that states dedicated airlift capacity must be available and extremely responsive to meet supported commanders' immediate operational or tactical priorities.

- Accordingly, the Department concludes joint force commander direct support airlift requirements for a theater of operations cannot be routinely satisfied through a common-user airlift service.

Maximizing Use of Today's Airlift Assets. The Department evaluated four options for how intratheater airlift responsibilities could be assigned to the Services. These options ranged from assigning all significant fixed-wing airlift (such as the C-27J) to the Air Force for both general and direct support, to the Army employing all Joint Cargo Aircraft exclusively in direct support of Army forces.

- The Department found the option that provided the most value to the joint force was to assign the C-27J to the Air Force and Army. This will allow all C-27J aircraft to conduct operations identified in the Joint Cargo Aircraft Concept of Operations, with the ability to alternate between either role, regardless of Service alignment, similar to how strategic airlift aircraft alternate from intertheater to intratheater airlift.[6] A challenge to this approach is a need to gain requirement visibility and access to available/allocated airlift capacity.

Increasing Visibility of Airlift Requirements and Capacity. U.S. Transportation Command recently conducted an assessment of organizational options for Operational Support Airlift aircraft, which normally perform organic direct support missions.

- An assessment recommendation accepted by the Department is to employ the Joint Airlift Logistics Information System – Next Generation across all Geographic Combatant

[6] The Joint Cargo Aircraft Concept of Operations specifies the Air Force provides a common-user pool, while the Army provides Time Sensitive/Mission Critical direct support to Army forces.

Command theaters to standardize the airlift process and gain visibility over direct support requirements and available capacity. Shared visibility and joint oversight maximizes potential use of airlift assets while ensuring they remain under Service component control to meet TS/MC movement needs. Although this effort focuses on improving visibility of Operational Support Airlift operations, expanding it to increase the enterprise-wide visibility of *all* airlift requirements and operations is the Department's desired objective.

Common Deployment and Distribution Control Mechanisms. The Department recognizes the need for improving mechanisms to control deployment and distribution operations at the theater level to maximize airlift potential.

- To meet this need, U.S. Transportation Command, in conjunction with the Services and Geographic Combatant Commanders, is pursuing common supporting capabilities to enhance airlift aircraft employment and data visibility as part of a joint, integrated enterprise. One successful initiative is implementation of the Joint Deployment Distribution Operations Centers within Geographic Combatant Command structures to better integrate and optimize distribution operations.

Operations centers, such as this one in Qatar, enable the flexible use of airlift aircraft to alternate between mission areas. The USCENTCOM Joint Deployment Distribution Operations Center in Kuwait has significantly improved the ability to effectively and efficiently coordinate movement operations.

U.S. Air Force photo by SrA Brian Ferguson

Updating the Joint Cargo Aircraft Concept of Operations. As a result of the QRM, the Air Force, Army, and U.S. Transportation Command are updating the Joint Cargo Aircraft Concept of Operations and revising the Services' Joint Cargo Aircraft Memorandum of Agreement to fully embrace multi-use of the C-27J across traditional Service employment roles. Specifically, the Air Force will make necessary adjustments to ensure the Air Force C-27J can conduct Army direct support missions when requested, and the Army will make certain its C-27J variant can be fully integrated into a common-user airlift system when available/allocated.

Adapting Airlift Policy and Doctrine. Finally, the Department will take action to ensure its airlift vision and need to maximize the utility of intratheater airlift aircraft, including contracted airlift, is addressed through changes to policy and doctrine, including Department of Defense Instruction 4500.43 (*Operational Support Airlift);* Joint Publication 3-17 (*Joint Doctrine and Joint Tactics, Techniques, and Procedures for Air Mobility Operations);* and Joint Publication 3-30 (*Command and Control for Joint Air Operations).*

Looking Forward. The 21st Century operational environment demands responsive theater airlift capabilities. The ability to provide a balanced application of airlift across the theater is the key to operational flexibility. Developing common capabilities and processes for sharing movement requirements and accessing airlift capacity provides the means to optimize scarce intratheater airlift assets, and will be a focus in the future. Continuing to bridge traditional boundaries for airlift general support and direct support requires sustaining the ongoing partnership between the Services and Geographic Combatant Commanders, and the support of Congress, to enhance joint operations and maximize warfighter support.

D. Unmanned Aircraft Systems / Intelligence, Surveillance, Reconnaissance

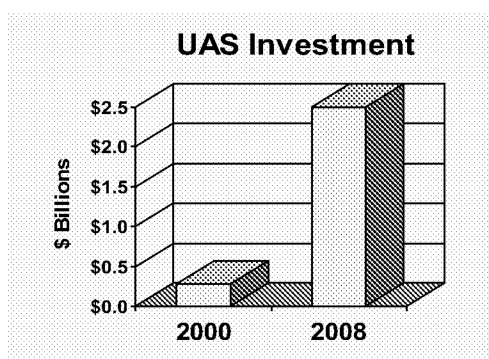
Executive Summary. Persistent reconnaissance and surveillance capabilities provided by Unmanned Aircraft Systems (UAS) have proven invaluable force multipliers in Iraq and Afghanistan. Consequently, the Department has experienced a dramatic increase in operational demand for UAS assets. In response, the Department has significantly increased investment in new Unmanned Aircraft Systems / Intelligence, Surveillance, and Reconnaissance (ISR) platforms, sensors, payloads and architectures. Concurrent with growing demand for UAS/ISR systems, the rapidly evolving operational battlespace has led to new and emerging mission sets which present challenges and opportunities for developing, acquiring, and employing UAS/ISR capabilities.

The Department's vision is to integrate UAS/ISR capabilities seamlessly into the Intelligence Enterprise in support of warfighters and the nation.

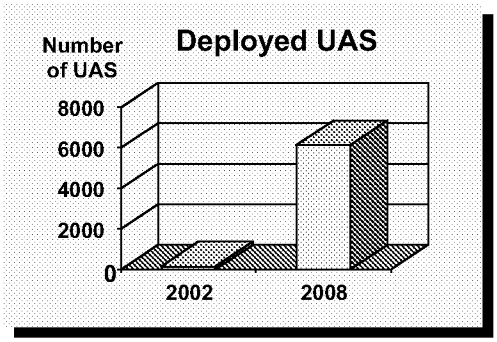
The Department has determined it is appropriate for each Service to develop, acquire, and operate unmanned aircraft systems, while developing and implementing improvements to increase jointness and interoperability of UAS/ISR capabilities. During the QRM, a UAS/ISR issue team, co-led by the Under Secretary of Defense for Intelligence and U.S. Strategic Command, developed steps to address challenges associated with UAS/ISR planning and direction; Tasking, Processing, Exploitation, and Dissemination (TPED); data standards and interoperability; communications architecture; and airspace access. These initiatives, which address improvements in oversight, integration, and interoperability of UAS/ISR capabilities, will collectively achieve significant increases in the Department's warfighting effectiveness.

An Army infantryman with 82nd Airborne Division at Fort Bragg NC prepares to launch a RQ-11 Raven UAS into the air. The Raven is a Group 1 UAS (see Glossary for UAS category description). UAS are employed at all echelons of command to meet reconnaissance, surveillance, and target acquisition needs.

UAS/ISR Challenges. Warfighter demand for UAS/ISR capabilities has increased exponentially over the past several years, due in large part to the unique operational needs of ongoing irregular warfare operations in Iraq and Afghanistan. These operations often require General Purpose Forces and Special Operations Forces operating in tandem to find and track mobile, elusive and fleeting targets, rather than traditional imaging of fixed, structural targets. Given their ability to provide a persistent aerial reconnaissance and surveillance capability against these highly perishable targets, UAS are increasingly tasked to support irregular warfare missions. UAS have surpassed 500,000 flight hours supporting operations in Iraq and Afghanistan alone. The



Growth in UAS Investment



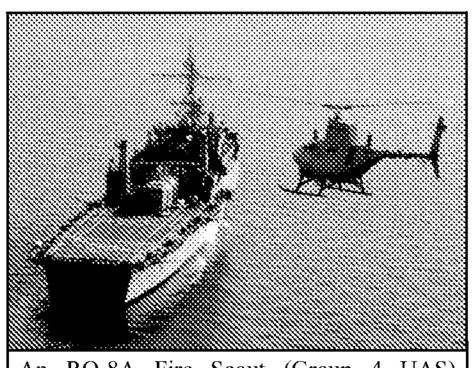
Growth in UAS Deployments

significant increase in demand for UAS/ISR capabilities is also driven by our military's ability and need to engage targets with high precision around the globe. The Department continues to progress toward meeting increased demand for UAS/ISR capabilities. For example, the number of deployed UAS has increased from approximately 167 aircraft in 2002 to over 6,000 in 2008, while defense investment in UAS capabilities has dramatically grown from $284 million in Fiscal Year 2000 to $2.5 billion in Fiscal Year 2008. While it is clear warfighters understand the essential capabilities UAS deliver to the fight, it is also clear that new missions and future applications present long-term challenges and opportunities for the development, acquisition and employment of these critical systems.

UAS/ISR Vision. The future vision for UAS/ISR capabilities is in concert with the 2008 *Defense Intelligence Strategy*, which calls for a fully and seamlessly integrated Intelligence Enterprise. To achieve this vision, UAS/ISR capabilities must be developed, acquired, and operated in a manner which allows full integration of collected intelligence from the tactical to national levels. The Department will continue to provide direction and advocacy to coordinate UAS/ISR development and acquisition across the Services, Combat Support Agencies, Combatant Commands, and our interagency partners. Future UAS/ISR capability enhancements will focus on increasing aircraft performance and improving communications, data links, and weapon and sensor payloads.

Decisions and Initiatives. The Department has determined the following initiatives hold the most potential for significantly enhancing warfighting effectiveness and avoiding unnecessary duplication of effort.

Planning and Direction for ISR Support to Warfighters. The Defense Department has well-established processes for determining joint force priorities. However, the highly dynamic environment of current operations in Afghanistan and Iraq, along with other new and emerging requirements, have stressed our ability to plan for and provide sufficient UAS/ISR capabilities. Recognizing this, the Department has developed new, more responsive oversight, guidance development, and planning structures and processes. These changes will help the Department better define joint UAS/ISR priorities and integrate multi-mission capable UAS/ISR collection, processing, exploitation, analyses and dissemination activities.



An RQ-8A Fire Scout (Group 4 UAS) Vertical Takeoff and Landing Tactical Unmanned Aerial Vehicle (VTUAV) System prepares to land aboard the amphibious transport dock ship USS Nashville (LPD 13).

- In concert with the Department's Joint Capability Integration and Development System, the Battlespace Awareness Capability Portfolio Management process identifies and mitigates ISR capability gaps. Leveraging these processes, the Under Secretary of Defense for Intelligence and U.S. Strategic Command, as the warfighters' ISR proponents, work together to champion resources needed to meet Combatant Commanders' UAS/ISR priorities.

- The Deputy Secretary of Defense has directed the Undersecretary of Defense for Acquisition, Technology and Logistics to lead a UAS Task Force to develop initiatives that will enhance operations, enable interdependencies across the Department's Components, and streamline UAS acquisition. Additionally, the Department chartered the U.S. Joint Forces Command Joint UAS Center of Excellence to support Combatant Commanders and Military Departments by facilitating development and integration of common UAS operating standards, capabilities, doctrine and training.

A fully armed MQ-9 Reaper (Group 5 UAS) taxis before a mission in Afghanistan. The MQ-9 Reaper provides persistent surveillance and target engagement capabilities to warfighters in Iraq and Afghanistan.

U.S. Air Force photo by Staff Sergeant Brian Ferguson

- A Department of Defense ISR Task Force is focused on leveraging all elements of the Intelligence Community to rapidly acquire and deploy ISR assets in support of U.S. Special Operations Command and U.S. Central Command operations in Iraq and Afghanistan. The ISR Task Force is integrating ISR and strike capabilities while working toward mainstreaming and institutionalizing UAS/ISR related processes in the Department's Planning, Programming, Budgeting, and Execution cycle.

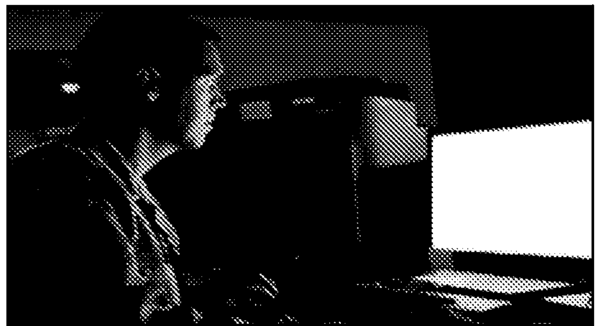
- U.S. Strategic Command is leading efforts to develop an ISR Force Sizing Construct for the Department. This initiative will develop a sound analytical foundation for future ISR allocation and procurement decisions.

- The Department has completed a Persistent ISR Joint Capabilities Document which identifies needed improvements to provide joint force commanders with more effective capabilities. The two highest priority capability gaps identified are attaining broad visibility and traceability throughout the intelligence collection, analysis, and distribution process, and improving multi-intelligence collection strategies in support of joint force commanders.

- In October 2007, the Department took a major step toward improving the Defense ISR Operations Enterprise by integrating functions performed by U.S. Strategic Command's Joint Functional Component Command for ISR and the Defense Joint Intelligence Operations Center to form the Defense Intelligence Operations Coordination Center (DIOCC). The DIOCC is responsible for validating, recommending priorities, and registering defense intelligence collection requirements, including UAS/ISR requirements, with the Intelligence Community. As the DIOCC continues to mature, its alignment with the National Intelligence Coordination Center will improve their rapid synchronization and timely operational support to Combatant Commanders.

<u>Tasking, Processing, Exploitation, and Dissemination (TPED)</u>. TPED comprises the people, processes, and systems that transform collected data into operationally executable intelligence.

TPED enables warfighters to request collection and intelligence products tailored to meet their operational needs. TPED is vital to the effectiveness of any ISR system, and TPED implications must be considered when planning UAS acquisition and employment. Currently, requirements for UAS-derived actionable intelligence outpace TPED capacity, and future projections suggest this mismatch will continue temporarily. Over time, multiple TPED processes have been created to support UAS operations. Furthermore, the breadth of current and emerging UAS/ISR missions have caused TPED processes and systems associated with each intelligence discipline (signals, imaging, etc.) to differ across the Services, Combat Support Agencies, and from national to tactical assets and applications. As a result, the Department's ability to accurately define TPED mission needs has not kept pace with the rapid development and employment of UAS/ISR capabilities. Accordingly:


U.S. Air Force photo by Master Sergeant Steve Cushman

An imagery analyst at Langley Air Force Base, Virginia reviews previous damage assessments from Hurricane Katrina between contingency taskings from U.S. Central Command. Reach-back exploitation analysts provide tailored intelligence products to customers including SOF and domestic disaster relief agencies.

- The Department is leading a comprehensive effort to redefine TPED in order to enable Services and Combat Support Agencies to develop and operate the various TPED systems using common standards and rule sets. The Joint Staff, as part of the ISR Task Force, is addressing TPED issues and concerns across the Services, including capacity, manpower, storage requirements, technology, and exploitation/dissemination timeliness. The U.S. Joint Forces Command Joint UAS Center of Excellence will work with the Joint Staff and the Office of the Under Secretary of Defense for Intelligence to review UAS TPED-related tasks to establish basic training qualifications, standards, and objectives. Ultimately, the Department will establish a community-wide definition of TPED to support development of concept of operations, joint doctrine, and capability requirements documentation.

- The Under Secretary of Defense for Intelligence, in coordination with the Services, is sponsoring an annual Empire Challenge capability demonstration that provides a venue for UAS, ground station and TPED interoperability assessment. Empire Challenge provides a key opportunity to identify and correct interoperability issues uncovered during this month long series of test events.

<u>Data Standards and Platform Interoperability</u>. As Services and Defense Agencies develop UAS/ISR capabilities, collected data formats and transmission protocols must be standardized to ensure UAS/ISR platforms become truly interoperable with joint and service TPED architectures. Effective sensor data and metadata formats and standards will promote interoperability between the databases and ground stations—such as the Distributed Common Ground System—used by Combat Support Agencies, Services, Intelligence Community, and interagency partners. These systems are crucial to sharing data from national to tactical levels of operation.

- The Under Secretary of Defense for Acquisition, Technology, and Logistics, in concert with the Joint Chiefs of Staff, is developing a joint acquisition approach to satisfy warfighter requirements. This approach will capture the benefits of standardized platforms, communications and logistics.

- The Under Secretary of Defense for Intelligence, in conjunction with the Joint Chiefs of Staff and UAS Task Force, is addressing the need for a Joint Capabilities Document for UAS Interoperability to resolve UAS/ISR interoperability issues. This document will create the foundation that will lead to identification of information and communications architectures, sensor data and interoperability standards and provide a link to a Joint UAS Concept of Operations.


Airmen prepare to land an MQ-1 Predator (Group 4 UAS) at Ali AB Iraq. UAS/ISR operations rely upon robust communications architectures for command, control, and data dissemination.

U.S. Air Force photo by Airman 1st Class Christopher Griffin

Communications Architecture. UAS/ISR relies heavily on communications to command and control aircraft and sensors for disseminating collected data. As the number of deployed UAS increase, more communication links, bandwidth and spectrum, and protected communications paths are required. Meeting the resultant frequency spectrum demand is a significant challenge. Furthermore, to meet increased warfighter demands for ISR support, the Services have developed methods for employing UAS tailored to their individual operating environments. However, one Service's methods may not be consistent with other Service or joint communications architectures. While Service-specific methods have delivered capability to warfighters, a more comprehensive approach will ensure communication demands are better managed to improve interoperability and cross-Service support, especially when satellite support is constrained or not possible. Accordingly:

- The UAS Task Force has identified the need to: (1) ensure effective spectrum planning and guidelines are incorporated into all UAS development efforts; and (2) Service and joint oversight verify compliance with these guidelines.

- The Department is expanding its Airborne Intelligence Surveillance and Reconnaissance Model to include all those entities requiring connection to the communications architecture. This change will better enable the Department to model and plan for dynamic communications architecture requirements.

Airspace Access for Operational and Training Missions. Combat effectiveness of our joint warfighters requires UAS to operate safely, efficiently, and have readily-available access to the National Airspace System. By 2013, the Services estimate they will require over one million flight hours for UAS operational and training missions. Due to high mission demands and limited restricted airspace availability, the majority of UAS flight hours will be accomplished outside of restricted airspace. Accordingly, the Department is seeking to better define technological, procedural, and standardized training qualifications to ensure UAS have access to appropriate classes of airspace to fulfill Service and national needs. This effort will require a concerted approach by the Department working alongside federal, state and civilian organizations. In support of this objective:

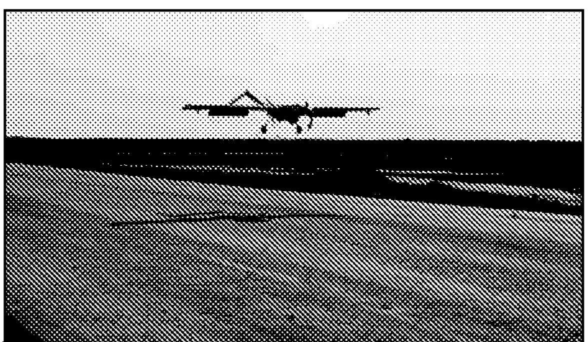
- The UAS Task Force is developing an 18 month plan that focuses on alleviating flight restrictions for all classes of UAS and supports near-term Service operational and training requirements in the National Airspace System.

An RQ-4 Global Hawk (Group 5 UAS) unmanned aerial vehicle is towed back to its hangar following a mission at a deployed location in Southwest Asia. The Global Hawk requires access to all classes of airspace for the conduct of operational and training missions.

- U.S. Joint Forces Command Joint UAS Center of Excellence is leading a coordinated review of current and future Department UAS airspace access requirements for all classes of UAS, and leading a Service review to develop a minimum set of UAS pilot/operator qualification requirements and/or standards to operate in the National Airspace System.

- U.S. Joint Forces Command Joint UAS Center of Excellence has identified three areas necessary to ensure access to applicable classes of the National Airspace System: (1) Airworthiness Certification; (2) establishment of standardized basic UAS qualifications consistent with Federal Aviation Administration guidelines for each class of airspace; and (3) development of sense and avoid technology. Working with the Services, the U.S. Joint Forces Command Joint UAS Center of Excellence will ensure these areas are addressed during UAS development.

Looking Forward. Capabilities provided by UAS are essential to today's warfighters. With newly emerging UAS missions and still-maturing ISR applications, the Department is aggressively pursuing opportunities to improve development, acquisition and employment of UAS. The Department's vision of seamlessly integrating UAS/ISR capabilities into the Intelligence Enterprise requires developing interagency and Congressional partnerships to increase airspace access and improve communications connectivity around the globe. Additionally, the Defense Department must better integrate its capabilities with growing UAS efforts of other federal agencies and partner nations. With the support of the Congress, the Department will continue to appropriately resource UAS platforms and associated TPED support to meet growing warfighter demand for ISR capabilities.



An RQ-7B Shadow (Group 3 UAS) begins its landing sequence following a flight to provide troops operating in Iraq with another set of eyes. Shadows are employed by the Marine Corps and Army.

V. The Road Ahead: Interagency Opportunities

Today's complex security environment places increased demands on the capabilities and resources of departments and agencies across the U.S. Government. Individually, departments and agencies are not as effective as when we unify our actions toward achieving a common vision. The Department strongly supports initiatives to increase unity of effort across the government for addressing our common national security problems. While significant progress toward this end has been made over the past five years, continued improvement requires a sustained focus on developing whole-of-government strategies and plans, as well as addressing operational seams between military and civilian agencies. During the QRM, the Department explored interagency issues and problems associated with key national security challenges, including cooperative security, stability operations, irregular warfare, and homeland defense and civil support. While these activities are core mission areas for the Department, they require substantial military and civilian interaction. QRM results affirm our need to continue to strongly support initiatives to build a cohesive, whole-of-government approach to our Nation's enduring security challenges.

The Department's vision is to support maturation of whole-of-government approaches to national security problems. Solutions to address strategic and operational security challenges will be based on employing integrated flexible, mutually-supporting interagency capabilities.

Vision. The Department supports institutionalizing whole-of-government approaches to addressing national security challenges. The desired end state is for U.S. Government national security partners to develop plans and conduct operations from a shared perspective. Toward this end, the Department will continue to work with its interagency partners to plan, organize, train, and employ integrated, mutually-supporting capabilities to achieve unified action at home and abroad.

An Afghan engineer talks with a member of the Nangarhar Provincial Reconstruction Team at a metal working shop in the Nangarhar province of Afghanistan. The team assesses community needs and builds schools, government centers, roads, medical facilities and basic infrastructure throughout the area.

Photo by Staff Sergeant Joshua T. Jasper, U.S. Air Force

- An essential element of this vision is establishing a coherent framework for developing whole-of-government approaches for addressing national security challenges. A framework that includes commonly understood strategic concepts, operational principles, relationships between agencies, and roles and responsibilities would help delineate how to best coordinate and synchronize efforts as well as transition between military-led and civilian-led activities during operations.

- As proposed by the 2006 QDR, whole-of-government national security planning would be facilitated by publishing an authoritative national-level strategic guidance document that addresses interagency roles and responsibilities, resolves seam issues between agencies, and establishes priorities for planning and development of each organization's capabilities.

- Perhaps the most important critical element of this vision is the human dimension – developing a federal workforce trained and educated in a manner that fosters mutual understanding across agencies, expands knowledge of other agencies' roles and missions, and increases opportunities for building relationships across the Federal Government as well as with state and local governments.

Initiatives. As summarized throughout this report, the Department is pursuing initiatives to address our internal roles and missions issues. However, QRM results also reinforce the need for the Department to continue to work with our national security partners on complex roles and missions seam issues. To advance whole-of-government solutions, the Department strongly supports the following initiatives.

<u>Strategic and Operational Planning</u>. Several ongoing initiatives will improve how the interagency conducts national level planning.

- The Department of Defense and Department of State, in coordination with other agencies, are building an interagency planning framework to provide a prevention, response, and contingency capability to address foreign states at risk or in the process of instability, collapse, or post-conflict recovery.
  - This initiative to develop a whole-of-government planning approach and supporting tools are the result of National Security Presidential Directive 44 (and is now authorized under Title XVI of the 2009 National Defense Authorization Act). Led by the Department of State's Coordinator for Reconstruction and Stabilization, this planning framework is supported by the Interagency Management System (IMS), which provides a structure for civilian planning and implementation of reconstruction and stabilization activities at the strategic, operational, and tactical level. The IMS structure is also built to interface and integrate with existing military organizations when necessary. The capacity for the IMS is provided by the Department of State's as yet fully implemented or funded Civilian Stabilization Initiative, of which the Civilian Response Corps was recently partially funded via supplemental appropriation.


A Civil Affair unit member with the Parwan Provincial Reconstruction Team (PRT) hands out toys at a school opening in Kabul, Afghanistan.

- The Department is working with the U.S. Agency for International Development to improve collaboration, coordination, and synchronization of existing foreign-based strategic guidance and operational plans to take advantage of lessons learned from recent operations. The newly published U.S. Agency for International Development "Civil-Military Cooperation Policy," which calls for improved coordination with the military, demonstrates significant potential. The Department of Defense will continue to support this positive step towards creation of mutually supportive development-based and military-based plans.

- For homeland security, the Departments of Defense and Homeland Security are establishing a pilot Task Force for Emergency Readiness consisting of a small group of interagency planners to develop plans that ensure a whole-of-government response to disasters. The task force will integrate local, state, and federal organizations, as well as the private sector. The pilot task force will begin in five states within the next calendar year.

- At the national level, the Department supports development of a whole-of-government strategic planning document that outlines national objectives, priorities and specific actions for improving interagency coordination and operational planning.

Concept Development. Over the last several years, the Department has developed Joint Operating Concepts that propose future interagency activities, including concepts for cooperative security, irregular warfare, stability operations and homeland defense and civil support. These JOCs were developed in informal collaboration with the Department of State and other agencies. Although they incorporate a broader interagency perspective than previous Department-centric documents, there are opportunities for continued improvement, to include conducting comprehensive whole-of-government capability and capacity gap analyses across all lines of operation.

- The Department of Defense advocates establishing a formal forum for collaborating with other elements of the U.S. Government on Joint Operating Concepts. The objective is to continue to evolve JOCs into truly whole-of-government concepts that would better define responsibilities across the whole-of-government, such as border security, disaster relief operations abroad, and domestic counterterrorism security programs, among other shared security challenges.

A member of the U.S. Navy amphibious assault ship USS Kearsarge (LHD 3) provides medical care during hurricane relief operations in Haiti. The Department of Defense advocates expanding whole-of-government collaboration on concepts such as disaster relief operations abroad.

Authorities and Resources. Fiscal Year 2006 National Defense Authorization Act Section 1206 "Global Train and Equip" and Section 1207 "Security and Stabilization Assistance" authorities have proven highly effective at combining assets to address urgent national security problems. These programs recognize the need to augment, not supplant, what other agencies can bring to the table – particularly the Department of State and U.S. Agency for International Development – with Defense Department capabilities that address mutual needs in the field.

- Internally, the Department will continue developing capabilities for stabilization, reconstruction, foreign internal defense, and counterinsurgency operations supported by force growth initiatives, new doctrine, operational concepts, adjusting roles of the civilian work force, and enhancing training and education.

- Externally, the Department will continue to collaborate with the Congress and Department of State to explore new authorities that would better integrate capabilities and funding priorities for these shared missions.

- The Department of Defense strongly supports the State Department's Civilian Stabilization Initiative budget request to continue development of expeditionary civilian capabilities in eight U.S. Government departments and agencies.

Interagency Secure Communications Challenges. While all agencies can communicate on unclassified networks, not all agencies and departments required to plan and conduct operations together are able to communicate with each other on classified networks. For example, information sharing between Federal Government departments and local/state entities involved with homeland security is predominately over unclassified networks. Similarly, information sharing concerning other threats, emergency and disaster management, planning, and other domestic security and response is underdeveloped.

- In cooperation with its interagency partners, the Department will continue to aggressively pursue solutions that ensure it can communicate over classified networks with critical domestic partners.

National Security Professional Development. Many lingering challenges between interagency staffs may be partially attributable to a lack of understanding and appreciation of each others' organizational cultures, priorities, requirements, and practices. Traditionally, civil servants and military members have few formal opportunities for interagency training, education, and professional development. Beyond rudimentary familiarization at staff courses, personnel systems have not typically encouraged professional development that fosters a deep understanding of other agencies. In 2007, the President directed the creation of a "National Security Professional Development" system to address these cross-agency challenges.

- In support of national security professional development, the Department is working proactively with its partners to provide more students from other agencies access to courses at Defense Department educational institutions, notably the National Defense University.

Future Opportunities.

Conducting Stabilization and Reconstruction Operations. Today, military forces are conducting a wide range of civil-military operations and activities, including security and policing assistance, humanitarian relief, reconstruction, governance, civil capacity building, medical and security cooperation. Hardly new to the Department, military forces have performed these missions for more than a century and likely will continue to do so in the future. However, recent operations have exposed gaps between civilian and military capabilities, and highlighted a need to develop a better understanding of how civilian-military efforts must be mutually supportive and when operations should transition between military-led and civilian-led activities. National Security Presidential Directive (NSPD) 44 *"Management of Interagency Efforts Concerning Reconstruction and Stabilization"* and Title XVI of the 2009 National Defense Authorization

Act have made a substantial first step in building interagency capabilities and conducting strategic and operational planning.

- While NSPD-44 and Title 16 of the 2009 National Defense Authorization Act broadly define responsibilities of various departments during foreign stabilization and reconstruction operations, full realization of the ongoing capabilities development for these types of operations will not be realized without full funding of the Civilian Stabilization Initiative.

Resources to Increase Civilian Expertise. Lessons learned in recent operations stress the critical need to further develop deployable civilian expertise for conducting stabilization, reconstruction, and counterinsurgency operations. Today, civil agencies and departments have insufficient resources for carrying out missions associated with transition from violence to lasting stability.

- Accordingly, the Department supports establishing a better balance between the civil and military instruments of national power by significantly increasing resources needed for governance, strategic communication, security assistance, civic action, and economic reconstruction and development.

Strategic Communication. The Department of Defense recognizes strategic communication as a process through which information activities (including public affairs, psychological operations, information operations, public diplomacy, and policy) are harmonized and synchronized with other operations. The Department will continue to improve the alignment of actions and information with policy objectives to integrate strategic communication into defense missions and to support larger U.S. policies as well as the State Department's public diplomacy priorities.

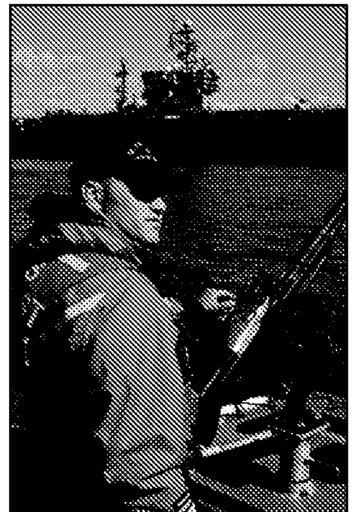
- The Department has significant capabilities and resources to support strategic communication priorities, particularly to counter ideological support to terrorism in Iraq and Afghanistan. We are committed to using our operational and informational activities and strategic communication processes in support of the Department of State's broader public diplomacy efforts. This cooperation will better enable the U.S. Government to engage foreign audiences holistically and with unity of effort.

- The Department of Defense and Department of State will expand our partnership to conduct strategic communication planning in support of the Global War on Terror, building partnership capacity, and regional issues. This partnership encompasses the full range of information and Theater Security Cooperation activities to synchronize efforts; improve regional and cultural expertise; develop and deliver information products; and train international partners to build their information networks.

Authorities and Oversight. Funding and authorities dedicated solely to individual agencies may not be sufficient to ensure that the activities of multiple agencies are fully integrated and that all seam issues between organizations are addressed. "Stovepiped" funding and authorities could have the unintended effect of encouraging the development of uncoordinated approaches to national security challenges as well as unneeded competition between departments and agencies.

- The Department recognizes the need for authorities and approaches to funding for whole-of-government operations.

Looking Forward. In summary, the Department of Defense places a high priority on integrating whole-of-government capabilities to deal with shared challenges to our Nation's security. Future conflict will require integrated planning and implementation efforts as well as smooth transitions between our military forces and civilian counterparts, not just to win wars, but to prevent them and mitigate the underlying causes of conflicts and instability. In order to plan and execute essential national security tasks at home and abroad, we seek to increase defense and civil support and building partnership capacity in addition to fielding fully-ready joint forces. Since our Nation's future security depends equally on interagency cooperation, coordination, and integration efforts, building unity of effort requires us to expand the concept of jointness beyond the Department of Defense. To help establish the right balance between our Nation's capabilities, we strongly support increasing resources and capacities in other departments and agencies, notably the Department of State and the U.S. Agency for International Development.



A Coast Guard Petty Officer from Winthrop, MA mans a M-240 machine gun aboard a rigid hull inflatable boat as the conventionally-powered aircraft carrier USS John F. Kennedy (CV 67) moves into port.

U.S. Coast Guard photo by Public Affairs Specialist 3rd Class Lisa Hennings

GLOSSARY

The following information on specific concepts, processes, and definitions supplement text in the Quadrennial Roles and Missions Review Issue Team sections.

A. Irregular Warfare Key Terms and Concepts

- **Counterinsurgency (COIN):** Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency.

- **Counter-terrorism (CT):** Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism.

- **Foreign Internal Defense (FID):** Participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, and insurgency.

- **General Purpose Forces (GPF):** All forces except Special Operations and Strategic Forces. General Purpose Forces are not limited to any one domain (i.e., General Purpose Forces are not only ground forces).

- **Irregular Warfare:** A violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will.

- **Special Operations Forces (SOF):** Those Active and Reserve Component forces of the Military Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations.

- **Stability Operations:** An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.

- **Unconventional Warfare (UW):** A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery.

B. Cyber Key Terms and Concepts

- **Cyberspace:** A global domain within the information environment consisting of the interdependent network of information technology, infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

- **Global Information Grid (GIG):** The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems.

C. Intratheater Airlift Key Terms and Concepts

- **Time Sensitive / Mission Critical (TS/MC) Movement Requirements:** Justification for organic transportation assets to conduct direct support mission are based on need to satisfy TS/MC requirements. TS/MC requirements create a demand for delivery of equipment, supplies, and personnel that are generally non-routine in nature and must be delivered to the point of need or point of effect in an accelerated time period. These demands require the lift capacity to be supremely responsive to the supported commander's immediate operational or tactical priorities. TS/MC demands cannot routinely be accommodated via planned resupply and movement processes where efficiency is the primary consideration. (Note: Although no specific response time is specified, depending on the operational scenario and unit mission, TS/MC movement requirements are usually conducted with less than 24 hours notice.)

- **Point of Need:** A physical location designated by the JFC as a receiving point for forces or commodities, for subsequent employment, emplacement, or consumption.

- **Point of Effect:** A physical location designated by the functional component commander, Service component commander or a subordinate commander to support operations normally within the combat zone.

- **Port of Debarkation (POD):** The geographical point at which cargo or personnel are discharged. This may be a seaport or aerial port of debarkation; for unit requirements; it may or may not coincide with the destination.

- **Port of Embarkation (POE):** The geographic point in a routing scheme from which cargo or personnel depart. This may be a seaport or aerial port from which personnel and equipment flow to a port of debarkation; for unit and non-unit requirements, it may or may not coincide with the origin.

D. Unmanned Aircraft Systems / Intelligence, Surveillance, Reconnaissance Key Terms and Concepts

- **Command and Control:** The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2.

- **Unmanned Aircraft System (UAS):** The system, whose components include the necessary equipment, data communication links, and personnel to control and employ an unmanned aircraft. The unmanned aircraft system is composed of six components: the aircraft, payloads, data communication links, ground control stations, ground support equipment, and ground operators.

- **JUAS Categories:** A classification system for current UAS based primarily on a categorization schema that groups UAS according to three enduring attributes: UA weight, normal operating altitude, and speed.

    - **Group 1 UAS.** UAS typically less than 20 pounds in weight and normally operate below 1,200 feet Above Ground Level at speeds less than 250 knots

    - **Group 2 UAS.** UAS in the 21 – 55 pound weight class and normally operate less than 3,500 feet Above Ground Level at speed less than 250 knots.

    - **Group 3 UAS.** UAS weigh more than 55 pounds, but less than 1320 pounds. They normally operate below 18,000 feet Mean Sea Level at speeds less than 250 knots.

    - **Group 4 UAS.** UAS weigh more than 1,320 pounds and normally operate below 18,000 feet Mean Sea Level at any speed.

    - **Group 5 UAS.** UAS weight more than 1,320 pounds and normally operate higher than 18,000 feet Mean Sea Level at any speed.

E. Interagency Opportunities Key Terms and Concepts

- **Strategic Communication:** Focused U.S. Government processes and efforts to understand and engage key audiences to create, strengthen or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power.

QRI1

Automatic Dependent Surveillance Broadcast (ADS-B)

Surveillance development for Air Traffic Management

As air traffic is predicted to increase steadily over the coming years, there is a clear need to ensure that standards of safety and efficiency are maintained, or even enhanced. This is recognized by the Single European Sky programme in Europe (SESAR) and the NextGen programme in the U.S.A. (read FAST article - Demonstrating the green trajectory), the two major bodies driving the Air Traffic Management (ATM) development over the coming years.

Automatic Dependent Surveillance Broadcast (ADS-B) is all about communications between aircraft, and also between aircraft and ground. Both are vital in ensuring safe flights and efficiency in terms of fuel use, time and emissions. ADS-B is an integral part of the planned efficiency drive towards 2020.

Taking advantage of the latest technology, ADS-B is designed to be retrofit on aircraft flying today. Here, we will look at aspects associated with the retrofit and take a look at the developments that are planned for the future.

Christine VIGIER
Design Management Avionics
Airbus Upgrade Services

ADS-B summary

In its final form, ADS-B is designed to ease Air Traffic Control (ATC) as the number of approaches grows, enhancing safety and increasing airport capacity.
In the air, the information provided by ADS-B enhances the pilots' traffic awareness, allowing more optimal flight levels leading to fuel savings.
ADS-B is considered in two parts as described:

- ADS-B OUT provides a means of automated aircraft parameter transmission between the aircraft and the ATC.

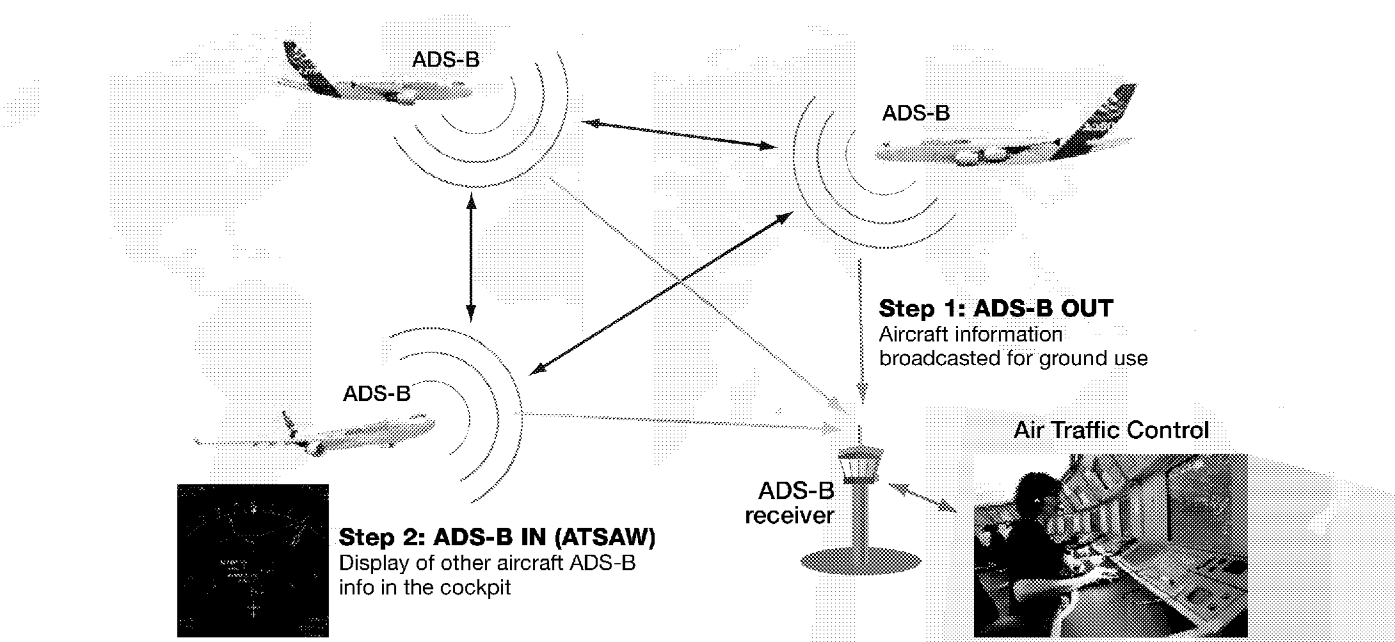
- ADS-B IN provides automated aircraft parameter transmission between aircraft themselves.

glossary

ADC: Air Data Computer
ADIRS: Air Data/Inertial Reference System
ATC: Air Traffic Control
ATSAW: Air Traffic Situational Awareness
DMC: Display Management Computer
EHS: Enhanced Surveillance
EIS: Electronic Instrument System
FCOM: Flight Crew Operating Manual
FM: Flight Manual
FMS: Flight Management System
FWC: Flight Warning Computer
GPS: Global Positioning System
HFDR: High Frequency Data Radio
IRS: Inertial Reference System
MCDU: Multi-purpose Control Display Unit
MMR: Multi-Mode Receiver
NRA: Non-Radar Airspace
OANC: On-board Airport Navigation Computer
OANS: On-board Airport Navigation System
OMS: On-board Maintenance System
SATCOM: Satellite Communication
SPI: Special Position Identification

First steps involved in ADS-B

Figure 1



ADS-B OUT

Figure 2

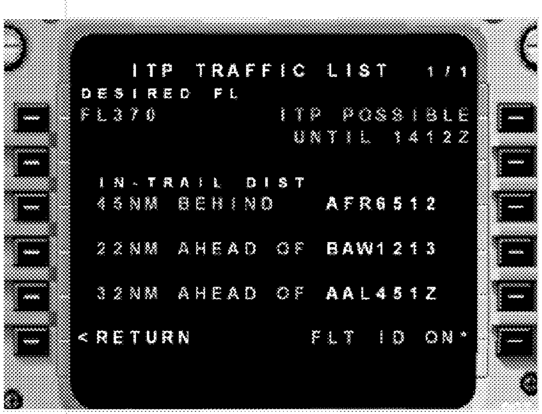
	DO-260	DO-260B
Equipment required	• ATC transponder enhanced capable • MMR (with GPS capability) • Wiring provision EHS	• ADS-B OUT DO-260B • FWC
Availability date	Now	As per mandate (refer to figure 10)

Example on MCDU

Figure 3

In this example, the MCDU (Multi-purpose Control and Display Unit) shows the identity and the relative horizontal position of three aircraft. The pilot can see immediately that a flight level change to FL370 is not possible until 1412Z time, as computed by the TCAS (Traffic alert and Collision Avoidance System).

A different flight level can be requested as clearly indicated, taking into account the surrounding aircraft positions, trajectories and speeds.



STEP 1: ADS-B OUT

ADS-B OUT automatically transmits aircraft parameters from the aircraft to the ATC on ground. There is no need for the pilot's action and it conforms to EASA regulations on ADS-B OUT, for Non-Radar Airspace (NRA) operations. The capability must be declared in the FCOM and the FM shall be updated (see figure 2).

STEP 2: ADS-B IN (ATSAW)

The Airbus approach to ADS-B IN is named the Air Traffic Situational Awareness (ATSAW) which enables the reception of ADS-B information from other aircraft in the vicinity. As for the ADS-B OUT, the capability must also be declared in the FCOM and the FM updated (figure 4).

ATSAW is splited in two steps:
- Step 2A: ATSAW operation in flight
- Step 2B: ATSAW operation on ground

STEP 2A: ATSAW OPERATION IN FLIGHT

a) ATSAW
- Improves cooperation with ATC (better understanding of ATC instructions),
- Improves the detection of opportunities for flight level changes in standard separation for reduced fuel savings and a reduction of CO_2 emissions,
- Improved efficiency on approach,
- Enhances identification and information on target aircraft,
- Increases runway capacity.

b) ATSAW with ITP (In Trail Procedures) today defined on the North Atlantic ocean (see figure 3):
- Enables more frequent altitude changes by temporarily reducing standard separation,
- Enables flying at the optimum flight level,
- Provides significant fuel savings.

STEP 2B: ATSAW ON THE GROUND

- Enhanced situational awareness during surface operations.

NEXT STEPS

STEP 3: SEQUENCING AND MERGING

The objective of the future step is to enable the flight crews to achieve and maintain automatically a given spacing with designated aircraft.
The two principle maneuvers are 'remain behind' and 'merge behind'.
The operational benefit will be the enhanced traffic regularity during the approach to airports with heavy traffic allowing increased airport capacity.

How does ADS-B work?

ADS-B OUT

It uses ATC transponders to transmit aircraft information to the ground, using the Mode S 1090 MHz Extended Squitter with a refresh rate of 0.5 seconds.

ADS-B IN (ATSAW)

Figure 4

	Step 2A	Step 2B
Equipment required	• ATC transponder EHS • MMR (with GPS capability) • EIS2 • Wiring provision • EHS traffic selector • FWC standard	As for Step 2A + OANC
Availability date	Early 2011	2013 TBC

Example on Navigation Display and MCDU

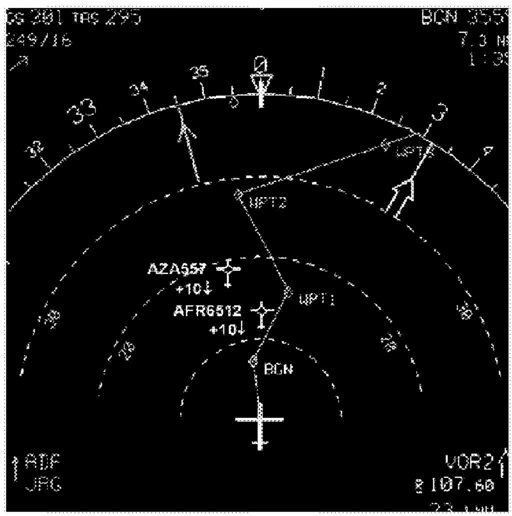


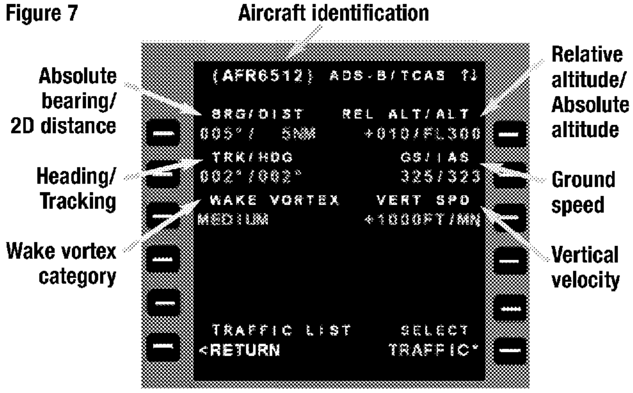
Figure 5

The Navigation Display (ND) shows the aircraft orientation and relative information from aircraft in the vicinity.

Figure 6

Additional information shown on the MCDU.

Figure 7



The Pilot elects to see more information on AFR6512 by the menu selection.

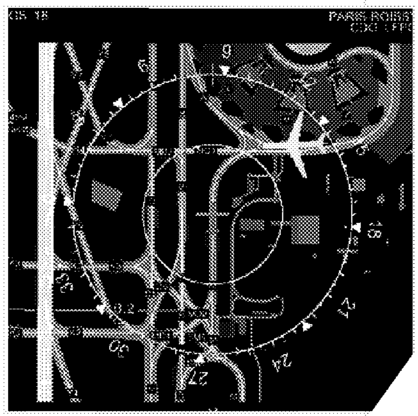
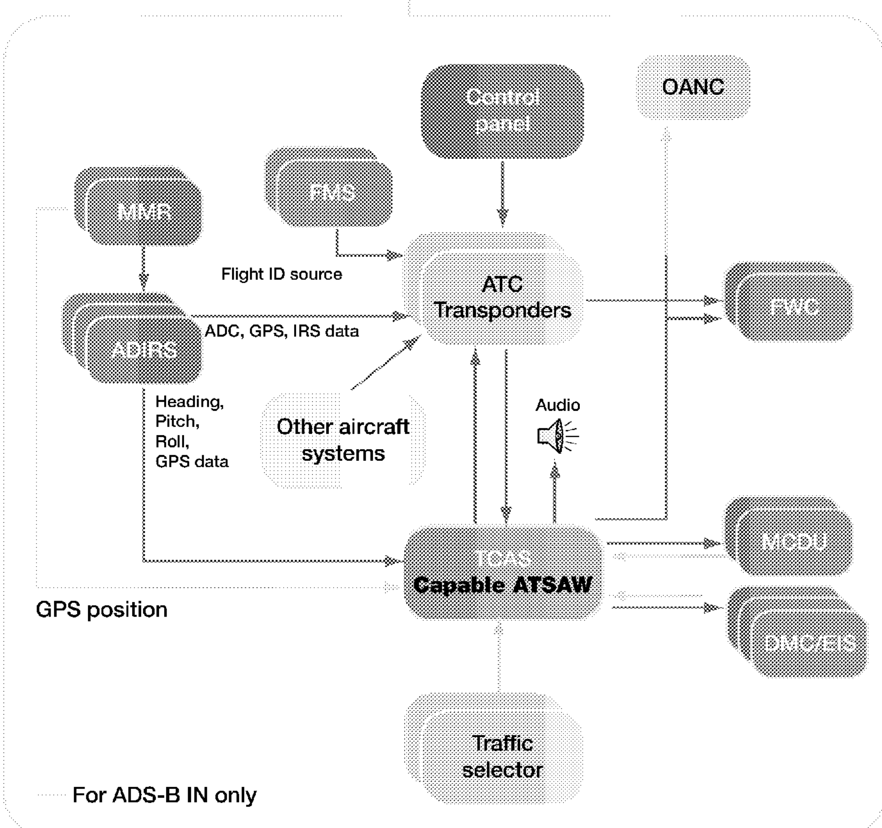


Figure 8

The ND indicates the position and trajectory of other aircraft on taxiways

Architecture for ADS-B OUT and for ADS-B IN

Figure 9



ADS-B IN

On aircraft, it is the TCAS computer that receives and treats the ADS-B information coming from ATC transponders of surrounding aircraft. The information is then displayed on the Navigation Display (ND) and the MCDU (see figures 5, 6 & 7). When ATSAW is activated and if the ADS-B information is available from aircraft in the vicinity, the following information is available for each pilot:

- Aircraft identification
- Absolute bearing/2D distance
- Heading/Tracking
- Wake vortex category
- Relative altitude/Absolute altitude
- Ground speed
- Vertical velocity

Aircraft architecture required for ADS-B OUT

ADS-B OUT NEEDS

- ATC transponders at minimum DO-260 standard.
- Additional wiring associated with peripheral equipment,
- MMR in hybrid architecture with GPS capability.

CURRENT FLEET STATUS

Aircraft currently flying in Europe are generally well equipped for the transition to ADS-B OUT as the prerequisite ATC transponders Mode S (DO-260) are already required to meet the former enhanced surveillance mandate. Aircraft greater than five years of age and operating outside of Europe are more likely to need a new transponder in order to achieve ADS-B capability.

ADS-B IN

STEP 2A

- TCAS capable
- Additional wiring
- Traffic selector in cockpit
- EIS2 capable

STEP 2B

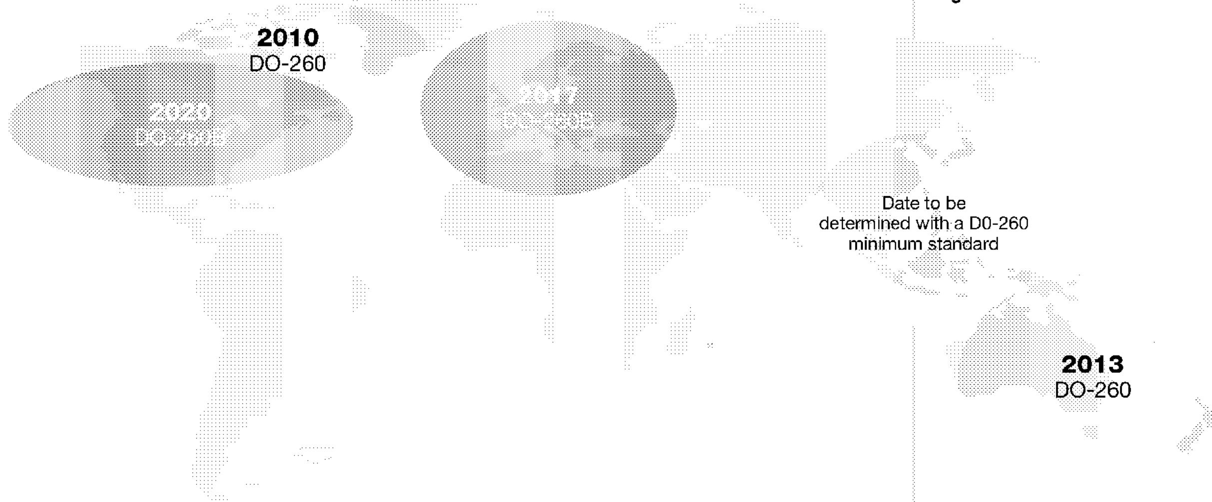
Step 2A + OANC
(On-board Airport Navigation Computer)

ADS-B IN TRIALS

To pioneer and test the new functions associated with ADS-B IN, trials are scheduled with the involvement of Eurocontrol and certain airlines which will have the ATSAW capability, some from production and others by retrofit. The European trials will commence in early 2011.

Mandates

Figure 10



ADS-B OUT MANDATES

Current operational requirements or mandates are already in service and others are anticipated. The figure 10 shows areas where a mandate already exists, such as the Hudson Bay, and also shows anticipated mandates in other regions. The upcoming mandates in Europe and North America require a new standard (DO-260B) which implies an upgrade to the FWC and connections between the MMR and the ATC transponder. This will enable additional benefits in terms of safety, flight efficiency and situational awareness, thanks to the GPS data enabling the transmission of more accurate information on aircraft positions and the improved latency in broadcasts.

CONTACT DETAILS

Christine VIGIER
Design Management Avionics
Airbus Upgrade Services
Tel: +33 (0)5 67 19 02 17
Fax: +33 (0)5 62 11 08 47
christine.vigier@airbus.com

Conclusion

Whilst the initial drivers from SESAR and NextGen are motivated by the need to maintain and where possible enhance safety standards, the commercial implications for operators are not forgotten. The benefits from the Automatic Dependent Surveillance Broadcast (ADS-B) are not only for Air Traffic Control (ATC), but also for the airlines, flight crew and passengers.

ADS-B OUT eases the flight crew and ATC workload, resulting in fuel and time savings thanks to more efficient approaches.

ADS-B IN presents additional opportunities for fuel and time savings, in particular by the utilization of 'In Trial Procedures' for long range flights in the oceanic airspace, maintaining safety.

ADS-B is in the early stages of a roadmap vision up until 2020 and has been adopted by SESAR and NextGen. Airbus Upgrade Services will continue to develop new solutions to ease flight operations, thus contributing to reduce the congestion in future Air Traffic Management.

EXPLOITING THE AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST SYSTEM VIA FALSE TARGET INJECTION

THESIS

Domenic Magazu III, Captain, USAF

AFIT/GCO/ENG/12-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCO/ENG/12-07

EXPLOITING THE AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST SYSTEM VIA FALSE TARGET INJECTION

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Domenic Magazu III, MS

Captain, USAF

March 2012

AFIT/GCO/ENG/12-07

EXPLOITING THE AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST SYSTEM VIA FALSE TARGET INJECTION

Domenic Magazu III, MS

Captain, USAF

Approved:

Robert F. Mills, PhD, (Chairman)	2 MAR 12 Date
David J. Robinson, Lt Col, USAF (Member)	3/9/12 Date
Jonathan W. Butts, Maj, USAF (Member)	2 Mar 12 Date

AFIT/GCO/ENG/12-07

Abstract

A new aircraft surveillance system, Automatic Dependent Surveillance-Broadcast (ADS-B), is being introduced by the Federal Aviation Administration (FAA) with mandated implementation in the United States by the year 2020. The rapid deployment of the system with current test-beds spread across the U.S. leaves very little chance for anyone to test the abilities of the system and more importantly the flaws of the system.

The research conducted within this thesis explores some of the weaknesses of the system to include the relative ease with which false aircraft targets can be injected. As part of a proof of concept, false ADS-B messages were successfully generated using a system comprised of GNU Radio, a Universal Software Radio Peripheral (USRP), and software developed by the author.

The ability to generate, transmit, and insert spoofed ADS-B messages on the display of a commercial ADS-B receiver, identified and exploited a weakness of the ADS-B system. Four demonstrations, conducted within an experimental environment, displayed the potential uses of the system created through this research and its associated impacts.

Acknowledgments

I would like to thank my thesis advisor(s) Lt Col David Robinson and Dr. Robert Mills for their patience and stellar support throughout the entire process of developing this thesis.

I'd also like to thank my entire family back at home. You've had a hand in the successes I've been able to enjoy and molded me into the person I am today. I am eternally grateful for all that you have done.

Last, but certainly not least, I'd like to thank my wife and son. You gave me the strength and support to pursue a monumental task and push through the many obstacles along the way. I could not have done this without you!

Domenic Magazu III

Table of Contents

Page

List of Figures

List of Equations

EXPLOITING THE AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST SYSTEM VIA FALSE TARGET INJECTION

I. Introduction

1.1 General Issue

Around December 17, 2009, it was reported that militants in Iraq had purportedly used $26 off-the-shelf software to intercept unencrypted live video feeds from United States Predator drones. Data captured could have provided the militants with information detrimental to US operations. The Wall Street Journal marked this incident "the emergence of a shadow cyber war within the U.S.-led conflicts overseas" [1]. Bringing this issue to modern day, imagine an adversary capable of receiving and displaying the exact location of all U.S. and allied aircraft performing missions over hostile territory. This hypothetical scenario is becoming a reality with the implementation of the latest Federal Aviation Administration (FAA) aircraft surveillance system, Automatic Dependent Surveillance-Broadcast (ADS-B).

In an effort to save fuel and money while enhancing aircraft safety, the FAA has begun actions to overhaul their traditional radar based surveillance system with a next generation (NextGen) solution based on ADS-B technology. Rather than relying on ground based radar to determine an aircraft's position, a unit onboard the aircraft determines the exact coordinates of the aircraft using the Global Positioning System (GPS) satellite constellation. That information is then automatically reported via air-to-ground and air-to-air data communication links at a fixed rate, depending on the aircraft's current state (enroute, taxiing, etc.). Because aircraft traffic volume is growing at a phenomenal rate, approaching the limits of current systems, the swift implementation of a new system is vital. For that reason, like any new technological advancement, security may not always be at the forefront of the system's development.

1.2 Problem Statement

The implementation of a new aircraft surveillance system has far reaching implications on the commercial sector as well as military. The NextGen system significantly enhances aircraft safety and efficiency, but the security of the system is a great concern. In particular, the air-to-air communications are unencrypted and unauthenticated. One must consider the vulnerability of such a system that does not encrypt or authenticate their communications. In fact, research by McCallie et al. [2] investigated several specific attack scenarios and the severity level of each attack; however no solutions were developed to carry out these scenarios.

Commercial aircraft companies are in the process of determining how to equip their fleets with the appropriate equipment in order to meet the FAA mandate. In addition, military program offices are cautiously planning the extent of implementation with security and financial concerns at the forefront. As the mandated deadline for ADS-B implementation draws closer, aircraft are forced into compliance without answers to multiple security questions. The problem does not stop at American borders. There are already areas of the world that have implemented ADS-B. For example, the entire continent of Australia has full coverage of ADS-B and utilizes this resource for commercial aircraft surveillance [3]. Other large projects to implement the new system include China [4]. A complete look at the security of ADS-B should be instituted before the world commits whole heartedly to a new system shrouded with security concerns.

This research, in particular, presents a proof-of-concept demonstration of how false targets can be generated.

1.3 Research Objectives

The purpose of this research is to demonstrate the relative ease of generating ADS-B messages using arbitrary data. Furthermore, the system developed to generate ADS-B messages relies on inexpensive hardware and software to display the versatility one may have in designing such a system. The hardware to be used is a Universal Software Radio Peripheral (USRP) as the radio frequency (RF) front end and GNU radio as the development toolkit to build the software defined radio (SDR) application for signal processing.

Once the system is created, it will help resolve many questions proposed towards the safety and security of ADS-B. In particular, can an individual receive and display aircraft in real-time? Can aircraft messages be spoofed? If spoofing is possible, can the messages be inserted and displayed on a commercial ADS-B receiver?

1.4 Research Focus

The focus of this research is on positional ADS-B messages. ADS-B contains multiple subtype formats for broadcasting aircraft data, this research will focus on downlink format (DF) 17, subtype 5 messages. These messages contain information such as aircraft ID, altitude, latitude, and longitude, which provide the potential for false targets to be inserted on a radar display.

In addition to the 1090 MHz frequency, the FAA has approved the 978 MHz Universal Access Transceiver (UAT) link for use by general aviation aircraft flying at lower altitudes. Although this link is used for ADS-B data communication it was not included within the scope of this research.

1.5 Investigative Questions

This research hopes to answer several questions

1. What is required to generate properly encoded ADS-B messages?
2. How can a system comprised of a USRP and GNU Radio be developed both to generate and transmit ADS-B messages?
3. If a system can be built, will it remain relatively inexpensive?
4. How can false ADS-B messages be inserted into the ADS-B network?

1.6 Approach

Using various sources, most notably, Radio Technical Commission for Aeronautics (RTCA) meeting notes [6], a system was created with the ability to generate ADS-B messages and subsequently broadcast them. In conjunction with a digital signal processing application, C++ code was written to generate the messages and perform proper preparations to transmit those messages. The process included multiple encoding equations and finally the transformation into hexadecimal representation to ensure the proper waveform for ADS-B messages.

After building the system, several demonstrations were generated and tested. The success of the demonstrations was recorded and discussed to prove or disprove the potential uses of the system created.

1.7 Implications

McCallie et al. [2] introduced some potential vulnerabilities of ADS-B. This research goes even further by demonstrating how those weaknesses can be exposed successfully. Those affected by these weaknesses include multi-billion dollar commercial airlines and military aircraft, within the U.S. and around the globe.

1.8 Preview

This document is outlined in the following manner. Chapter II provides an in-depth literature review on aircraft surveillance history, ADS-B, digital signal processing, software defined radio, and the USRP family. Chapter III describes the system development for the proof of concept system. Chapter IV contains results, discussion, and analysis of the system's capabilities. Finally, Chapter V contains conclusions, a summary of the research performed, and recommendations for future research related to ADS-B message exploitation.

II. Literature Review

2.1 Chapter Overview

This chapter presents an overview of past, present, and future Air Traffic Control (ATC) systems in order to provide background necessary to understand how the current system came into use, why this system needs to be replaced, and an introduction into future generation ATC systems. With regard to the future ATC systems, the focus of this review will be on the main area of this research, Automatic Dependent Surveillance-Broadcast (ADS-B). The chapter also includes information pertaining to software defined radio, digital signal processing (DSP), and the USRP family.

2.2 ATC History

2.2.1 Early ATC Techniques

During the early stages of flight, little to no equipment existed for in-flight navigational aids. In addition, there was no governing body within the United States to set and enforce standards, giving the appearance that improvements to navigation would not come quickly. Pilots relied on a single ground controller using flags during the day or a light at night to signal instructions to takeoff, land, or turn. Because there was no capability, such as radios, to communicate information during flight, the controller would inform the pilot of weather information or the presence of other aircraft in the same route before takeoff. Weather changes or other pertinent information could not be relayed to the pilot once they were off the ground [7].

Pilots also had to use known landmarks such as cities, railroad tracks, and/or water towers to determine their position and make any necessary corrections. This can be compared to Visual Flight Rules (VFR) used today. VFR are established by the Federal Aviation Administration (FAA) and allow a pilot to operate the aircraft in a free-flight manner when conditions allow proper operation and control [8]. The pilot assumes responsibility for separation from other aircraft.

Shortly after these techniques, a slight improvement was introduced utilizing lighted runways or beacons set apart by a mandated distance [7]. This improved VFR flying, however, as air traffic increased each year, the need for better instruments when navigating through poor conditions (i.e. adverse weather) was essential, resulting in radar based systems becoming the navigational aid of choice.

2.2.2 Introduction of RADAR

Radio detection and ranging, also known as radar, was developed during World War II. Its design was shrouded in secrecy, but shortly after the war completed, its benefits were revealed, and the use of radar for both military and commercial use became more prevalent. Radar works through the emission of electromagnetic (radio frequency) waves by a directional or rotating antenna dish. Those radio waves then reflect off an object and return back to the source where the signal is gathered by a receiver and the target is placed on the plan position indicator (PPI), the display within the ATC tower [9]. A typical radar system is comprised of secondary surveillance radar (SSR) and primary surveillance radar (PSR). These are coupled with radio communications to form a complete ATC system. These systems came about during the 1950's which marked the beginning of radar use for ATC purposes [10].

2.2.3 Present ATC System

During the late 1950's, the U.S. government became involved with air traffic management and regulation through the Federal Aviation Act of 1958, signed by President Eisenhower [22]. This Act created the Federal Aviation Agency which later became the Federal Aviation Administration (FAA). Since that time, the FAA has taken action to administer and enforce regulations, develop and maintain the national infrastructure, and monitor the air picture across the United States of America. To date, the FAA controls 750 ATC facilities, 18,000 airports, and 4,500 air navigation facilities providing complete coverage of the National Airspace System (NAS) [2]. The cost to maintain and operate these facilities is quite large. Approximately 150 million dollars is spent each year in operational and maintenance costs by the FAA [11]. As the systems continue to age, maintenance costs continue to escalate, which is a primary motivation for ADS-B implementation.

As discussed earlier, most modern ATC systems are comprised of PSR and SSR. PSR works solely on the signal reflecting off an aircraft or other object and the reflected signal returning to the receiver, normally positioned in the same location as the transmitter. The orientation of the radar antenna determines the bearing of the aircraft relative to the radar site, while the distance is determined by the length of time it takes for the signal to be emitted and for the reflected signal to return to the origin of the transmission [12]. PSR is completely passive and does not require any action from the object being tracked. The main disadvantage of PSR is that it can reflect off birds, ground objects, and atmospheric phenomena, which can cause issues for air traffic controllers. Due to this disadvantage, PSR has been augmented with Air Traffic Control Radar Beacon System (ATCRBS), also known as SSR.

SSR employs special equipment onboard the target aircraft. Interrogation signals are sent from the ground station antenna just as with PSR. Once an aircraft receives the interrogation signal, a transponder aboard the aircraft returns a coded reply signal containing information such as aircraft identification and altitude. Because the aircraft transmits the reply message, SSR provides greater signal strength which translates to greater range and improved performance. SSR also decreases the power needed by the ground station transmission since the signal will not need to reflect and return [Figure 1].

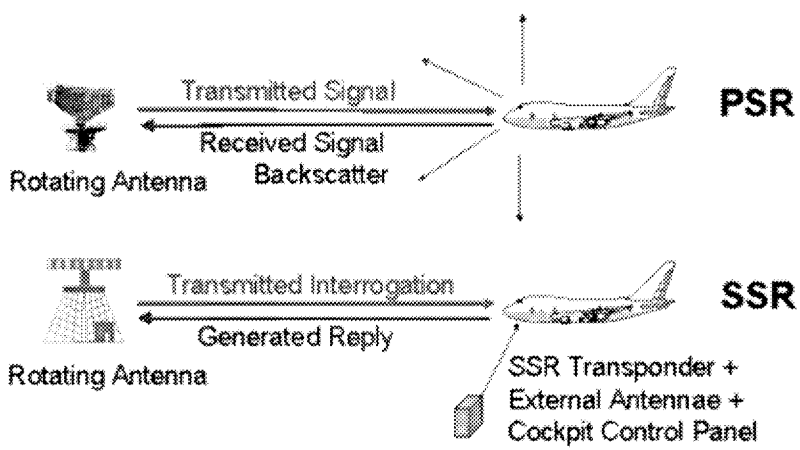


Figure 1 - Graphical representation of PSR and SSR [13]

One drawback of SSR is its dependent nature, with dedicated equipment on the ground and on the aircraft. In most cases, PSR and SSR will be coupled together to accommodate both aircraft with and without transponders. Additionally, PSR is required for air defense, detecting non-cooperative targets.

2.2.4 Current ATC Limitations

Current radar systems are quickly reaching their maximum capacity due to shortcomings in visibility propagation, limitation of line-of-sight, limitation of voice communications and the lack of digital data links [14][15]. Additionally, synchronous garbling is another concern in which the interrogation signal of SSR invokes a response from more than one aircraft, causing the replies sent by both aircraft to overlap at the receiver leading to loss of information at the ATC facility.

Compounding the interference of messages is the rapid growth of air traffic. Air traffic has increased 32% within the last decade and is projected to nearly double by the year 2028 [Figure 2]. Currently, air traffic controllers handle 9 to 15 aircraft at any one point. With the current radar system and projected increase in air traffic, experts believe controllers could be required to handle approximately 45 aircraft at any one point, a situation that is infeasible to manage and completely unsafe [16] [17].

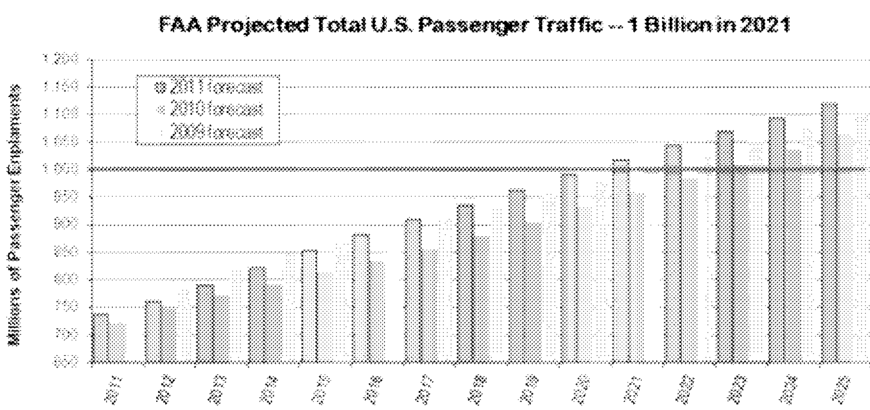


Figure 2 - Rapid air growth over the next decade and a half. Expected to double air traffic by 2025 [18].

2.3 NextGen Solution

2.3.1 FAA Decision

With the release of the FAA's final decision [19], they solidified their choice to move forward with the implementation of ADS-B technology as part of the next generation (NextGen) national airspace system. In addition, in August of 2007, the FAA awarded the International Telephone and Telegraph (ITT) corporation a contract to field a national system capable of providing a comprehensive set of ADS-B services for the United States [20] [21]. Because the FAA is charged with providing a safe and efficient airspace for both civil and military aircraft [22], the armed services are also affected by the FAA's decision.

2.3.2 ADS-B Around the World

ADS-B is also being adopted on a global scale. Europe has a slightly more aggressive implementation plan with hope of wide spread implementation by 2015 as compared to 2020 for implementation within the U.S. [23] [24]. ADS-B standardization in Europe is being driven by the Requirements Focus Group (RFG), containing members from the European Organization for the Safety of Air Navigation, FAA, European Organization for Civil Aviation Equipment, Radio Technical Commission for Aeronautics (RTCA), and participation from nations such as Australia, Canada and Japan [23]. The RFG is also working closely with the International Civil Aviation Organization (ICAO) to ensure global interoperability for ADS-B. ICAO codifies the principles and techniques of international air navigation and fosters the planning and development of international air transport to ensure safe and orderly growth.

2.3.3 NextGen Components

NextGen is comprised of several components working simultaneously to collect information and disseminate it via a broadcast transmission [Figure 3]. Its main source of information is from the constellation of GPS satellites. GPS sensors aboard an aircraft determine its location, which is then joined with information from the aircraft's navigational system or Flight Management System (FMS). The FMS provides information such as the flight plan to ensure the aircraft is following its designated path.

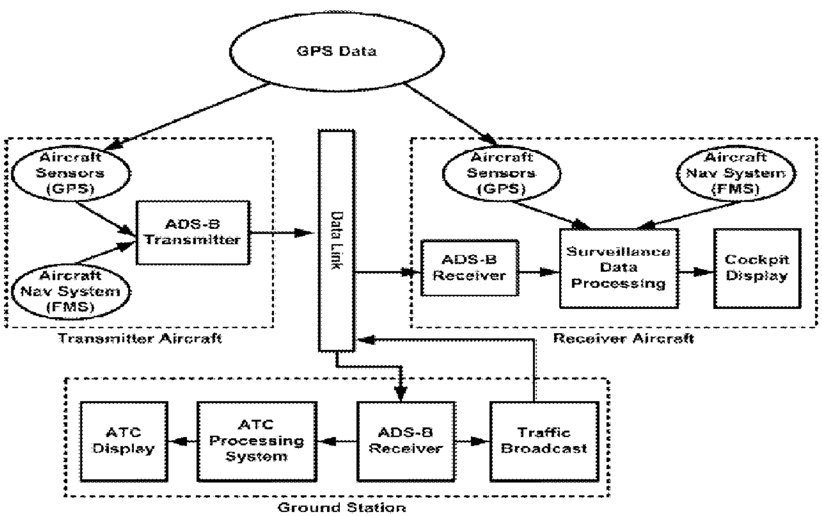


Figure 3 - Major components of the ADS-B system [2]

The FMS and GPS data is fused and broadcasted to other aircraft and ground stations. Both receiving aircraft and ground stations perform similar operations on the message to interpret and display the information on the control display unit (CDU) [2].

2.3.4 ADS-B Explained

ADS-B's main purpose is to determine the position of an aircraft and then broadcast that information, along with its altitude, call sign, heading, and aircraft type automatically (i.e., without an SSR interrogation signal) to other aircraft and to air traffic control ground facilities. ADS-B is *automatic* in that it does not require any action or input by the pilot and there is no interrogation from the ground required. It is also *dependent* because it relies on onboard equipment to gather the ADS-B data and *broadcast* it to other ADS-B users and it is a means of providing *surveillance* and traffic coordination.

ADS-B was created with compatibility and ease of transition in mind. It was built using similar aspects of the current aircraft surveillance transmission mode called Mode S or mode select. Mode S operates by interrogating aircraft by a specific aircraft identification number. Only the aircraft possessing the correct identification number will reply to an interrogation with its flight information, eliminating issues with synchronous garbling. Transmission types prior to Mode S include Modes A and C. Mode A provided aircraft identification and Mode C provided altitude. Mode S provides greater capabilities, primarily in the form of aircraft information to include identity, intent, capability and location [25].

ADS-B is similar to Mode S in that it uses the same transmission frequency of 1090 MHz. It differs in that the message is 112 bits, 120 μs long and are "squitter" messages [17] [26]. A squitter message is simply a transmitted message not invoked by any interrogation [Figure 4].

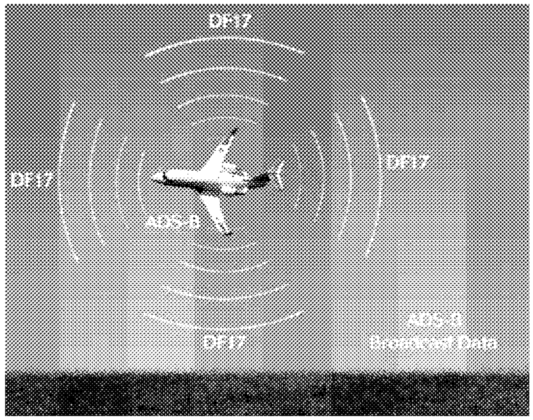


Figure 4 – Broadcasting of ADS-B squitter message [27]

As shown in Figure 5, 56 of the 112 bits are for ADS-B specific data to include altitude and airborne position (latitude and longitude). The remaining bits are used for message format, aircraft address, parity check, and finally a few bits for the transponder communication capability.

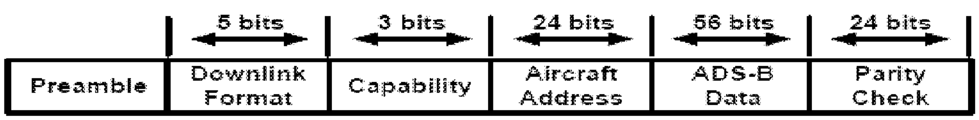


Figure 5 - Diagram showing the fields of the ADS-B message [2]

Pulse Position Modulation (PPM) is used for encoding and transmitting the message [26] [29]. The PPM for each pulse results in the data occupying either the first or second half of the entire pulse, which in effect is the same as Manchester encoding [Figure 6].

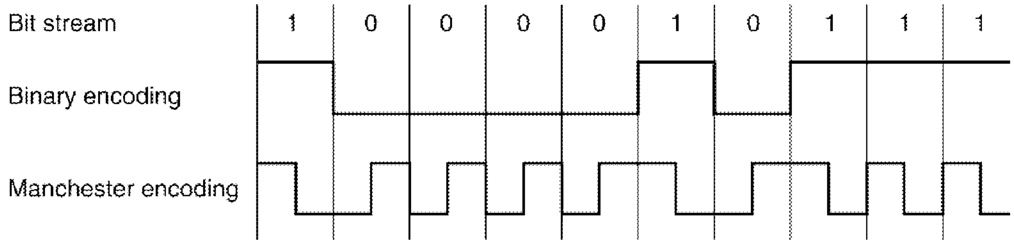


Figure 6 - Manchester encoding

There are two types of equipment for ADS-B messages, with one being *ADS-B In* and the second being *ADS-B Out*. ADS-B Out provides the ability to broadcast messages to ground stations and to other aircraft within the appropriate receiving range. As demonstrated by the Los Angeles ADS-B trials, air-to-air reception ranged from 0 to 110 nautical miles [30] [31] [32]. ADS-B In is responsible for receiving, decoding, and displaying messages within the cockpit or ATC tower. As mentioned previously, by 2020, all aircraft flying within the United States will be required to be equipped with ADS-B Out. Currently there is no mandate for ADS-B In onboard aircraft, but without the usage of this equipment, many of the advantages of ADS-B cannot be utilized.

2.4 Advantages of NextGen

One of the biggest advantages of ADS-B is the ability to provide coverage where radar could not reach before. The primary area in which this is relevant is transoceanic navigation [33]. With current systems, the radar picture is limited by land based radar. ADS-B overcomes this limitation through the utilization of GPS satellites, broadcasts from other aircraft, and ground stations to generate its air picture. Strategically placed broadcast stations provide the ability to receive nearby transmissions and broadcast them out to anyone within range. Therefore with careful placement of ATC facilities, aircraft will maintain the air picture around them, providing greater accuracy, resolution, integrity and safety.

Related to coverage, an added advantage is the smaller footprint of ADS-B facilities. This allows the FAA to deploy ADS-B transmitters/receivers on structures such as oil rigs many miles out from land which can then act as Automatic Dependent Surveillance-Rebroadcast (ADS-R) stations [37] [Figure 7]. ADS-R receives ADS-B position broadcasts and rebroadcasts the information to near-by aircraft [34] [35]. In addition to a smaller footprint, operation and maintenance of ADS-B equipment and facilities will be significantly cheaper. The average radar-based facility costs approximately $1-$4 million dollars while an ADS-B site will cost approximately $100-$400 thousand [36].

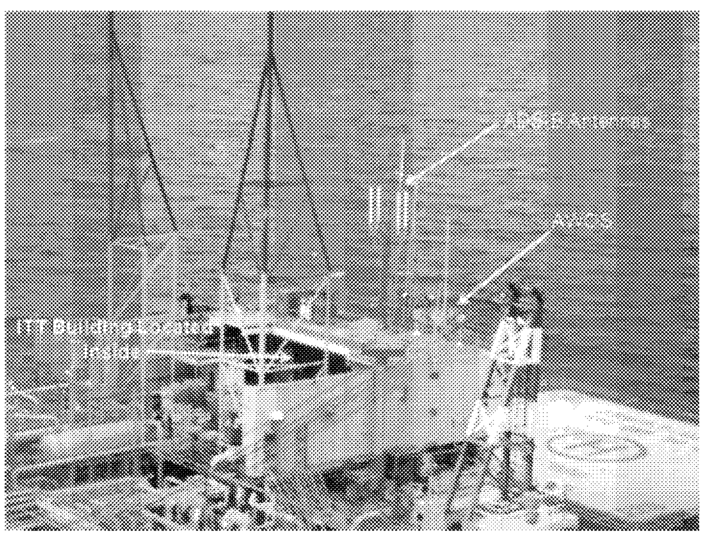


Figure 7 - ADS-B equipment aboard an oil rig [37]

Another advantage of ADS-B is more precise management of aircraft on their approach for landing. As described by Randy Babbitt, the FAA Administrator, ADS-B provides "greater precision and reliability" [38]. Because the aircraft transmit location every second, data flows at nearly real-time, as compared to updates of five to ten seconds for traditional radar. The controller can take advantage of this feature and are able to reduce the amount of space between each aircraft, thus increasing the airport's throughput [39] [40]. A 2000 FAA study, demonstrated how aircraft could reduce their separation from the current standard of 4300 feet to only 750 feet [10]. This is a drastic change from the current methods which focus on aircraft flying a more rigidly structured and uniform flight path [41]. The ability to decrease separation allows aircraft to perform continuous descent landing, as opposed to the current stair-step practices [42]. In the stair-step method, aircraft alternately descend and then level off by accelerating engine speed. These short bursts of engine speed burn enormous amounts of fuel, increase noise, and cause more emissions. The elimination of the stair-step process could result in airlines saving millions of dollars in fuel costs. The United Parcel Service used ADS-B for one year and realized a savings of 250,000 gallons of fuel. The fuel savings generated additional benefits such as a 30% reduction in emissions and a 34% reduction in noise [43] [44].

Widespread usage of ADS-B also introduces the concept of Free Flight [45] to the NAS. The Free Flight model could introduce further savings in fuel as well as faster flight times for passengers with the ability of aircraft pilots to formulate a more direct route from their point of origin to the aircraft's destination. Aircraft routes would no longer be so rigidly structured and uniform or determined by ground controllers before the flight takes place [41]. This is the result of more frequent reporting of the ADS-B surveillance system (reports every 1 second), *ADS-B In* technology, and the ability to receive precise aircraft position data in locations where PSR and SSR could never reach.

In addition to these positive results, Alaska's Capstone program, an experiment in testing ADS-B technology and its effect on air traffic controller workload, produced even more optimistic results. During the trial period, 208 aircraft were equipped with ADS-B. Normal flights in and out of the Alaskan region were monitored. After program completion, surveys of controllers found that 57% said they had spent less time providing Instrument Flight Rules (IFR) separation services, and 79% felt their overall efficiency increased with ADS-B. Additionally, ATC saw a reduction of 18% in controller communications while at the same time reducing the fatal accident rate by nearly half [42] [46].

Providing a better air picture to the pilots is yet another advantage. An aircraft with both ADS-B Out and ADS-B In can provide pilots with a more fluid response to situations since they have a clear picture of the air as well as the ground without relying on voice communications between themselves and air traffic controllers, as is the current case with radar-based systems. This allows for faster response and corrective actions while providing the pilot with strong confidence in the air picture.

Finally, ADS-B has the potential to augment the Traffic Collision Avoidance System (TCAS) [47]. Although TCAS is not at the end of its life cycle, ADS-B operates in a similar fashion, giving the systems the capability to enhance their ability to avoid mid-air collisions. TCAS works by interrogating aircraft (similar to SSR) within the vicinity and tracking aircraft by their replies to those interrogations. TCAS then determines if the aircraft has entered the 'protection volume' or safety zone of another aircraft. If an aircraft has entered that zone, a traffic advisory is sent to the aircraft. If the aircraft does not make the necessary correction a resolution advisory (vertical maneuver command) is released to avoid a mid-air collision [48]. Not only will ADS-B provide mid-air collision avoidance, but aircraft continue to transmit ADS-B messages while on the ground. This provides surface surveillance for runway incursion avoidance and ramp management [49]. Although many advantages exist, like all new technologies, there also exist disadvantages or vulnerabilities.

2.5 Vulnerabilities of ADS-B

ADS-B consists of GPS for an aircraft's coordinates, a transponder, a barometric altimeter, and the associated wiring to connect them. While each of these components offer potential avenues of attack, most are beyond the scope of this research and will not be discussed further. The attacks to be focused on are those aimed at exploiting the ADS-B messages being transmitted and received by an aircraft. Additional reading on GPS failures and information integrity can be found at [50] [51] [52]. Other sources [14] [52] outline ADS-B message attack scenarios in which the system could be exploited by nefarious users which will be described in the following paragraphs.

2.4.1 Passive Monitoring

In December of 2009, the Wall Street Journal reported that insurgents had purportedly intercepted live video feeds from unmanned aerial vehicles controlled by the United States military [1]. A related concern with ADS-B is the ability for any individual to purchase equipment that is capable of receiving and translating ADS-B messages providing a mechanism to passively monitor aircraft for possible ill intent. Dick Smith, former chairman of Australia's Civil Aviation Administration, explained how terrorists with a laptop, transponder and antenna could intercept ADS-B messages and utilize them to track aircraft of law enforcement, high profile politicians, commercial aircraft, or military aircraft [53].

Additionally, with the advent of smart phone markets, applications have been released that will plot an ADS-B equipped aircraft on a map. The user can download this application for free and monitor their local air traffic. The paid version of this application provides additional information such as live aircraft movements, flight path contrails, the ability to search for an aircraft by flight number, aircraft altitude, speed, plane type, and transponder "squawk" codes. This application costs a user only $3.99. Applications of this sort are purely passive and only allow an individual to monitor without affecting an aircraft's display or causing any harm to an ATC facility. The next section discusses actions that will lead to the alteration of messages or the display aboard an aircraft or at an ATC facility.

2.4.2 Active Attacks

The first type of active attack on the ADS-B system is the ability for a malicious person to jam the signal at the ground station. There will be approximately 800 ground stations placed 150 to 200 miles apart [19] [20]. Development of facilities for performing ADS-B communications have already begun and completion is projected for 2013 [42]. Locating a ground station and gaining close proximity to it will likely not be difficult because they are numerous and their general locations have already been designated [Figure 8].

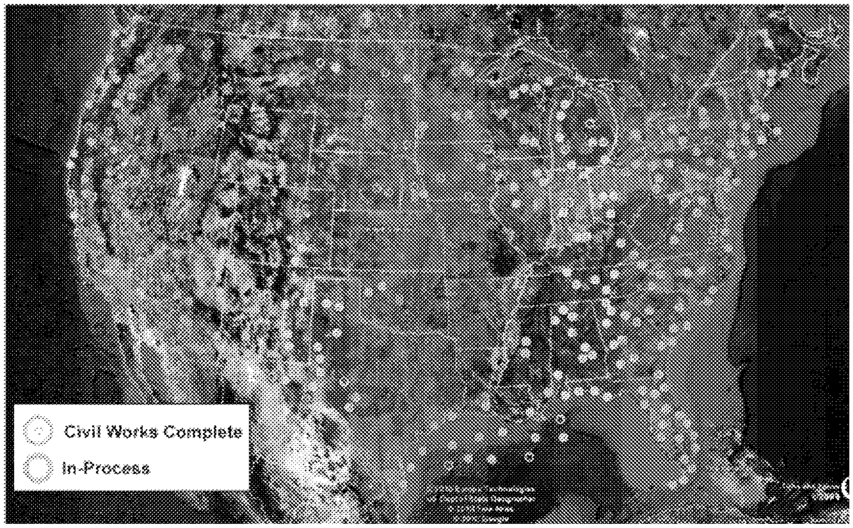


Figure 8 - Map showing ADS-B ground facility status [37].

Related to this attack is jamming a specific aircraft. Although an attacker could jam a single aircraft's receiver from the ground, once the aircraft goes beyond line-of-sight it will no longer be susceptible to the attack.

Another active attack vector is the injection of ghost targets on the display of aircraft as well as ground stations. The user would need to transmit the 112 bit ADS-B message, which would then be received by the ground station and displayed for pilots and air traffic controller(s).

Spoofing aircraft on a ground station facility will not yield high success as the facilities will use primary surveillance radar to verify the ADS-B messages [28], however this verification cannot be implemented aboard an aircraft [54]. Because there is no current methodology allowing interoperability of ADS-B and legacy radar systems on an aircraft, what is shown on the display cannot be verified or corrected [55][56]. A controller within an ATC facility also has the ability to reference logged flight plans to determine if a target is a ghost inject or not. Again, the ability to perform this cross check is not available to pilots. Suggestions have been made through prior research that signal tracking, ADS-B data filtering, evaluation directional characteristics of an ADS-B signal, track change reports, and flight intent, can provide information validation, eliminating the ghost inject scenario [57]. Because these validation techniques are not currently being employed they will not be discussed further.

Although it is out of the scope of this research, something of importance to note is the ADS-B system will use the backbone infrastructure of AT&T to connect the air traffic management picture. This provides a vector through the Internet to infiltrate and/or disrupt the air traffic control system. Access to the system could grant a malicious user the ability to disrupt, destroy, or deny ATC services.

2.6 ADS-B Test Equipment

Many companies have begun production of light-weight and inexpensive hardware for both aerial enthusiasts and pilots alike to become familiar with the new ADS-B system. One such piece of equipment, the SBS-1eR, is made by Kinetic Avionic Products Limited based out of the United Kingdom. The SBS-1eR is about the size of the human hand and provides many features to include tracking of Mode-S/ADS-B equipped aircraft, built-in air traffic and FM radio, and software capable of being run on a laptop or PC with Windows operating system. The software provides a virtual radar screen displaying any aircraft broadcasting ADS-B in the area. Figure 9 is a screen capture of the virtual display generated by the software, showing a location within Ohio, currently tracking two aircraft.

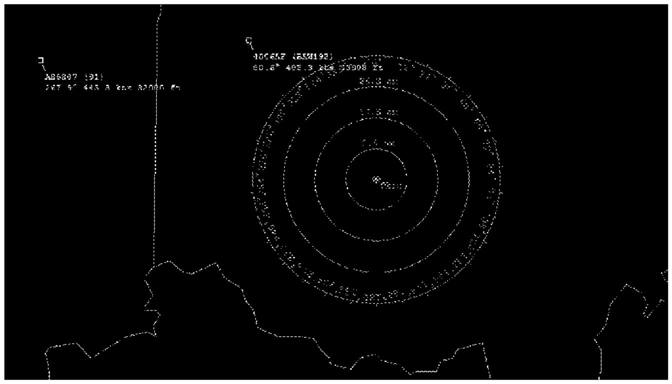


Figure 9 - SBS-1eR virtual radar screen currently tracking two aircraft

Along with displaying the aircraft on the "radar screen", additional information can be obtained for a given aircraft to include altitude, speed, exact location via GPS coordinates, country of origin, planned track, and aircraft identification in hexidecimal format [Figure 10].

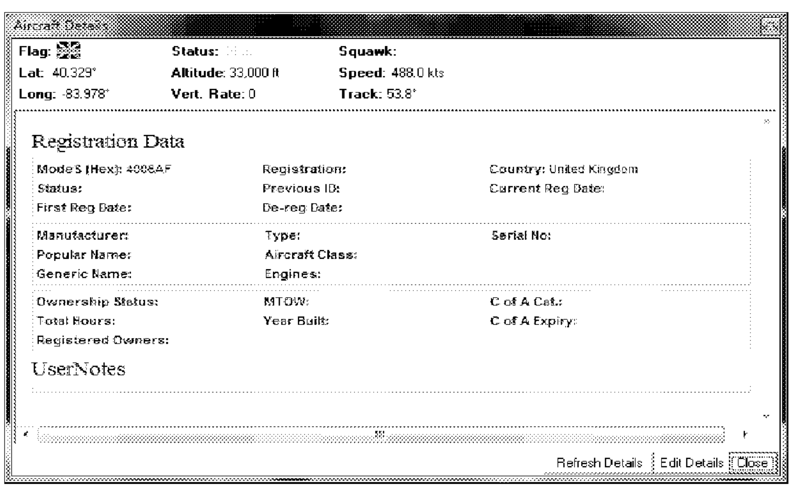


Figure 10 - Aircraft information displayed by SBS-1eR

The SBS-1eR will be used throughout this research for monitoring live and ghost inject traffic. This equipment will be used to validate the proof of concept system proposed by this thesis.

2.7 Universal Software Radio Peripheral

The USRP is a flexible USB or Ethernet device capable of connecting to a laptop or PC [Figure 11]. The USRP provides a front end for software defined radio applications. It is made up of a motherboard which contains four digital-to-analog converters, four analog-to-digital converters, a field programmable gate array (FPGA) discussed in the next section, and a USB or Ethernet controller [Figure 12]. Additionally, the USRP motherboard has the ability to support four daughterboards, two for receive and two for transmit.

Figure 11- USRP N200

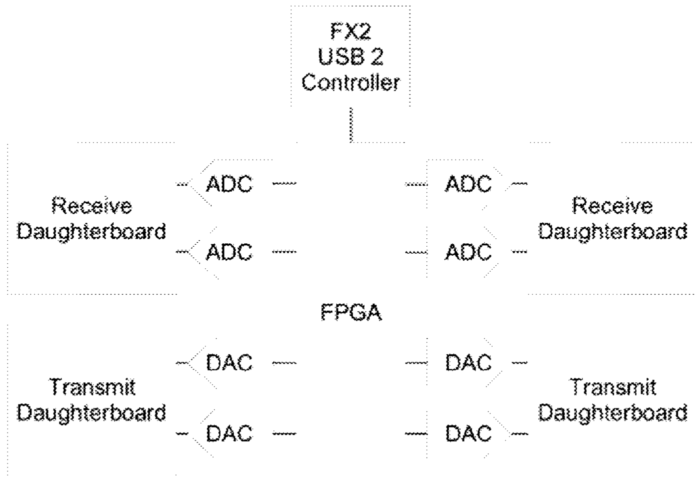


Figure 12 - USRP block diagram

Both the USRP and associated daughterboards are developed by Ettus Research, LLC. The daughterboards vary greatly in their capability, with some performing receive actions and others performing both receive and transmit functions, also called transceivers. The daughterboards allow a software defined radio application to operate at various frequencies depending on the specific board purchased [58].

2.8 FPGA/Digital Down Conversion

One of the main components of the USRP is a Xilinx FPGA. The FPGA performs the process of digital down conversion (DDC). This involves taking a band pass RF signal and mixing it to a lower frequency, which lowers the sample rate while retaining all information. DDC is used when the signal of interest occupies a small portion of the entire bandwidth. To illustrate the process, take a signal at the 45-47MHz range, the band of interest is only 2MHz. The RF signal would be digitized at a sample rate of 100 million samples per second if it were not down converted. This follows the

Nyquist theorem which states the sampling rate should be no less than two times the rate of the highest frequency [54]. DDC brings the signal of intent down to baseband, a signal measured from zero hertz to a cut-off frequency which would be 2 MHz for this example. At this point the baseband signal can be sampled at a much lower rate, on the order of 4-5 MHz. DDC adds the advantages of simplifying any further signal processing on the data, allows more processing to fit within the FPGA, and reduces the power requirement of the FPGA.

2.9 GNU Radio Basics

GNU Radio is free software that provides a framework for developing software defined radio applications using readily-available, low-cost external RF hardware and commodity processors. In addition, the recommended hardware for GNU Radio interface is the USRP.

GNU Radio uses the Python programming language for high-level organization, policy and GUI control, while using C++ for performance-critical signal processing blocks. Different source files are released for free download on the GNU Radio wiki page. Implementing the different software radios is as easy as downloading the source files and installing on a Linux based machine [59].

One such release was provided by Nick Foster, an employee of Ettus Research, who developed a simple Mode S/ADS-B receiver. It was released in October of 2010 for download from the GNU Radio site. It has the ability to decode and display ADS-B messages to the command window. Once decoded, the output can be exported to multiple interfaces to include keyhole markup language (KML) for Google Earth, which is a popular application for plotting data in three dimensional space.

2.10 Summary

Using the information gained through this literature review an individual now has the general knowledge to begin the development of an ADS-B message generator as well as an ADS-B transmitter. In the following chapter, the author will discuss the methodology in building such a system.

III. Methodology

3.1 Chapter Overview

This chapter will describe the methodology used in designing a system capable of both receiving and transmitting ADS-B messages. The software, hardware, and coding will be discussed as well as the limitations experienced throughout the process of creating the system. The system described will then be used to demonstrate that ADS-B messages can be spoofed causing ghost injects to be inserted and displayed on the commercial ADS-B receiver.

3.2 Hardware and Software

3.2.1 Computer

The computer used during these experiments was a Dell® Precision 690 with Intel® Quad-Core Xeon processers operating at 3.00GHz. The choice of this system was based on availability. When designing a system similar to this, considerations should be made in the processing power of the computer used. The processer operating at 3.00GHz will provide enough calculations per second to meet requirements for this system. All modern processors should handle the calculations for digital signal processing as the majority of processing will occur within the USRP.

3.2.2 Operating System

The operating system chosen was Ubuntu 10.10, Maverick Meerkat, released in October of 2010. Ubuntu is an open source operating system built around the Linux kernel. Ubuntu 10.10 has proven to be an extremely stable version and much of the development for GNU Radio has taken place on this version, hence the decision to use it.

Ubuntu operating systems are freely available at ubuntu.com. There are multiple ways to install the operating system, all of which are described at the Ubuntu website. The install for these experiments were accomplished through disc boot. It is assumed that the reader has a working knowledge of Ubuntu Linux and specific details for installing/configuring are not provided here. The next step is deciding on a platform for building SDR applications.

3.2.3 SDR Design Platform

GNU radio was chosen for the experiments in this thesis. It is written using two different programming languages. The higher level language to create SDR applications is written in Python. The lower level language which will perform the critical signal processing is C++. This SDR toolkit was chosen for the following reasons. GNU radio has a very large following and comes with pre-configured signal processing blocks for generating SDR programs, alleviating a significant portion of the learning curve required to transmit and receive radio frequency (RF) signals. In addition to having pre-configured processing blocks, the toolkit is completely free for use and experimentation. A final reason was the availability of previously developed code for receiving ADS-B messages using the standard GNU radio library [60]. This program, called *GR-AIR-MODES*, provides insight into the decoding of ADS-B messages and helps to provide the foundation for creating, manipulating, and transmitting ADS-B messages and its associated data.

3.2.4 USRP

The USRP was chosen for its great flexibility and modular architecture. The USRP family is developed and sold by Ettus Research, LLC. This device provides the front end for the SDR application, the two specific devices used are the USRP N200 and USRP2 [Figure 13]. The USRP2 was released in September of 2008. The specifications of the USRP2 include a Xilinx Spartan 3-2000 FPGA, gigabit Ethernet interface, two 100MS/s, 14 bit analog-to-digital converters (ADC), two 400 MS/s, 16-bit digital-to-analog (DAC), and an SD card reader. The USRP N200 is very similar to the USRP2 with the only differences being the RF bandwidth increasing to 50 MHz from 25MHz and an onboard Flash memory instead of an SD card for firmware and configuration. This allows for easier programming over the network.

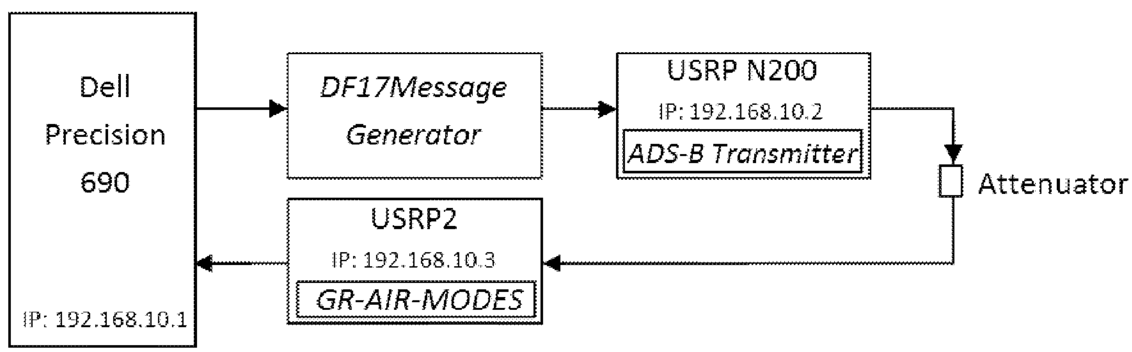


Figure 13 - System block diagram for testing/troubleshooting

3.2.4.1 USRP Daughterboards

With each USRP the appropriate daughterboard must be installed to provide the required RF coverage. The daughterboards are also manufactured and sold by Ettus Research. Since ADS-B messages are transmitted at the 1090MHz frequency the WBX daughterboard was chosen [Figure 14]. The specifics of the WBX daughterboard include a frequency range of 50 MHz to 2.2 GHz, transmission power of 30 to 100 mW, and dual synthesizers for independent transmit and receive frequencies. Both the USRP2 and USRP N200 will be using the WBX daughterboard.

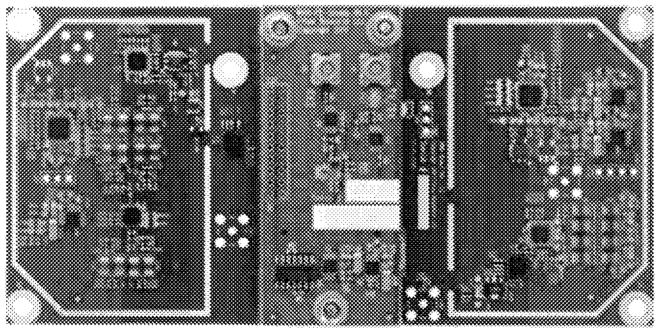


Figure 14 - WBX daughterboard

3.2.4.2 USRP Firmware

The USRPs were configured with the latest version of the Universal Hardware Driver (UHD) for better compatibility between the computer system and the USRP devices. The UHD provides a single driver that can be used across all USRP devices. Prior to the integration of UHD, each USRP device had its own specific driver and the ability to communicate between USRPs was extremely difficult if not impossible [59]. To use both UHD and GNU Radio a bash script is freely available at http://code.ettus.com/redmine/ettus/projects/uhd/wiki. In order to install the latest UHD and GNU radio versions simply copy and paste the code to a shell file within the home directory. Through the command line navigate to the location of the file and perform an execution command (./UHDandGNURadio.sh). The script will download the most current software and complete all installation steps.

3.2.5 Testing GNU Radio and USRP Install

To ensure proper installation of the above items, the *UHD+GNURadio* build provides some useful tools to include 'uhd_find_devices', which finds all properly configured URSPs and another application 'uhd_usrp_probe', which provides all specifications of those USRPs, to include firmware and daughterboard information. These applications can be found within the directory of the *UHD+GNURadio* installation within the /uhd/host/utils directory. When running these scripts, be sure the devices are connected to a gigabit Ethernet port or they will not be recognized on the network and errors will result. When networking USRPs, be sure to set the Internet Protocol (IP) address to 192.168.10.#. Setting the IP address can be accomplished through another tool installed with *UHD+GNURadio*. Appendix A contains information on the USRP device configuration settings and how to change them.

3.3 Commercial ADS-B Receiver

In order to validate the information received, a commercial device was also purchased called the SBS-1eR. The SBS-1eR, developed by Kinetic Avionic Products Limited, is a commercial device developed to receive and decode ADS-B messages. The device also contains a built in very high frequency radio receiver for listening to air traffic communications. It has an extremely small footprint and can connect to a PC or laptop via USB or Ethernet [Figure 15].

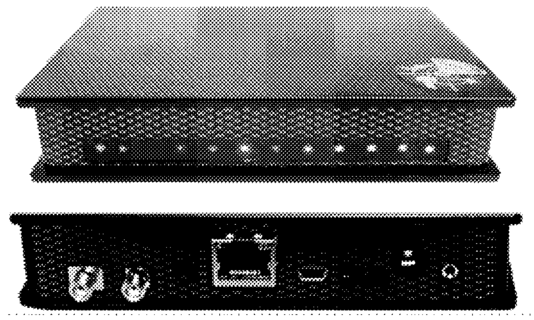


Figure 15 - Front and rear view of SBS-1eR

The SBS-1eR also includes Basestation Virtual Radar software, which provides a virtual radar screen on the PC for viewing aircraft movements [Figure 16]. The display will provide information such as aircraft ID, altitude, latitude, longitude, callsign, and much more within the right side of the display. The aircraft's position will be displayed on a virtual radar screen within the top left corner and finally the altitude in the bottom left corner.

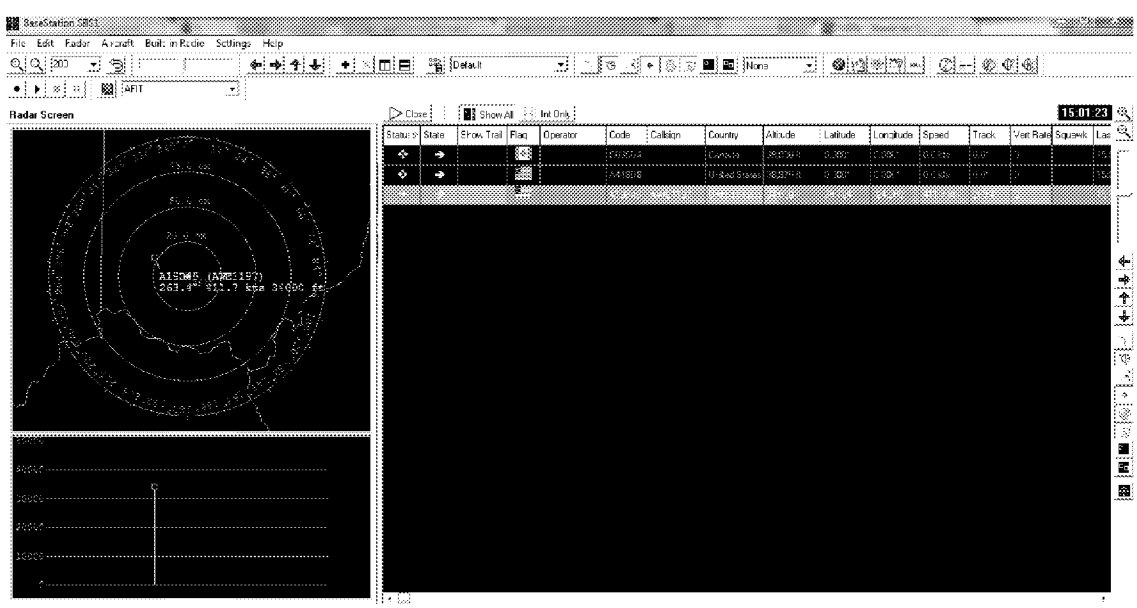


Figure 16 - SBS-1eR virtual radar screen currently tracking an aircraft

3.4 USRP ADS-B Receiver Install

There are two methods used within this research to receive ADS-B messages. The first is the SBS-1eR, which will display the aircraft on its software-based virtual radar screen. The second method is to download, build, and run the *GR-AIR-MODES* program. The subsequent paragraphs will go into the process of building the receiver and some detail on the options the program provides to the user.

Similar to the UHD and GNU Radio build script, the ADS-B receiver program is available for free and is easy to download through a git repository [60]. Github is a web-based hosting service for software development projects. Developers can store their code on the website and make changes as needed, which can then be downloaded by users of the application. Using a simple command will download all the necessary files for building and running the program :

git clone git://github.com/bistromath/GR-AIR-MODES.git

After completion, a *GR-AIR-MODES* folder is located in the current directory. If any errors occur they will be displayed within the command prompt window. All errors should be corrected before continuing. In order to begin receiving data, a USRP must be functioning properly with the latest UHD version and a proper daughterboard, capable of receiving within the 1090MHz range.

After all hardware and software has been installed and compiled correctly, the program can be run by navigating to the *GR-AIR-MODES* folder and opening the src/python directory. Simply executing the uhd_modes.py file will begin the capturing of

ADS-B/Mode-S messages. There is no GUI, but messages will be displayed within the command prompt showing all relevant data fields [Figure 17]. If an error is received the USRP may have a different IP than the program expects. Simply open uhd_modes.py in a text editor. Line 63 of the code sets the IP of the USRP source, change it to the IP set during the steps followed in section 3.2.5.

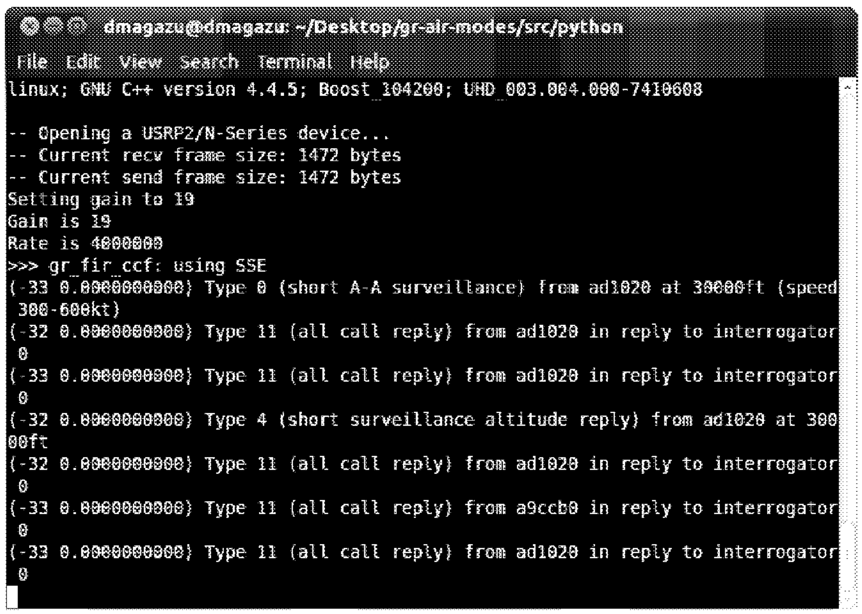


Figure 17 - Command window displaying the *GR-AIR-MODES* program running

There is also a command line switch, -K, that will allow the user to 'record' all data captured to a KML file. KML uses eXtensible Markup Language to encode geographic modeling data. KML files can then be used within Google Earth. After running the *GR-AIR-MODES* program with the –K option invoked, open Google Earth and import the KML file. All aircraft broadcasting ADS-B messages will be displayed on the three-dimensional map. Although elementary, be sure to choose the correct antenna before running the program. The antenna can be chosen through the –A command followed by the antenna name. With the WBX daughterboard, there are two options, the receive (RX) only antenna or the transceiver (TX/RX). There is no difference between the two antennas, but the USRP will default to RX. If the antenna being used is not connected to RX, it may give the appearance the program is not receiving ADS-B messages.

3.5 Demodulating the Pulse Train

As discussed in Chapter II, a typical ADS-B message is 120 μs long and uses PPM for transmitting the bits. PPM is a form of signal modulation where the bits are transmitted in one of two possible time slots; for ADS-B the time slot equals one microsecond [Figure 18]. A "1" or "0" is denoted by a pulse in the first or second half (0.5 μs) of the time slot, respectively.

3.5.1 Preamble Detection

The first step in demodulating the pulse train is to determine the presence of a signal. The first four pulses in Figure 18 are considered the preamble. The preamble serves as a flag and time sync, notifying a receiver that a message will begin 8μs from the first preamble pulse. The preamble does not follow conventional PPM principles (a pulse in every time slot). A method for overcoming this deviation is to represent the gaps as consecutive "0" bits.

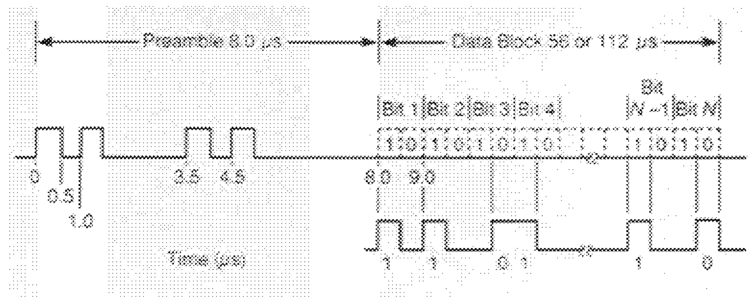


Figure 18 - 120 microsecond ADS-B message waveform

3.5.2 Message Reception

After the preamble has been detected, the individual bits need to be identified for message decoding. The bits are detected through a threshold setting based on the pulse amplitudes of the preamble. This requires the pulses to remain at relative constant amplitude throughout transmission. Pulses violating the threshold could cause bit errors and ultimately the message would be discarded. Once the bits have been received successfully, *GR-AIR-MODES* begins to decode the bits based upon the message type and the message format. DF17 messages have a particular placement for the individual components of the message. To ensure proper decoding, the format must be known to ensure the correct bits are used for altitude, aircraft ID, etc. The ADS-B message is broken into six parts including the preamble [Figure 19].

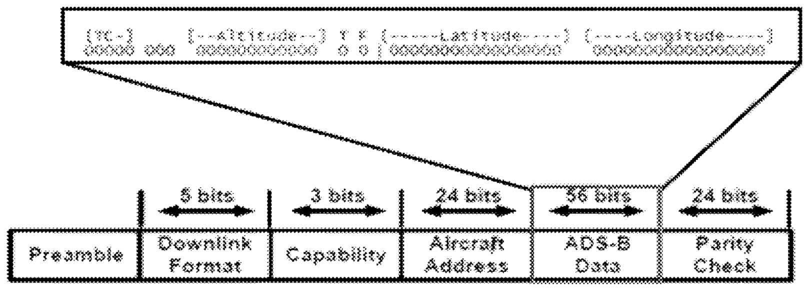


Figure 19 - ADS-B message format. Modified from [2].

The first field of the message is the DF type; as discussed ADS-B messages are set to 17 or 10001 binary. The next field is the capability field or subtype field. This field describes the specific data being transmitted by the ADS-B message. The subtype message focused on for this research is subtype five, positional reports. This field will be set to "101" for all tests. Following the capability field is the aircraft's ID, which is a three byte field that contains the ICAO designation for each aircraft. The aircraft ID is assigned for the life of the aircraft but can be changed if necessary. Following the aircraft ID are the 56 bits of ADS-B data, containing information about the altitude, latitude, and longitude of the aircraft. Finally, the last field is the parity check, which is 24 bits. The parity bits are obtained using a cyclic redundancy check polynomial applied to the first 88 bits of the message.

3.5.3 Downlink Format and Aircraft ID Decoding

The first two fields can be converted to decimal format from its current binary format to determine the DF type and capability field. Because the aircraft ID is in hexadecimal notation (6 hex characters) no decoding is necessary. Decoding the altitude, latitude, and longitude requires multiple calculations and will be discussed next.

3.5.4 Altitude Decoding

The altitude is comprised of 12 bits (bits 41-52). In order to decode the altitude, bit number eight of the 12 bits, counting from left to right, is removed. This is known as the Q bit. This bit determines whether the altitude is being reported in 25 foot increments (set to '1') or 100 foot increments (set to '0') [Figure 20]. After determining the increment value, the first seven bits are shifted to the right, essentially eliminating the Q bit. This will leave a binary number that can now be converted to decimal. Once in decimal format, the number is multiplied by the increment (25 or 100), and the final step is to add 1,000 to it.

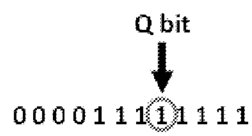


Figure 20 - Q bit representation for altitude

For example, assume the altitude bit pattern is 000011111111. Since the Q bit is set to one, the altitude is being reported in 25 foot increments. The Q bit is then eliminated, which leaves 000001111111 or 127 decimal. Next, the decimal number is multiplied by 25 for a product of 1,175. Finally, 1,000 is added to give a decoded altitude of 2,175 feet.

3.5.5 Latitude and Longitude Decoding

The next decoding to take place is the latitude and longitude. These two fields are each 17 bits. There is an additional two bits designated for Compact Position Report

(CPR) format, which makes 36 bits total for this information. CPR was developed for ADS-B messages to reduce the number of bits required to transmit positional data. Accuracy for ADS-B messages is within 5.1 meters, since the Earth's circumference is around 40,000 kilometers that would require almost 7.8 million position values (40,000m/5.1m) or 23 bits of data (2^23 = 8,388,608). In order to fit the positional data into 17 bits, the higher order bits are eliminated. The higher order bits contain information such as the hemisphere in which the aircraft is located. Since an aircraft in most cases will remain within the same hemisphere for the lifetime of the aircraft, they can be eliminated. In order to accomplish this without causing ambiguity, the Earth is divided into odd and even latitude and longitude zones [Figure 21]. In order to determine the precise location, both odd and even CPR messages must be received. These two formats differ slightly in their calculations, but will be used to narrow down the location of the aircraft to an X and Y coordinate within one zone to within the 5.1 meter accuracy mentioned earlier.

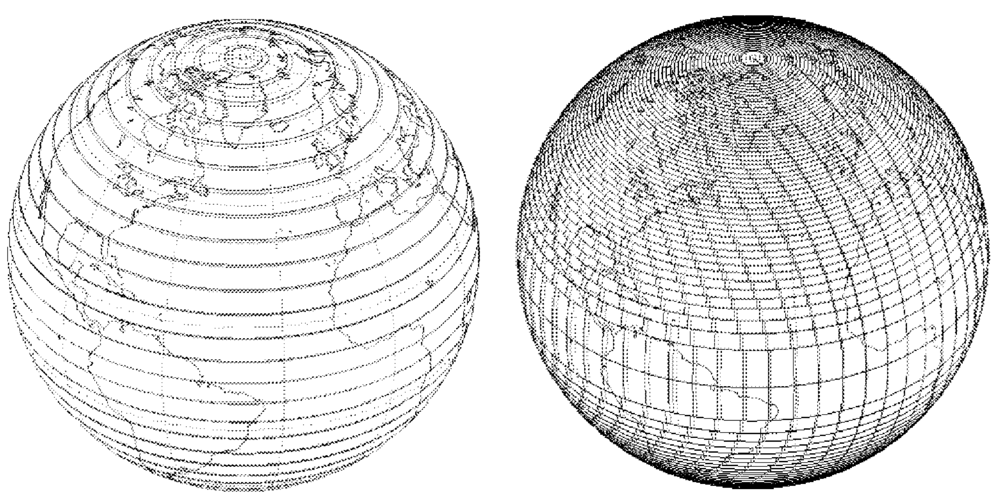


Figure 21 – Latitude (left) and longitude (right) zone boundaries [6]

The equations throughout the decoding process were found at [61]. The first step in decoding is to calculate the latitude index designated by the letter *j* as shown in Equation 1. *Lat(0)* and *Lat(1)* are the odd and even format messages received.

$$j = \left(\frac{59 * Lat(0) - 60 * Lat(1)}{131072}\right) + \frac{1}{2} \quad (1)$$

Following that the recovered latitude (*Rlat*) is calculated. This calculation is performed for both the odd and even messages [Equation 2]. For this equation, the zone size is designated by the variable $Dlat_i$. $Dlat_1$ and $Dlat_0$ differ slightly with an odd message equal to 360/4*(Number Of Zones-1) and an even message equal to 360/4*(Number of Zones). The number of zones equals 15 as this is the amount of zones within each quadrant of the Earth. The modulus function within this equation returns the remainder of dividing the first variable by the second variable.

$$rlat(i) = Dlat_i * \left(\text{modulus}(\text{j}, 60) + \frac{Lat(i)}{131072}\right) \quad (2)$$

The next variable to determine is the number of longitude zones (*NL*). This is determined by using the *rlat* value from the previous equation. A lookup table [Appendix C] is used to determine the *NL(rlat)* value. Next is the width of the longitude zone (*ni*) which is calculated by dividing 360 by *NL – i*. Further decoding leads us to the *longitude index* [Equation 3].

$$Longitude\ Index = \frac{\left(Lon(0) * (NL(i) - 1)\right) - \left(Lon(1) * NL(i)\right)}{131072} \tag{3}$$

Finally, the longitude of the second message received (the odd message) is found using [Equation 4].

$$Longitude = Dlon(i) * \left(\frac{\left(modulus(longitude\ index, ni)\right) + Lon(i)}{131072}\right) \tag{4}$$

The final field to decode is the parity check. The parity bits are calculated through a cyclic redundancy check (CRC) with a generating polynomial and using the first 88 bits of the ADS-B message [Equation 5]. It is assumed the user has general knowledge of how CRC bits are generated and will not be covered in great detail. Information for generating CRC bits can be found at [62].

$$\boldsymbol{G(X) = 1 + x^{3} + x^{10} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24}} \tag{5}$$

The preceding discussion focused on decoding the ADS-B message bits. Encoding an ADS-B message is essentially the reverse.

3.6 USRP and ADS-B Transmission

Just as in receiving, the transmission of ADS-B signals will require the correct hardware to transmit the messages at 1Mb/second at the carrier frequency of 1090MHz. For this setup, all equipment previously described was used. The use of the GNU radio companion (*GRC*) was used in the creation of the transmitter. *GRC* is a GUI application installed with the *UHD+GNURadio* script. To run *GRC* the command *gnuradio-companion* should be executed. Within the *GRC* are pre-built blocks that allow construction of SDR applications in a drag-and-drop fashion. The flow of information is then created by connecting each block's output to another block's input. The beginning block is called the source and the flow of information will end with a sink. When a *GRC* application is executed, Python scripts that control the USRP radios are automatically generated.

Figure 22 shows a *GRC* representation for the *ADS-B Transmitter*. A file source is used to provide the binary representation of the ADS-B message. This message has been properly encoded with all ADS-B message components as discussed in section 3.5, Figure 19. It has also been generated using proper PPM coding. Next is the *packed-to-unpacked* block, which extracts message bits from the file one bit at a time and prepares it for transmission. As the name states, this block receives packed data (hexadecimal format) and unpacks it into its binary format. For example, a hexadecimal "A" received from the file will be unpacked to "1010". A "1" read from the binary file will result in a pulse with amplitude of one, a "0" will result in no pulse.

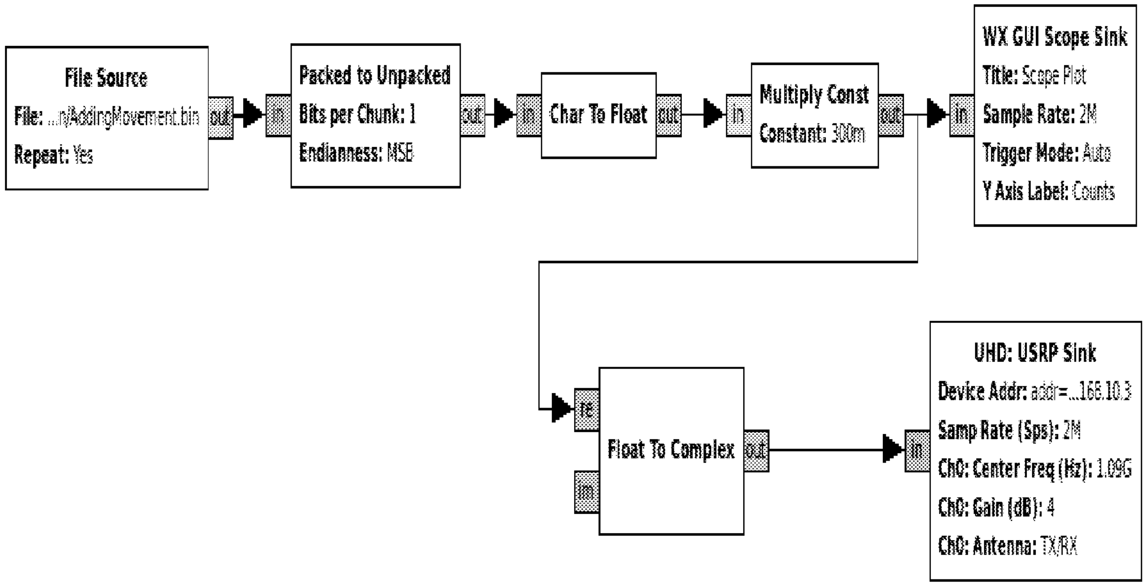


Figure 22 - GNU Radio Companion screenshot containing the *ADS-B Transmitter* application

The *char-to-float* block converts the binary bits to a floating point representation, which allows manipulation of the data using floating point numbers. For this case, the amplitude of one is multiplied by 0.3, decreasing the amplitude of the pulse from a height of 1 to 0.3. This is performed because the USRP cannot handle amplitude of 1 without causing pulses to overlap (smear), which would result in errors in our message.

There are two sinks for this *GRC* program. The *scope sink* is included to aid in troubleshooting issues with the signal and does not affect the application. The second sink is the USRP. Before the signal flows to the USRP, it goes through a *float-to-complex* block, this converts floating point data to complex data for upconversion to RF (1090 MHz).

The parameters of the USRP include the IP address of the USRP, sample rate, transmission gain, and antenna choice. The sample rate should be set to 2Ms/s in order to satisfy Nyquist's Theorem, described earlier. The transmission gain was set to default at four, best results when running the program were found between a gain of one and four. Finally, the antenna used throughout the research was the transceiver (TX/RX).

Another SDR application was designed within *GRC* to assist in troubleshooting any issues with the transmission of ADS-B messages [Figure 23]. The blocks involved with this application are a USRP source, a *complex-to-magnitude* block, and a *scope sink*. The USRP is tuned to the 1090MHz frequency and uses the *complex-to-magnitude* block to perform amplitude demodulation on the received signal, which is then fed into a *scope sink* for a visual look of the received message.

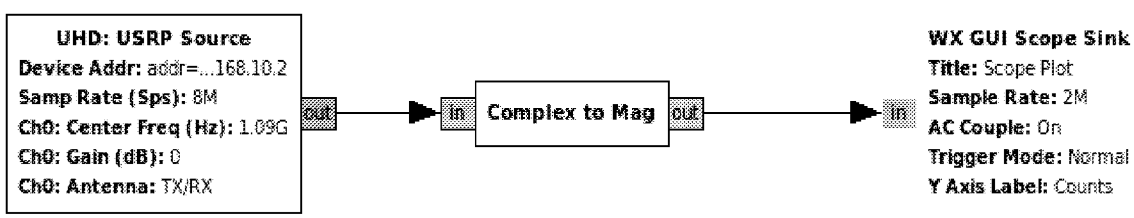


Figure 23 - *GRC* view of the ADS-B troubleshooting application

Using two USRPs connected by a 30 dB attenuator, a message was transmitted and received [Figure 13]. The results of that transmission were observed with the *scope sinks*. These two scope plots show the message before transmission [Figure 24] and the message upon receiving it with the other USRP [Figure 25].

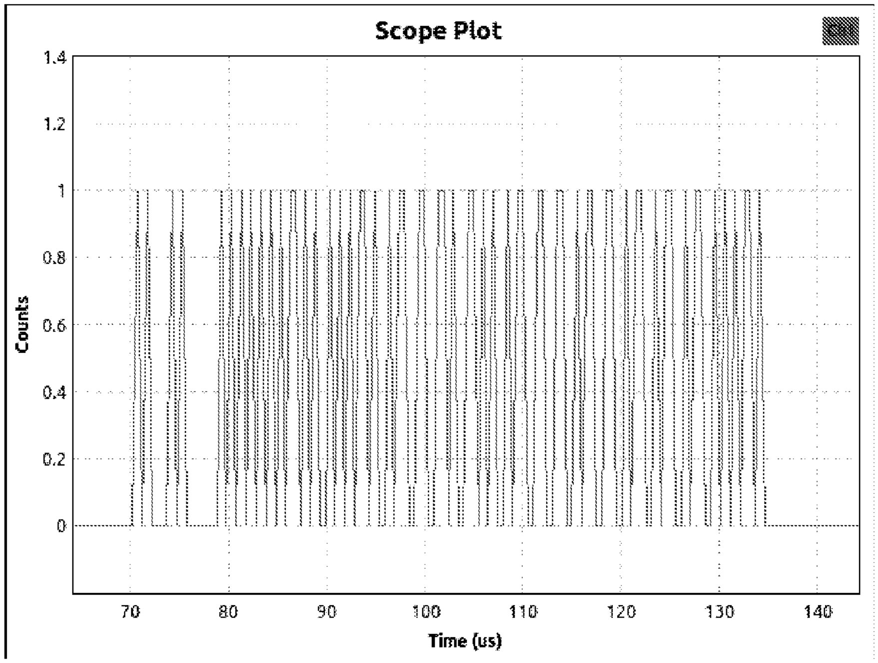


Figure 24 - Scope plot of transmitted message

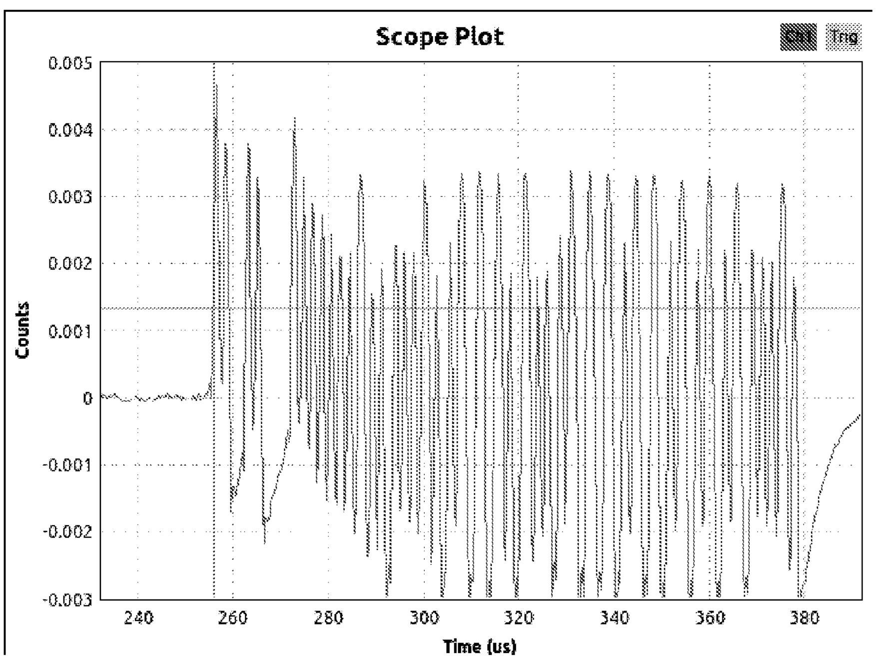


Figure 25 - Scope plot of received message

3.7 ADS-B Message Generation

The preceding sections have created the foundation for generating and transmitting ADS-B messages. This section discusses the calculations necessary to create the data file containing the encoded aircraft ID, altitude, positional data, and CRC bits. Appendix B contains a C++ program that accepts data input and generates a properly encoded ADS-B message.

Encoding an ADS-B message requires four inputs: aircraft ID, altitude, latitude and longitude. The aircraft ID will be entered as hexadecimal characters (0-9 & A-F). The altitude will be an integer divisible by 25, as all altitude will be encoded in 25ft increments for greater precision (compared to 100ft increments). Finally, the latitude and longitude inputs represented by degrees, minutes, and seconds (DDDMMSS) will be entered in decimal format. The DDDMMSS information is converted to decimal degrees for latitude and longitude using the following formula:

$$Decimal\ Degrees = Degrees + \frac{Minutes}{60} + \frac{Seconds}{3600} \qquad (6)$$

After converting latitude and longitude into decimal numbers, it must be determined if they will be negative or positive. Using Figure 26, locations north of the equator will yield positive latitudes while locations south of the equator will be negative. Finally, locations east of the prime meridian will result in negative longitudes and vice versa for locations west of the prime meridian.

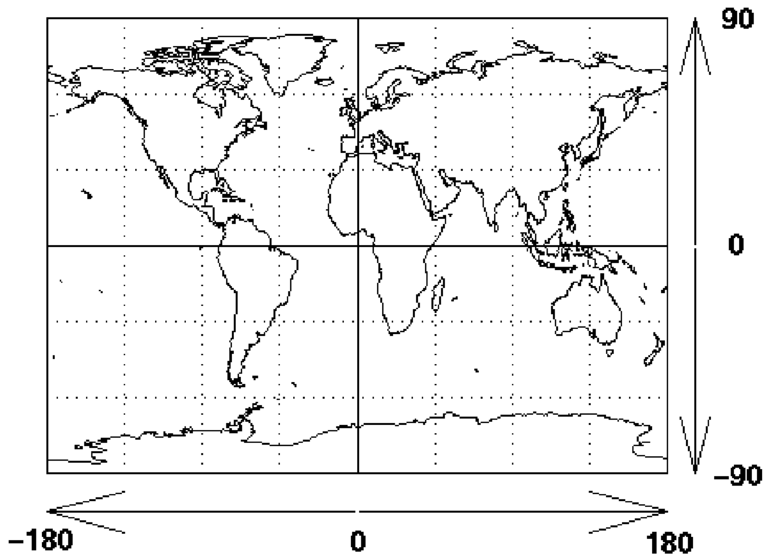


Figure 26 - Latitude and Longitude Measurements

3.7.1 DF Type

To construct the message as shown in Figure 19, the first step is to append the DF format type. This value, 0x8D or 10001101, is added to the message automatically by the C++ program. The first five bits (10001) equates to 17 decimal or the desired DF format type. The last three bits are a capability field referring to the specific data being transmitted, throughout this research this field will refer to positional data reports (subtype five).

3.7.2 Aircraft ID Generation

The next data to be entered is the aircraft ID. This is represented by six hex characters or three bytes of data. Since this information is entered as hexadecimal characters it does not need to be manipulated. It can be appended directed to the DF type and stored within the message array.

3.7.3 Altitude Encoding

Following the aircraft ID generation is the altitude calculations. This data is entered as a decimal number. To encode it requires subtracting 1,000 and then dividing the number by 25. As discussed earlier, room must be made for the Q bit. The values in the last four bits are held in memory. Following that, the first eight bits are shifted to the left by one. An OR is then performed to concatenate the shifted bits and the last four bits. To complete the encoding, the Q bit set to 1 (25 ft increments), is added in the eighth bit position. Similar to the aircraft ID, hexadecimal 0x58 is then appended to the front of the altitude to denote a type code of 11 (**01011**000), which equates to an airborne position report. The three zeros in the remaining in this field provide surveillance status within the first two bits and the antennas used in the last bit. These three bits are irrelevant to this research and will be set to "000" for all tests. The value for altitude is then stored within the message array.

3.7.4 Latitude and Longitude Encoding

The next two data inputs are the latitude and longitude. These require many more calculations but follow similar procedures as the decoding section. The first step is to determine $Dlat_i$, the latitude zone size [Equation 7]. These numbers will remain constant throughout the life of the program. *NZ* is the number of zones per quadrant which will be 15 at all times. The variable *i* refers to the format type (1 odd or 0 even).

$$Dlat_i = \left(\frac{360}{4*NZ-i}\right) \qquad (7)$$

After determining the *Dlat* values, the next calculation is the *YZ* value or Y coordinate within the Zone. This is calculated using the *Dlat* value and the latitude value input by the user [Equation 8]. The result of this equation will give an integer within the 17 bit limit. *Floor(x)* is defined as the greatest integer *k* such that $k \leq x$. For example, *floor(5.6)* will be equal to 5, while *the floor(-5.6)* equals -6. This integer is then assigned to a variable for later use.

$$YZ_i = \text{floor}\left(2^{17} * \left(\frac{\text{modulus}(lat, Dlat_i)}{Dlat_i}\right) + \frac{1}{2}\right) \qquad \textbf{(8)}$$

Realized latitude is then calculated. This value will be approximately the same value as that entered by the user. The latitude, *YZ* and *Dlat* values are all used for this calculation as shown in Equation 9. The realized latitude or *Rlat* value, calculated during this step is then used to determine the specific longitude zone or *NL*. *NL* is set via a look up table as described earlier.

$$Rlat_i = Dlat_i * \left(\left(\frac{YZ}{2^{17}}\right) + \text{floor}\left(\frac{latitude}{Dlat_i}\right)\right) \qquad \textbf{(9)}$$

Using the *NL* value returned by the lookup table [Appendix C], the longitude zone size (*Dlon*) can then be determined with the simple equation [Equation 10].

$$Dlon_i = \begin{cases} \dfrac{360}{NL(Rlat_i) - i} & \text{when } NL(Rlat_i) - i > 0 \\ 360 & \text{when } NL(Rlat_i) - i = 0 \end{cases} \tag{10}$$

Finally, the encoded longitude value is calculated. This is known as the *XZ* value or X coordinate within the Zone:

$$XZ_i = \text{floor}(2^{17} * \left(\left(\frac{\text{modulus}(longitude, Dlon)}{Dlon}\right) + \frac{1}{2}\right)) \tag{11}$$

After both numbers have been generated (*YZ* and *XZ*), they are concatenated onto each other. It should be noted that these numbers are not added together. The *YZ* value is shifted to the left 17 positions and then OR'd with the *XZ* value. This 34 bit value is now ready for transmission as an even message. In order to transmit as an odd message the bit in position #35 ("F" bit from Figure 19) must be set to "1". This value is then added to the message array in preparation for the final calculations before being written to a binary file.

3.7.5 CRC Bit Generation

The final step of encoding is to apply the CRC polynomial to compute the parity bits. The code for generating CRC bits has some preliminary bit manipulation before beginning the XORing. The first seven lines of code within the CalculateCRC112BitsOdd function ensure 4 bytes of data are in each of the variables to be XOR'd. Once this takes place, the individual portions of the message begin a loop that iterates until all 88 bits have gone through. The result of XORing the 88 bits with a 25 bit polynomial will result in a remainder of 24 bits. These bits are stored within the message array, which can now be written to a binary file. The file will be called *FinalMessage.bin*, located in the same directory as the *DF17MessageGenerator*. The user can then set this file to be the source of the *ADS-B Transmitter* [Figure 22].

3.7.6 Transmitting the Messages

Once the file is set as the source, there are two options for running the *ADS-B transmitter*. Those options are to run it from the *GRC* application or run it via command line. After execution begins, the scope plots for the *ADS-B Transmitter* as well as the ADS-B message analyzer (discussed earlier), will prove useful.

3.8 Summary

This chapter presented the development of a system comprised of a computer, USRP, and C++ code for generating acceptable ADS-B messages. Additionally, it discussed the process of decoding and encoding ADS-B messages for transmission. The next chapter discusses the validation of the system and covers some applications of how the system can be used to generate and inject false messages.

IV. Analysis and Results

4.1 Chapter Overview

This chapter will discuss the techniques used to validate the system developed in Chapter III. The first section will discuss the *GR-AIR-MODES* validation process. Following that will be the validation of the contributions of this research, the *DF17MessageGenerator* and the *ADS-B Transmitter*. Finally, demonstrations will be conducted and analyzed to display the potential capabilities of the system.

4.2 Validation of ADS-B Systems

It is reasonable to question the validity of *GR-AIR-MODES* and the *ADS-B Transmitter* created with the USRPs. *GR-AIR-MODES* depends on the code developed in [60] while the *ADS-B transmitter* application is dependent on the code developed in this research. The SBS-1eR commercial receiver was used to validate the operation of both *GR-AIR-MODES* and the *ADS-B Transmitter*. After validating the *GR-AIR-MODES* program it was used to validate the *DF17MessageGenerator*.

4.2.1 *GR-AIR-MODES* Validation

In order to validate the *GR-AIR-MODES* program, it was run side-by-side with the SBS-1eR multiple times. The intention of these experiments was to compare the data captured by both receivers. Should the commercial device and *GR-AIR-MODES* program capture similar data, it is assumed *GR-AIR-MODES* performs accurately.

During the side-by-side experiments, *GR-AIR-MODES* was run with the –K option invoked to store all ADS-B data within KML files for viewing within Google

Earth. This option was used to replicate the virtual radar screen generated by the SBS-1eR software. Throughout all experiments, the devices captured the exact same information. The results of one of the experiments conducted are shown in Figure 27. During this experiment, there was one aircraft broadcasting ADS-B data. This data was captured by both the SBS-1eR and *GR-AIR-MODES*.

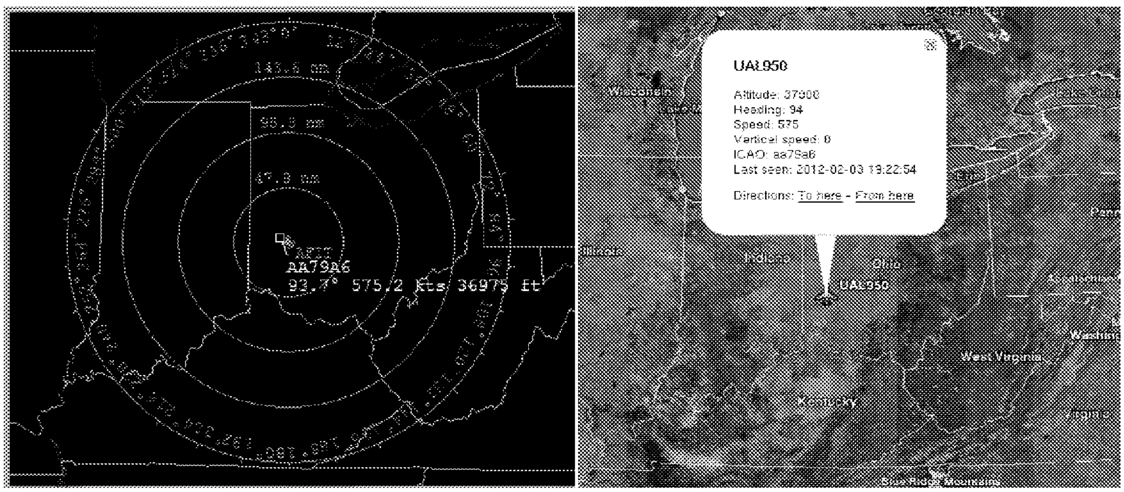


Figure 27 - Side-by-side view of SBS-1eR (left) and *GR-AIR-MODES* (right)

Additional data captured during this particular experiment included altitude, speed, and heading [Figure 28] [Figure 29]. Both devices were able to capture and decode precisely the same information with a heading of approximately 94°, a speed of 575 knots (~661 mph), an altitude of 37,000ft and a location of latitude 35.854721 and longitude -84.266113. A slight difference in longitude and altitude, shown within the figures below, is a result of the delay in capturing a screen shot for both programs (i.e., the aircraft kept broadcasting data so *GR-AIR-MODES* received one additional message with updated information).

Status	State	Show Trail	Flag	Operator	Code	Callsign	Country	Altitude	Latitude	Longitude	Speed	Track
					AA79A6		United States	36,975 ft	39.854°	-84.241°	575.2 kts	93.7°

Figure 28 - SBS-1eR captured data

```
(-31 0.0000000000) Type 17 subtype 05 (position report) from aa79a6 at (39.854721, -84.266113) (27.78 @ 350) at 37000ft
(-31 0.0000000000) Type 17 subtype 09-1 (track report) from aa79a6 with velocity 575kt heading 94 VS 0
```

Figure 29 - *GR-AIR-MODES* captured data

4.2.2 *DF17MessageGenerator* Validation

GR-AIR-MODES can then be used to validate the *DF17MessageGenerator*. For the purpose of validation, the –w command was used during *GR-AIR-MODES* execution. This command will display the ADS-B message in its hexadecimal format in the command prompt window [Figure 30]. The aircraft information, to include aircraft ID, altitude, and position, were then used as input for the *DF17MessageGenerator*. The message displayed by *GR-AIR-MODES* was then compared to the message generated by the *DF17MessageGenerator*. The *DF17MessageGenerator* produced the exact same results [Figure 31].

```
(-32 0.0000000000) Type 17 subtype 05 (position report) from ab7437 at (39.925827, -84.193542) (33.09 @ 347) at 36025ft
17 8dab7437 58b9929e02f39d 984e70 000000 0.0005643221084 0000000000
```

Figure 30 - Raw data displayed by *GR-AIR-MODES*

```
dmagazu@dmagazu: ~/Desktop
File  Edit  View  Search  Terminal  Help
This program will generate a Mode-S Downlink Format 17 Message, also known
as an Automatic Dependenet Surveillance Broadcast (ADS-B) Message.
Press 1 <ENTER> to begin message generator.
1
Enter an aircraft ID 3 Bytes (Example: BEEF11):
ab7437
Please enter an altitude (0ft - 50,000ft):
36025
Please enter your requested Latitude:
39.925827
Please enter your requested Longitude:
-84.193542
ADS-B Message : 8dab7437 58b99 29e02f39d 984e7000
############################################################
```

Figure 31 - *DF17MessageGenerator* validation message

4.2.3 *ADS-B Transmitter* Validation

The final step is to validate the *ADS-B Transmitter*. To perform this validation, the USRP N200 ran the *ADS-B Transmitter* with a file source containing the message from the previous validation (Aircraft ID AB7437, altitude 36025, latitude 39.925827 and longitude -84.193542). The USRP N200 then transmitted the message, which was received successfully by the SBS-1eR [Figure 32]. The results showed the successful reception and display of the ADS-B message [Figure 33]. The bottom left corner of the figure displays the altitude, the top left corner shows the virtual radar display with the aircraft plotted in the correct position, and the right side of the figure displays the aircraft's information to include the latitude and longitude points.

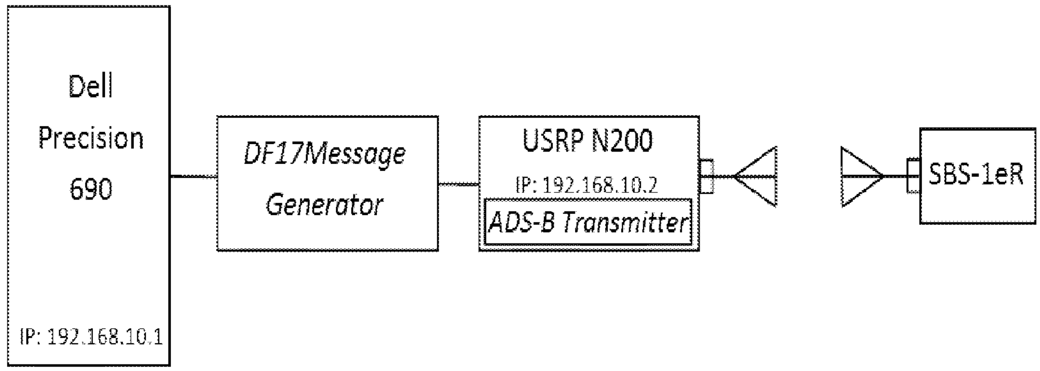


Figure 32 - System block diagram for implementation/use

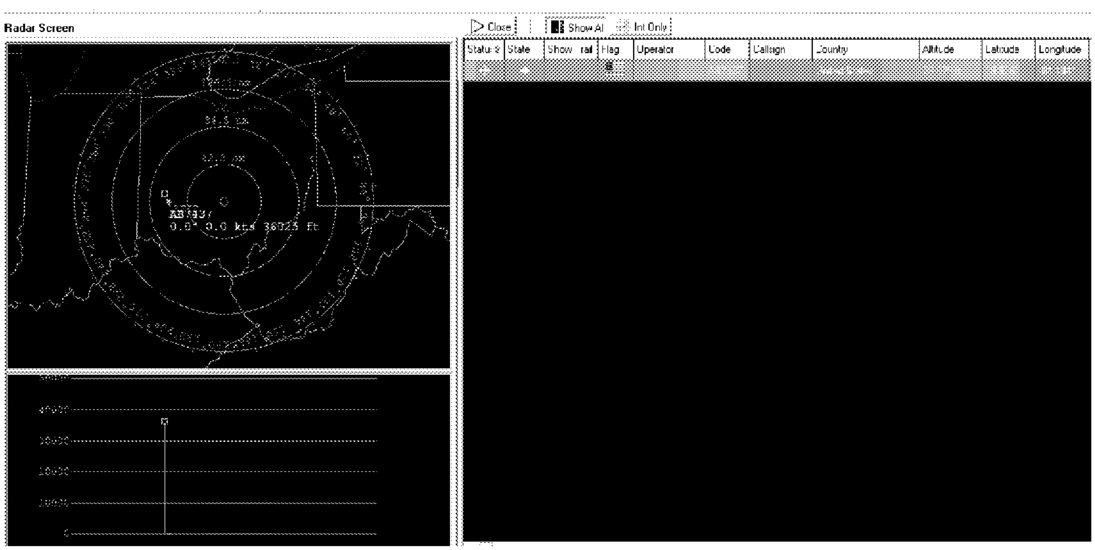


Figure 33 - *ADS-B Transmitter* Validation

4.3 Demonstrating the *DF17MessageGenerator* and *ADS-B Transmitter*

After completing the validation of the systems, four demonstrations were performed to exhibit the system's potential. All experiments were conducted using the

DF17MessageGenerator and the *ADS-B Transmitter*. The first demonstration was to plot multiple aircraft on the radar display of both *GR-AIR-MODES* and the SBS-1eR. Next, live data received by the SBS-1eR was observed, altered, and rebroadcast. The third demonstration plotted false aircraft following a live aircraft. Finally, an aircraft track was generated, which involves having a false target "move" through the airspace.

4.3.1 Flooding Radar Display

The first scenario tested was flooding the radar screen with false targets. To demonstrate this scenario, 10 aircraft messages were generated using the *DF17MessageGenerator* and then transmitted using the USRP/*ADS-B Transmitter*. Both *GR-AIR-MODES* and SBS-1eR were used to receive and plot the aircraft with varying locations and altitudes, as shown in Figure 34 and Figure 35. This technique could be implemented using as few or as many aircraft as desired to cause confusion within the airspace and in ground facilities.

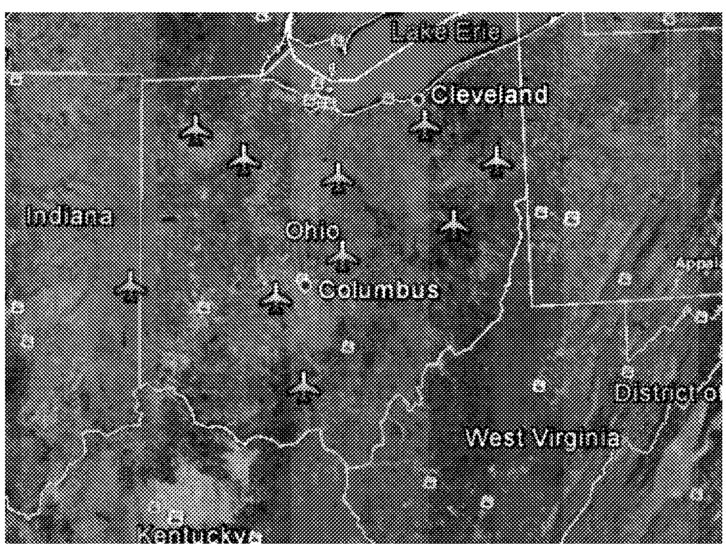


Figure 34 - Google Earth view of multi-aircraft scenario

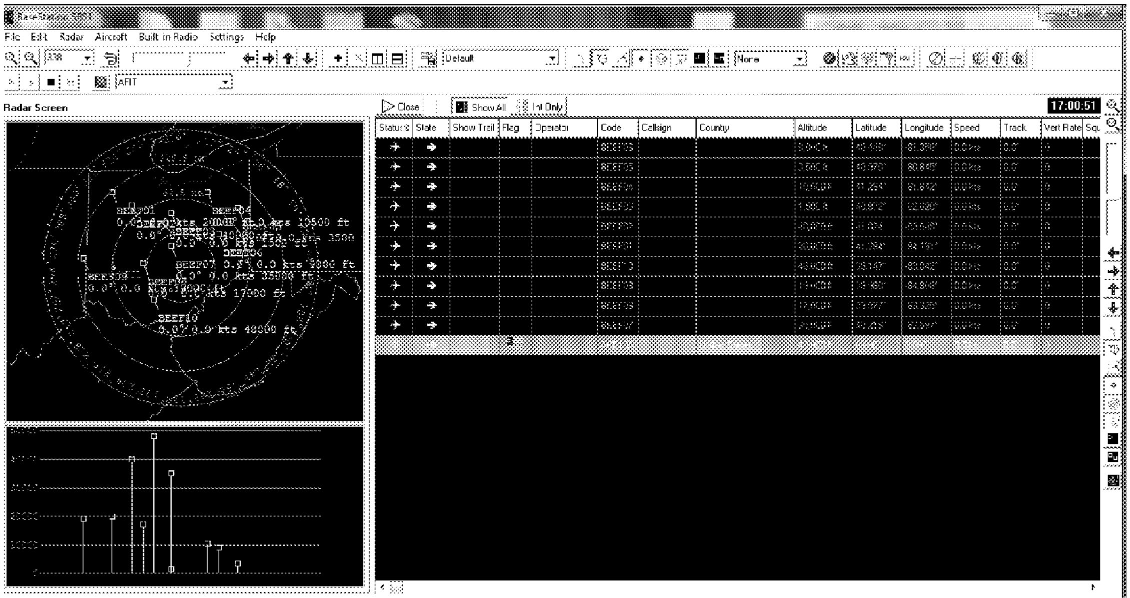


Figure 35 – SBS-1eR software view of multi-aircraft scenario

4.3.2 Altering Live Data

The next scenario requires the reception of live data, altering the information such as the altitude or location, and broadcasting the new spoofed message. This scenario could be used to "change" the position of an aircraft and cause confusion within the cockpit of an aircraft or at an ATC ground facility.

To demonstrate this scenario, live data was captured using the SBS-1eR. Once an aircraft broadcasting ADS-B messages appeared on the radar screen, its data was entered into the *DF17MessageGenerator* [Figure 36] with a different altitude and position.

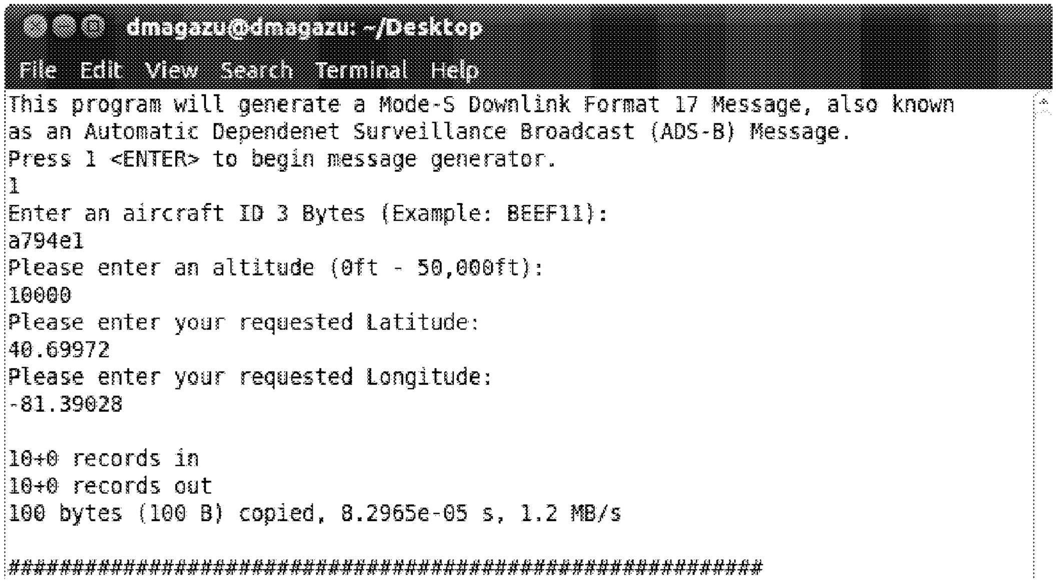
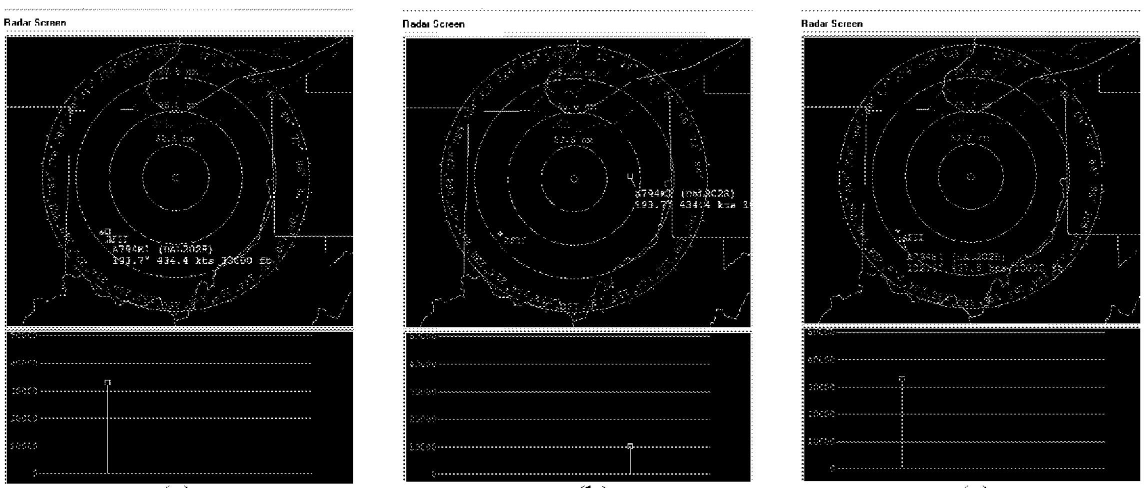


Figure 36 – Entering altered data for live data scenario

Using the *ADS-B Transmitter*, the spoofed message was then broadcast. After a few seconds, the SBS-1eR shows a change in data for the aircraft with aircraft ID A794E1. First, a change in altitude (from 33,000 ft to 10,000 ft) is observed and then the position changes to the spoofed position coordinates. The lag in positional change is due to the calculations involved in converting the odd and even messages to an exact X and Y coordinate within the latitude and longitude zones. Once the position has been determined, the aircraft seems to jump from its current location (a) to the false position (b). The position can be viewed in the top portion of the figure and the altitude can be observed within the bottom section. After turning the *ADS-B transmitter* off, the aircraft's true position and altitude return [Figure 37]. In (c), the aircraft is highlighted blue as the receiver interprets the change in altitude (from 10,000 ft to 33,000 ft), as the aircraft ascending. Of note, the figure gives the impression that the true aircraft position vanishes. This is due to the close proximity of the *ADS-B Transmitter* to the SBS-1eR, causing the commercial receiver to be flooded with the spoofed message, which is transmitted repeatedly. In reality, both the real aircraft and spoofed aircraft would appear on the display of an aircraft or ATC ground facility.

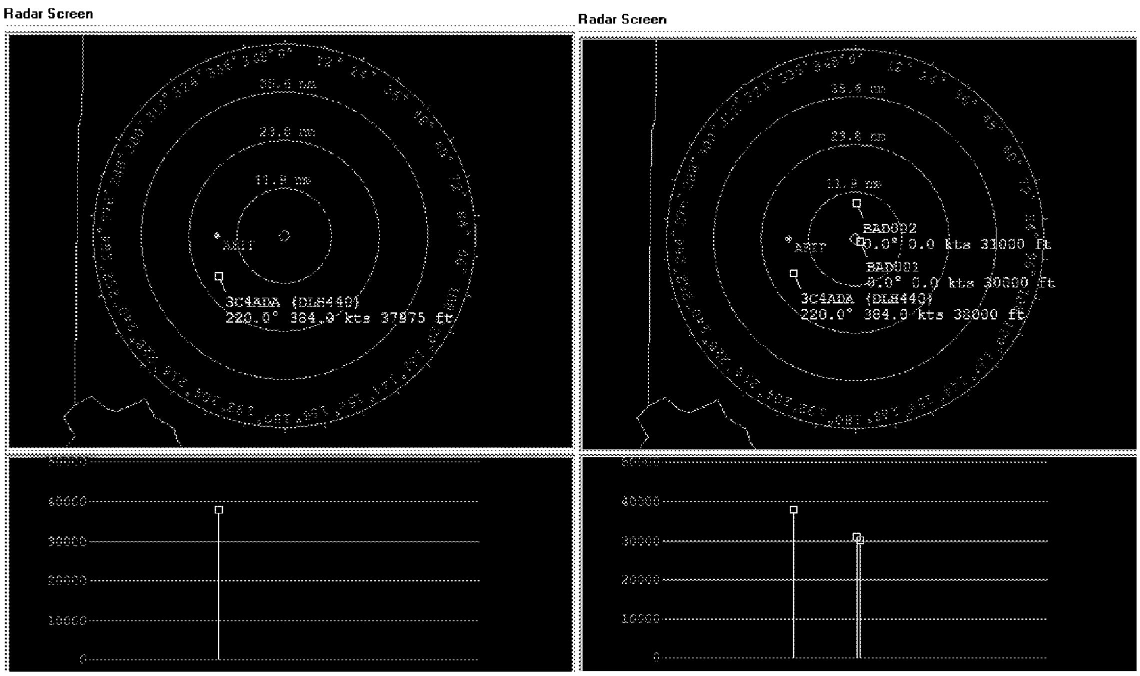


(a) (b) (c)

Figure 37 - Series of SBS-1eR screen captures (a) shows original aircraft data, (b) shows aircraft data of spoofed messages, and (c) shows aircraft returning to original location

4.3.3 False Aircraft Following

The third demonstration also awaited the reception of live aircraft data using the SBS-1eR. Once an aircraft was displayed, two ADS-B messages were generated with aircraft IDs of BAD001 and BAD002. Both false messages had coordinates trailing the aircraft by approximately 15-20 nautical miles. This demonstrates the ability to inject false aircraft in the vicinity of real aircraft in an expedient manner. If the locations of the false aircraft were closer to the target it may cause confusion for the pilots, which could lead to unnecessary corrections to avoid a mid-air collision.



(a) (b)

Figure 38 - Radar display for aircraft following scenario (a) shows the live aircraft and (b) shows the two spoofed aircraft trailing

4.3.4 Aircraft Track Generation

The final demonstration to be discussed is the production of an aircraft track. This involves having a false target "move" through the airspace by changing the position values in the ADS-B messages that are transmitted on a regular basis. This demonstration generated movement for one aircraft, however multiple false tracks could also be generated. This can also be applied to any of the previous demonstrations.

To execute this scenario, a message must be generated to establish the point of origin of the false aircraft. Subsequent messages should then follow within 1-10 seconds of each other using appropriate latitude and longitude points for movement in any direction [Figure 39]. The scenario produced an aircraft with Aircraft ID D3D3D3 moving in an eastward direction. The dots on the figure represent the reception of individual ADS-B messages. An update was sent once every second giving the impression the aircraft traveled over 50 nautical miles.

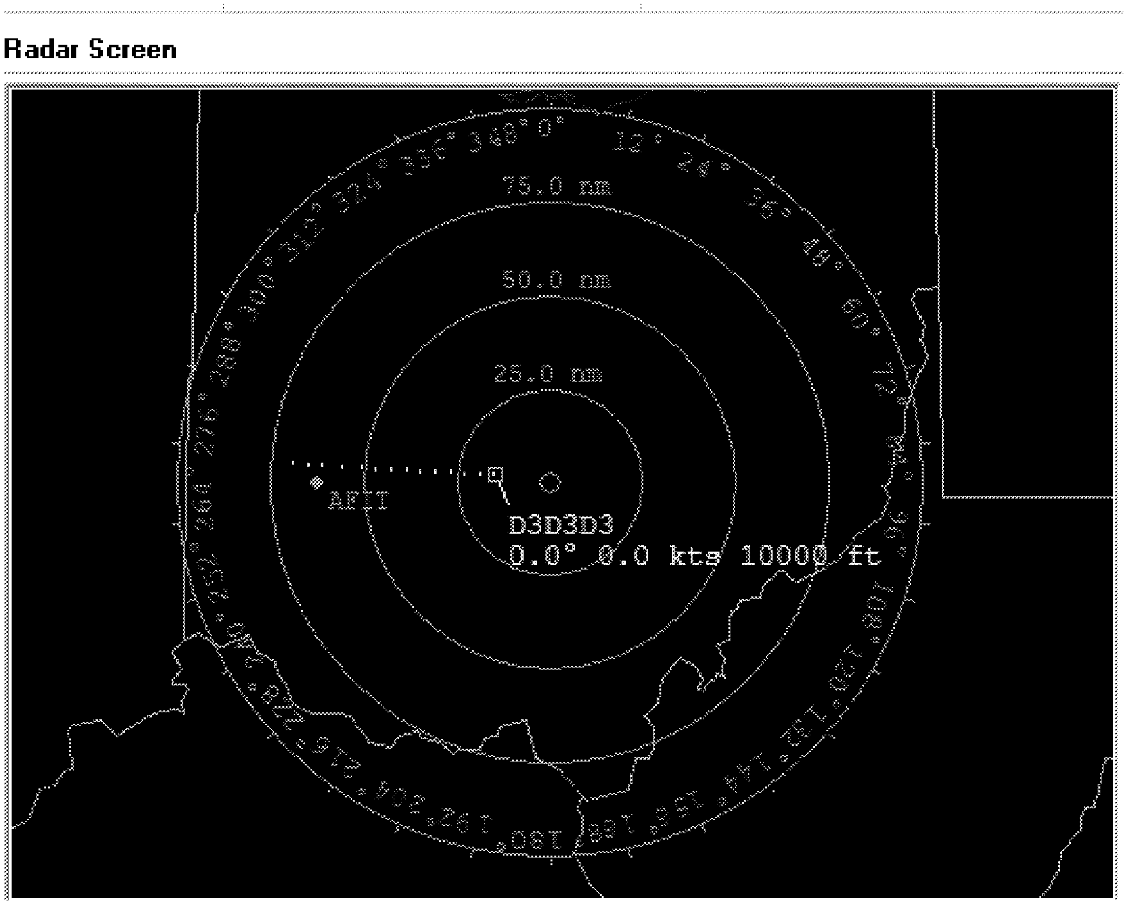


Figure 39 – SBS-1eR radar picture of false aircraft track

4.4 Summary

The demonstrations within this chapter emphasize the potential of the *DF17MessageGenerator* and *ADS-B Transmitter* to generate false/deceptive ADS-B messages. With a limited amount of time, it was not feasible to construct more demonstrations, however the work provided here creates a strong foundation for the capabilities of the system developed in this thesis. It is assumed by the amount of success already achieved that the uses of the system are only limited by the imagination.

V. Conclusions and Recommendations

5.1 Chapter Overview

This chapter reviews the work completed and offers conclusions on the information discovered through the experiments. The investigative questions from Chapter I will be reviewed first, then discussions on further research related to this topic, and finally a summary.

5.2 Conclusions of Research

The purpose of this research was to investigate the weaknesses of the NextGen system to include the ability to inject false targets on the display of a commercial receiver. Additionally, this work investigated the ability to develop a proof of concept system using relatively inexpensive equipment. The author concludes that this research successfully developed a system capable of generating ADS-B messages and transmitting them in accordance with ADS-B message protocol. Furthermore, the messages transmitted were successfully received and displayed by a commercial ADS-B receiver, the SBS-1eR.

5.3 Investigative Questions Answered

The research and methodology described in the previous chapters revealed the steps required to encode raw data and transform it into a properly formatted ADS-B transmission. The majority of the information for encoding could be found within RTCA DO 260 Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast which is purchasable for approximately $150.00. The reason the author did not purchase and use this document was to illustrate the ease in which an individual could find the necessary information as well as maintain anonymity.

The accomplishments of this thesis showed that with some knowledge of digital signal processing (DSP) and the ability to write code in Python and C++, it is possible to develop a system capable of generating acceptable ADS-B messages. "Acceptable" means good enough to be recognized by commercial off-the-shelf equipment that are used to decode ADS-B broadcasts. The messages ranged from single aircraft to multi-aircraft broadcasting. Additionally, the messages were used to generate aircraft tracks to imitate the travel of an aircraft across the radar screen of a receiving station.

The creation of the system took approximately six months for an individual with little to no background in DSP and RF communications. The system developed was composed of two USRPs with appropriate RF daughterboards and antennas, a Dell personal computer, and freely available software. In reality, once the system is built, two USRPs are not necessary. Excluding the second device and its associated daughterboard, the cost for creating this system was less than $5,000.00, with the USRP costing $1700.00, an antenna $35.00, WBX daughterboard $450.00, and the Dell Precision 690 costing approximately $2,000.00. The software for DSP applications along with the operating system came at no cost as they are freely available for download and use.

Finally, the potential capability of the system was also shown through the use of the system in four demonstrations. Those scenarios exhibited the use of the system in generating multiple false targets, altering live data being received, inserting false targets near real aircraft and lastly, creating an aircraft track.

5.4 Recommendations for Future Research

Although the system developed in this thesis has the ability to generate ADS-B messages, it currently can only create one message at a time. Future research should include generating multiple messages in a dynamic manner. The code, as currently written, will stack one message on top of another within the same file. This can be successful for most scenarios, to include all those discussed within chapter four. Future work could also include the development of separate functions to perform certain tasks such as generating a complete track with only a starting (both latitude and longitude) and end point.

In relation to work with generating a complete track, work with the 'great circle' calculations could prove to be useful in generating tracks for aircraft and the associated latitude and longitude points along a given track. The great circle premise states that for any two points on the surface of a sphere, there exists a circle that goes through both of those points. With further research into these calculations, it could then be incorporated into the current code for expedited long track message generation.

The system proved to work well within the experimental environment. However, it was not tested on real systems within an aircraft or at an ADS-B ground station. The low power of the USRP makes it ideal for the environment in which this thesis took place and prevents the transmissions from causing any interference or reception by aircraft equipped with ADS-B In. This is a limiting factor in that the system could not be tested aboard aircraft to determine if the messages displayed upon the SBS-1eR would also show on the displays of a cockpit. Further real-world testing is therefore needed.

Additional research could be performed in the use of ADS-B subtype 9 messages. This provides aircraft speed and track information. When broadcasting spoofed messages throughout this research, it can be observed that the speed and track information located below the aircraft displayed on the SBS-1eR shows zeros. Having the ability to add this information to the current system would increase the appearance of an authentic aircraft broadcasting ADS-B data.

Finally, future research could be conducted with the non-commercial ADS-B data link, UAT or 978 MHz. Experiments could be conducted to test if the current system would have the ability to generate false targets using this link.

5.5 Summary

The system produced through this research was comprised of the following components, GNU Radio for the software defined radio application, a USRP front end, and the development of a C++ program to properly encode messages. Through the validation techniques described in Chapter IV the system proved it has the ability to generate and transmit acceptable ADS-B messages. Moreover, the use of a commercial receiver was used to provide validation of receiving and displaying these false ADS-B messages.

The tools created through this research, the *DF17MessageGenerator* and the *ADS-B Transmitter*, have proved the hypothesis proposed by McCallie, et al [2] of spoofing ADS-B messages. These tools further show the weaknesses of the NextGen system. In conclusion, future research could identify further uses for this system.

Appendix A

Multiple devices per host

For maximum throughput, one ethernet interface per USRP2 is recommended, although multiple devices may be connected via a gigabit ethernet switch. In any case, each ethernet interface should have its own subnet, and the corresponding USRP2 device should be assigned an address in that subnet. Example:

Configuration for USRP2 device 0:

- Ethernet interface IPv4 address: 192.168.10.1
- Ethernet interface subnet mask: 255.255.255.0
- USRP2 device IPv4 address: 192.168.10.2

Configuration for USRP2 device 1:

- Ethernet interface IPv4 address: 192.168.20.1
- Ethernet interface subnet mask: 255.255.255.0
- USRP2 device IPv4 address: 192.168.20.2

Change the USRP2's IP address

You may need to change the USRP2's IP address for several reasons:

- to satisfy your particular network configuration
- to use multiple USRP2s on the same host computer
- to set a known IP address into USRP2 (in case you forgot)

Method 1: To change the USRP2's IP address you must know the current address of the USRP2, and the network must be setup properly as described above. Run the following commands:

```
cd <install-path>/share/uhd/utils
./usrp_burn_mb_eeprom --args=<optional device args> --key=ip-addr --val=192.168.10.3
```

Method 2 (Linux Only): This method assumes that you do not know the IP address of your USRP2. It uses raw ethernet packets to bypass the IP/UDP layer to communicate with the USRP2. Run the following commands:

```
cd <install-path>/share/uhd/utils
sudo ./usrp2_recovery.py --ifc=eth0 --new-ip=192.168.10.3
```

Appendix B

```
////////////////////////////////////////////////////////////
//Code developed to generate ADS-B messages//////////////
////////////////////////////////////////////////////////////

#include <iostream>
#include <fstream>
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <string>
#include <iomanip>

using namespace std;

long int completeMessageOdd[5];
long int completeMessageEven[5];
int Dlat0 = 6;              //even messages
double Dlat1 = 6.101694915254237288135593220339;  //odd messages
double pi = 3.14159265;
char buffer[30] = {0xA1, 0x40};

double Modulus(double val, double modval)
{

      if (val < 0) //Checking for negative angles
      {
            val = val + 360;
            int result = floor(static_cast<int>( val / modval));
            return val - static_cast<double>( result ) * modval;
      }
            else
            {
                  int result = static_cast<int>( val / modval);
                  return val - static_cast<double>( result ) * modval;
            }
}

int GenerateNlatValue(double latitude)
{
      double Nlat;
      double sqrtHold;
      double buff[63];
      int j = 2;
      for (int i = 2; i <=59; i++)
      {
      Nlat = 0.0;
      sqrtHold = 0.0;
      Nlat = (180/pi)*(acos(sqrt((1-(cos(pi/30)))/(1-
      (cos((2*pi)/i))))));
      buff[j] = Nlat;
      j++;
      }
```

```
	for (int k = 59; k >=2; k--)
	{
		if(latitude > buff[k])
		{

		}
		else
		{
			if (k < 2)
			{
				return 1;
			}
			return k;
		}
	}
}



int CalculateLatBitsOdd(double lat, double longitude)
{

	//Calculate YZ which will be what is put into our message
	double YZ;
	double modHold;
	int LatHex;
	modHold = Modulus(lat, Dlat1);
	modHold = (modHold/Dlat1);
	modHold = modHold * pow(2,17);
	modHold = modHold + .5;
	YZ = floor(modHold);

	//Calculate Rlatiude for airborne
	long double Rlat1;
	int floorHold;
	Rlat1 = (double)YZ / pow(2,17);
	floorHold = (lat/(double)Dlat1);
	floorHold = floor(floorHold);
	Rlat1 = Rlat1 + (double)floorHold;
	Rlat1 = Rlat1 * Dlat1;
	int NlLat = GenerateNlatValue(Rlat1);

	//Calcule DLongitude
	double Dlon1;
	if ((NlLat - 1) > 0)
	{
		Dlon1 = (360/((double)NlLat-1));
	}
	else
		Dlon1 = 360;

	//Calculate XZ the decimal representation of our longitude
	double XZ;
	modHold = 0;
	modHold = Modulus(longitude, Dlon1);
```

```
	modHold = (modHold/Dlon1);
	modHold = modHold * pow(2,17);
	modHold = modHold + .5;
	XZ = floor(modHold);

	//Ensure this fits into our 17 bit space
	long int YZ1 = Modulus(YZ,pow(2,17));
	long int XZ1 = Modulus(XZ,pow(2,17));
	long int LatLon;
	YZ1 = YZ1 << 17;
	LatLon = (YZ1 | XZ1);
	LatLon = (LatLon | 17179869184);
	completeMessageOdd[2] = LatLon;
return 0;
}

int CalculateLatBitsEven()
{
	double lat;
	double longitude;
	cout << "Please enter your requested Latitude: \n";
	cin >> setbase(10) >> lat;
	cout << "Please enter your requested Longitude: \n";
	cin >> setbase(10) >> longitude;
	CalculateLatBitsOdd(lat, longitude);

	//Calculate YZ which will be what is put into our message
	double YZ;
	double modHold;
	int LatHex;
	modHold = Modulus(lat, Dlat0);
	modHold = (modHold/Dlat0);
	modHold = modHold * pow(2,17);
	modHold = modHold + .5;
	YZ = floor(modHold);

	//Calculate Rlatiude for airborne
	long double Rlat0;
	int floorHold;
	Rlat0 = (double)YZ / pow(2,17);
	floorHold = floor(lat/(double)Dlat0);
	Rlat0 = (double)Rlat0 + floorHold;
	Rlat0 = Rlat0 * (double)Dlat0;
	int NlLat = GenerateNlatValue(Rlat0);

	//Calcule DLongitude
	double Dlon0;
	if ((NlLat - 1) > 0)
	{
		Dlon0 = (360/((double)NlLat));
	}
	else
	{
		Dlon0 = 360;
	}
```

```
	//Calculate XZ the decimal representation
	//of our longitude
	double XZ;
	modHold = Modulus(longitude, Dlon0);
	modHold = (modHold/Dlon0);
	modHold = modHold * pow(2,17);
	modHold = modHold + .5;
	XZ = floor(modHold);

	//ensure they will fit into a 17 bit message
	long int YZ1 = Modulus(YZ,pow(2,17));
	long int XZ1 = Modulus(XZ,pow(2,17));
	long int LatLon;
	YZ1 = YZ1 << 17;
	LatLon = (YZ1 | XZ1);
	completeMessageEven[2] = LatLon;

return 0;
}

long int CalculateAltitude()
{
	long int altitude;
	long int hold;
	cout << "Please enter an altitude (0ft - 50,000ft):  \n";
	cin >> setbase(10) >> altitude;
	altitude = (altitude + 1000)/25;
	hold = (altitude & 0x00F);
	altitude = (altitude & 0xFF0) << 1;
	altitude = (altitude | hold); //concatenate to the entire message
	altitude = (altitude | 0x010);
	altitude = (altitude | 0x58000); //Takes on the TC (0x58) field

return altitude;
}


long int GenerateAircraftID()
{
	long int address;
	long int df17;
	cout << "Enter an aircraft ID 3 Bytes (Example: BEEF11): \n";
	cin >> setbase(16);
	cout << setbase(16);
	cin >>  address;
	df17 = 0x8D;
	df17 = df17 << 24;
	df17 = (df17 | address);

return df17;
}
```

```
long int CalculateCRC112BitsOdd()
{
      long poly = 0xFFFA0480;
      long int a = completeMessageOdd[0];
      long int a2 = completeMessageOdd[1];
      long int a3 = completeMessageOdd[2];
      int j;
      long int b = a2;
      long int c = a3;
      long int d;
      long int hold;

      b = b << 12;
      d = (c & 0xFFF000000);
      d = d >> 24;
      a2 = (b | d);
      hold = (a3 & 0x000FFFFFF);
      hold = hold << 8;
      a3 = hold;



      for (j=1; j <= 88; j++)
            {
                  if((a & 0x80000000) != 0)
                  {
                        a = a ^ poly;
                  }
                  a = a << 1;
                  if((a2 & 0x80000000) != 0)
                  {
                        a = a|1;
                  }
                  a2 = a2 << 1;
                  if((a3 & 0x80000000) != 0)
                  {
                        a2 = a2|1;
                  }
                  a3 = a3 << 1;
            }
      completeMessageOdd[3] = a;
return 0;
}

long int CalculateCRC112BitsEven()
{
      long poly = 0xFFFA0480;
      long int a = completeMessageEven[0];
      long int a2 = completeMessageEven[1];
      long int a3 = completeMessageEven[2];
      int j;
      long int b = a2;
      long int c = a3;
      long int d;
      long int hold;
```

```
	b = b << 12; //Bit manipulation to push the message together
	d = (c & 0xFFF000000);
	d = d >> 24;
	a2 = (b | d);
	hold = (a3 & 0x000FFFFFF);
	hold = hold << 8;
	a3 = hold;

	for (j=1; j <= 88; j++)
		{
			if((a & 0x80000000) != 0)
			{
				a = a ^ poly;
			}
			a = a << 1;
			if((a2 & 0x80000000) != 0)
			{
				a = a|1;
			}
			a2 = a2 << 1;
			if((a3 & 0x80000000) != 0)
			{
				a2 = a2|1;
			}
			a3 = a3 << 1;
		}
	completeMessageEven[3] = a;
return 0;
}

long int ConvertForHexEditor(long int a, long int b, long int c, long
int d)
{
	long int ACID = a;
	int i = 1;
	int m = 2;
	while (i<=8)
	{
		ACID = (ACID & 0xF0000000);
		if (ACID == 0x00000000)
			buffer[m] = 0x55;
		else if (ACID == 0x10000000)
			buffer[m] = 0x56;
		else if (ACID == 0x20000000)
			buffer[m] = 0x59;
		else if (ACID == 0x30000000)
			buffer[m] = 0x5A;
		else if (ACID == 0x40000000)
			buffer[m] = 0x65;
		else if (ACID == 0x50000000)
			buffer[m] = 0x66;
		else if (ACID == 0x60000000)
			buffer[m] = 0x69;
		else if (ACID == 0x70000000)
```

```
            buffer[m] = 0x6A;
        else if (ACID == 0x80000000)
            buffer[m] = 0x95;
        else if (ACID == 0x90000000)
            buffer[m] = 0x96;
        else if (ACID == 0xA0000000)
            buffer[m] = 0x99;
        else if (ACID == 0xB0000000)
            buffer[m] = 0x9A;
        else if (ACID == 0xC0000000)
            buffer[m] = 0xA5;
        else if (ACID == 0xD0000000)
            buffer[m] = 0xA6;
        else if (ACID == 0xE0000000)
            buffer[m] = 0xA9;
        else if (ACID == 0xF0000000)
            buffer[m] = 0xAA;
        else


        ACID = a;
        ACID = (ACID << (i*4));
        i++;
        m++;
}
cout << " ";
ACID = b;
ACID = (ACID << 12);
i = 4;
while (i<=8)
{
        ACID = (ACID & 0xF0000000);
        if (ACID == 0x00000000)
            buffer[m] = 0x55;
        else if (ACID == 0x10000000)
            buffer[m] = 0x56;
        else if (ACID == 0x20000000)
            buffer[m] = 0x59;
        else if (ACID == 0x30000000)
            buffer[m] = 0x5A;
        else if (ACID == 0x40000000)
            buffer[m] = 0x65;
        else if (ACID == 0x50000000)
            buffer[m] = 0x66;
        else if (ACID == 0x60000000)
            buffer[m] = 0x69;
        else if (ACID == 0x70000000)
            buffer[m] = 0x6A;
        else if (ACID == 0x80000000)
            buffer[m] = 0x95;
        else if (ACID == 0x90000000)
            buffer[m] = 0x96;
        else if (ACID == 0xA0000000)
            buffer[m] = 0x99;
        else if (ACID == 0xB0000000)
```

```
                buffer[m] = 0x9A;
        else if (ACID == 0xC0000000)
                buffer[m] = 0xA5;
        else if (ACID == 0xD0000000)
                buffer[m] = 0xA6;
        else if (ACID == 0xE0000000)
                buffer[m] = 0xA9;
        else if (ACID == 0xF0000000)
                buffer[m] = 0xAA;
        else

        ACID = b;
        ACID = (ACID << (i*4));
        i++;
        m++;
}
cout << " ";

ACID = c;
i = 1;
while (i<=9)
{
        ACID = (ACID & 0xF00000000);
        if (ACID == 0x000000000)
                buffer[m] = 0x55;
        else if (ACID == 0x100000000)
                buffer[m] = 0x56;
        else if (ACID == 0x200000000)
                buffer[m] = 0x59;
        else if (ACID == 0x300000000)
                buffer[m] = 0x5A;
        else if (ACID == 0x400000000)
                buffer[m] = 0x65;
        else if (ACID == 0x500000000)
                buffer[m] = 0x66;
        else if (ACID == 0x600000000)
                buffer[m] = 0x69;
        else if (ACID == 0x700000000)
                buffer[m] = 0x6A;
        else if (ACID == 0x800000000)
                buffer[m] = 0x95;
        else if (ACID == 0x900000000)
                buffer[m] = 0x96;
        else if (ACID == 0xA00000000)
                buffer[m] = 0x99;
        else if (ACID == 0xB00000000)
                buffer[m] = 0x9A;
        else if (ACID == 0xC00000000)
                buffer[m] = 0xA5;
        else if (ACID == 0xD00000000)
                buffer[m] = 0xA6;
        else if (ACID == 0xE00000000)
                buffer[m] = 0xA9;
        else if (ACID == 0xF00000000)
                buffer[m] = 0xAA;
```

```
        else



        ACID = c;
        ACID = (ACID << (i*4));
        i++;
        m++;
}
cout << " ";

ACID = d;
i = 1;

while (i<=6)
{
        ACID = (ACID & 0xF0000000);

        if (ACID == 0x00000000)
                buffer[m] = 0x55;
        else if (ACID == 0x10000000)
                buffer[m] = 0x56;
        else if (ACID == 0x20000000)
                buffer[m] = 0x59;
        else if (ACID == 0x30000000)
                buffer[m] = 0x5A;
        else if (ACID == 0x40000000)
                buffer[m] = 0x65;
        else if (ACID == 0x50000000)
                buffer[m] = 0x66;
        else if (ACID == 0x60000000)
                buffer[m] = 0x69;
        else if (ACID == 0x70000000)
                buffer[m] = 0x6A;
        else if (ACID == 0x80000000)
                buffer[m] = 0x95;
        else if (ACID == 0x90000000)
                buffer[m] = 0x96;
        else if (ACID == 0xA0000000)
                buffer[m] = 0x99;
        else if (ACID == 0xB0000000)
                buffer[m] = 0x9A;
        else if (ACID == 0xC0000000)
                buffer[m] = 0xA5;
        else if (ACID == 0xD0000000)
                buffer[m] = 0xA6;
        else if (ACID == 0xE0000000)
                buffer[m] = 0xA9;
        else if (ACID == 0xF0000000)
                buffer[m] = 0xAA;
        else



        ACID = d;
```

```
            ACID = (ACID << (i*4));
            i++;
            m++;
      }
      cout << "\n";
}

long int GenerateCompleteDF17Message()
{
      long int address;
      long int altitude;
      long int position;
      long int crcBits;


      //Generate Aircraft ID and store in our buffer
      address = GenerateAircraftID();
      completeMessageOdd[0] = address;
      completeMessageEven[0] = address;

      //Generate Altitude and store in our buffer
      altitude = CalculateAltitude();
      completeMessageOdd[1] = altitude;
      completeMessageEven[1] = altitude;

      //Generate the Latitude and Longitude Bits, functions will store
      values in our buffer
      CalculateLatBitsEven();

      //Generate the CRC bits and store them in our buffer
      CalculateCRC112BitsOdd();
      CalculateCRC112BitsEven();


      //Can be used for troubleshooting purposes if you need to see the
      odd message remove comments from code below.
      //cout << setbase(16) << "Odd Message : " <<
      completeMessageOdd[0] << " " << completeMessageOdd[1] << " " <<
      completeMessageOdd[2] << " " <<           //completeMessageOdd[3]
      << "\n";

      //Convert for easy entry into hex file
      ConvertForHexEditor(completeMessageEven[0],completeMessageEven[1]
,completeMessageEven[2],completeMessageEven[3]);
      ofstream myfile;
      myfile.open ("FinalMessage.bin", ios::binary | ios::app);
      myfile.write(buffer, 30);
      myfile.close();
      system("dd if=/dev/zero of=zeroes.bin bs=10 count=10");
      system("cat FinalMessage.bin zeroes.bin > SecondaryMessage.bin");

      //Can be used for troubelshotting purposes if you need to see the
      even message.
      //cout << setbase(16) << "ADS-B Message : " <<
      completeMessageEven[0] << " " << completeMessageEven[1] << " " <<
```

```
        completeMessageEven[2] << " " <<
        //completeMessageEven[3] << "\n";

        ConvertForHexEditor(completeMessageOdd[0],completeMessageOdd[1],
        completeMessageOdd[2],completeMessageOdd[3]);
        myfile.open ("SecondaryMessage.bin", ios::binary | ios::app);
        myfile.write(buffer, 30);
        myfile.close();
        system("cat SecondaryMessage.bin zeroes.bin > FinalMessage.bin");

        //clean up
        system("rm SecondaryMessage.bin");
        system("rm zeroes.bin");
        cout << "\n";
        cout << "The ADS-B Message has been generated and is ready for
        transmission." << "\n";
        return 0;
}




int main()
{
        int choice;
        int exit = 0;
        system("clear");
        cout << "This program will generate a Mode-S Downlink Format 17
        Message, also known\nas an Automatic Dependenet Surveillance
        Broadcast (ADS-B) Message.\n";


        while(exit ==0)
        {
        cout << "Press 1 <ENTER> to begin message generator.\n";
        cin >> choice;
        if (choice == 1)
        {
        printf("#######################################################
        ## \n", GenerateCompleteDF17Message());
        }

        else
        {
        printf("Exiting............\n");
        exit = 1;
        }
        }

        return 0;
}
```

Appendix C

Condition	Transition Latitude		Number of Longitude Zones, NL	
	Degrees (decimal)	32-bit AWB (hexadecimal)		
If |lat| <	10.47047130	07 72 17 54	**Then NL(lat) =**	59
Else if |lat| <	14.82817437	0A 8B 68 08	**Then NL(lat) =**	58
Else if |lat| <	18.18626357	0C EE B8 80	**Then NL(lat) =**	57
Else if |lat| <	21.02939493	0E F4 48 D6	**Then NL(lat) =**	56
Else if |lat| <	23.54504487	10 BE 8E 9F	**Then NL(lat) =**	55
Else if |lat| <	25.82924707	12 5E 12 29	**Then NL(lat) =**	54
Else if |lat| <	27.93898710	13 DE 23 2C	**Then NL(lat) =**	53
Else if |lat| <	29.91135686	15 45 82 48	**Then NL(lat) =**	52
Else if |lat| <	31.77209708	16 97 EF 0B	**Then NL(lat) =**	51
Else if |lat| <	33.53993436	17 D9 C2 8B	**Then NL(lat) =**	50
Else if |lat| <	35.22899598	19 0D 3E 85	**Then NL(lat) =**	49
Else if |lat| <	36.85025108	1A 34 62 2C	**Then NL(lat) =**	48
Else if |lat| <	38.41241892	1B 50 C4 78	**Then NL(lat) =**	47
Else if |lat| <	39.92256684	1C 68 AE 77	**Then NL(lat) =**	46
Else if |lat| <	41.38651832	1D 6E 2F 8C	**Then NL(lat) =**	45
Else if |lat| <	42.80914012	1E 71 2A 88	**Then NL(lat) =**	44
Else if |lat| <	44.19454951	1F 6D 8F 49	**Then NL(lat) =**	43
Else if |lat| <	45.54626723	20 63 71 E6	**Then NL(lat) =**	42
Else if |lat| <	46.86733252	21 53 F0 D1	**Then NL(lat) =**	41
Else if |lat| <	48.16039128	22 3F 84 E9	**Then NL(lat) =**	40
Else if |lat| <	49.42776439	23 26 0C C7	**Then NL(lat) =**	39
Else if |lat| <	50.67150166	24 08 77 22	**Then NL(lat) =**	38
Else if |lat| <	51.89342469	24 E6 E8 E0	**Then NL(lat) =**	37
Else if |lat| <	53.09516153	25 C1 AD DF	**Then NL(lat) =**	36
Else if |lat| <	54.27817472	26 99 0A 48	**Then NL(lat) =**	35
Else if |lat| <	55.44378444	27 6D 3B A2	**Then NL(lat) =**	34
Else if |lat| <	56.59318756	28 3E 79 B3	**Then NL(lat) =**	33
Else if |lat|	57.72747354	29 0C F7 42	**Then NL(lat) =**	31
Else if |lat| <	58.84763776	29 D8 E2 B2	**Then NL(lat) =**	30
Else if |lat| <	59.95459277	2A A2 64 89	**Then NL(lat) =**	30
Else if |lat| <	61.04917774	2B 69 A9 E5	**Then NL(lat) =**	29
Else if |lat| <	62.13216659	2C 2E D0 D5	**Then NL(lat) =**	28
Else if |lat| <	63.20427479	2C F1 FC B2	**Then NL(lat) =**	27

Condition	Transition Latitude		Number of Longitude Zones, NL	
	Degrees (decimal)	32-bit AWB (hexadecimal)		
Else if |lat| <	64.26616523	2D B2 4C 60	Then NL(lat) =	26
Else if |lat| <	65.31845310	2E 72 DC 8C	Then NL(lat) =	25
Else if |lat| <	66.36171008	2F 30 C7 D8	Then NL(lat) =	24
Else if |lat| <	67.39646774	2F ED 27 0C	Then NL(lat) =	23
Else if |lat| <	68.42322022	30 A8 11 2E	Then NL(lat) =	22
Else if |lat| <	69.44242631	31 61 9B A1	Then NL(lat) =	21
Else if |lat| <	70.45451075	32 19 DA 2E	Then NL(lat) =	20
Else if |lat| <	71.45986473	32 D0 DF 12	Then NL(lat) =	19
Else if |lat| <	72.45884545	33 86 BA F3	Then NL(lat) =	18
Else if |lat| <	73.45177442	34 3B 7C CB	Then NL(lat) =	17
Else if |lat| <	74.43893416	34 EF 31 C5	Then NL(lat) =	16
Else if |lat| <	75.42056257	35 A1 E4 F8	Then NL(lat) =	15
Else if |lat| <	76.39684391	36 53 9E FA	Then NL(lat) =	14
Else if |lat| <	77.36789461	37 04 65 88	Then NL(lat) =	13
Else if |lat| <	78.33374083	37 B4 39 EB	Then NL(lat) =	12
Else if |lat| <	79.29428225	38 63 15 64	Then NL(lat) =	11
Else if |lat| <	80.24923213	39 10 ED 48	Then NL(lat) =	10
Else if |lat| <	81.19801349	39 BD A5 B2	Then NL(lat) =	9
Else if |lat| <	82.13956981	3A 69 0D 67	Then NL(lat) =	8
Else if |lat| <	83.07199445	3B 12 CB 8A	Then NL(lat) =	7
Else if |lat| <	83.99173563	3B BA 3A 96	Then NL(lat) =	6
Else if |lat| <	84.89166191	3C 5E 0E 81	Then NL(lat) =	5
Else if |lat| <	85.75541621	3C FB 4C 0F	Then NL(lat) =	4
Else if |lat| <	86.53536998	3D 89 48 8A	Then NL(lat) =	3
Else if |lat| <	87.00000000	3D DD DD DE	Then NL(lat) =	2
Else			NL(lat) =	1

Bibliography

1. Gorman, S., Dreazen, J. Y., & Cole, A. (2009). "Insurgents Hack U.S. drones: $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected." *Wall Street Journal*, A1.

2. McCallie, L. D., Butts, J., Mills, R. (2011). Exploring Potential ADS-B Vulnerabilities in the FAA's NextGen Air Transportation System. Retrieved from Defense Technical Information Center database.

3. Smith, D. (2011). *Has compulsory ADS-B for Australia been properly thought out?* Retrieved February 15, 2011 from http://www.dicksmithflyer.com.au/article_111.php

4. Niles, R. (2006). *China looks at ADS-B.* Retrieved March 12, 2011 from http://www.avweb.com/avwebflash/briefs/191750-1.html

5. Office of the Joint Chiefs of Staff (2006). Joint Publication 3-13: *Information Operations* (February 13, 2006).

6. Marshall, A. (2009). *An Expanded Description of the CPR Algorithm: ADS-B 1090 MOPS, Revision B, Meeting #29.* July 21-24, 2009.

7. Gilbert, G. (1973). *Historical development of the air traffic control system. IEEE Transactions on Communications,* 364-375. Retrieved from IEEE Xplore.

8. Hal Stoen. (2001) VFR Flight. Retrieved February 15, 2012 from http://stoenworks.com/vfr%20flight.html

9. Cohen, B., & Smith, A. (1998). Implementation of a low-cost SSR/ADS-B aircraft receiver decoder (SY-100). Paper presented at the *Digital Avionics Systems Conference, 1998. Proceedings., 17th DASC. the AIAA/IEEE/SAE,2* F44/1-F44/8 vol.2.

10. Livack, G. S., McDaniel, J. I., Battiste, V., & Johnson, W. W. (2000). The Human Element in Automatic Dependent Surveillance-Broadcast Flight Operations. Paper presented at the *Digital Avionics Systems Conferences, 2000. Proceedings. DASC. the 19th, 2* 5D4/1-5D412 vol.2.

11. Dunstone, G. (2010). *ADS-B Introduction/Tutorial* [PowerPoint slides]. Retrieved from http://www.scribd.com/tracon900/d/44649913-ADS-B-Introduction

12. Wolff, C. (2012). *Radar tutorial.* Retrieved February 15, 2012 from http://www.radartutorial.eu/02.basics/rp05.en.html

13. Ferrer, A., Carbonell, A., Perez, T., Larrosa, X. & Gonzalez, D. V. (2012). *Riding the skies.* Retrieved February 8, 2012 from http://surcandoloscielos.es/blog/frequently-asked-questions-ix-el- radar-3parte/

14. Purton, L., Abbass, H., & Alam, S. (2010). Identification of ADS-B System Vulnerabilities and Threats. *Australian Transport Research Forum 2010,* Canberra, Australia.

15. Boci, E. (2009). RF Coverage Analysis Methodology as Applied to ADS-B Design. Paper presented at the *Aerospace Conference, 2009 IEEE,* 1-7.

16. Harrison, M. J. (2006). ADS-X the next gen approach for the next generation air transportation system. Paper presented at the *25th Digital Avionics Systems* (Gorman, J.Y., & Cole, 2009) *Conference, 2006 IEEE/AIAA,* 1-8.

17. Wing-Shih Huang, Narayanan, R. M., & Feinberg, A. (2008). Multiple targets estimation and tracking for ADS-B radar system. Paper presented at the *Digital Avionics Systems Conference, 2008. DASC 2008. IEEE/AIAA 27th,* 3.C.1-1-3.C.1-10.

18. Babbitt, R. (2010). FAA Aerospace Forecast: Fiscal Years 2011-2031. *U.S. Department of Transportation Federal Aviation Administration Aviation Policy and Plans.* Retrieved April 3, 2011 from http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2011-2031/media/2011%20Forecast%20Doc.pdf

19. Federal Aviation Administration, Automatic Dependent Surveillance Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; OMB approval of information collection, 14 CFR Part 91, Federal Register, vol. 75(154), August 11, 2010.

20. Bruno, R., & Dyer, G. (2008). Engineering A US National Automatic Dependent Surveillance - Broadcast (ADS-B) Radio Frequency Solution. Paper presented at the *Digital Communications - Enhanced Surveillance of Aircraft and Vehicles, 2008. TIWDC/ESAV 2008. Tyrrhenian International Workshop on,* 1-6.

21. Boci, E., Sarkani, S., & Mazzuchi, T. A. (2009). Optimizing ADS-B RF coverage. Paper presented at the *Integrated Communications, Navigation and Surveillance Conference, 2009. ICNS '09.* 1-10.

22. United States Congress. *Federal Aviation Act of 1958.* Public Law No. 85-726, 85th Congress, 2nd Session. Washington: GPO, 1958.

23. Rekkas, C., & Rees, M. (2008). Towards ADS-B Implementation in Europe. Paper presented at the *Digital Communications - Enhanced Surveillance of Aircraft and Vehicles, 2008. TIWDC/ESAV 2008. Tyrrhenian International Workshop on,* 1-4.

24. Cedrini, V., Zacchei, M., & Zampognaro, V. (2008). ADS-B 1090ES Implementation: The CRISTAL-MED project. Paper presented at the *Digital Communications - Enhanced Surveillance of Aircraft and Vehicles, 2008. TIWDC/ESAV 2008. Tyrrhenian International Workshop on,* 1-5.

25. Garcia, M. L., Hoffman, J. M., Rowley, J. L., & Stone, D. L. (2007). Test for success: Next generation aircraft identification system RF simulation. Paper presented at the *Integrated Communications, Navigation and Surveillance Conference, 2007. ICNS '07,* 1-10.

26. Valovage, E. M. (2009). A Method to Measure The 1090 MHz Interference Environment. Paper presented at the *Integrated Communications, Navigation and Surveillance Conference, 2009. ICNS '09.* 1-8.

27. Stamper, W. (2005). "Understanding Mode S Technology". *RF Design Magazine,* 18-21.

28. Valovage, E. (2007). Enhanced ADS-B Research. *Aerospace and Electronic Systems Magazine, IEEE, 22*(5), 35-38.

29. Helfrick, A. (2004). *Principles of Avionics* (3rd ed.). Leesburg, VA: Avionics Communication Inc.

30. Bernays, D. J., Thompson, S. D., & Harman, W. H. (2000). Measurements of ADS-B Extended Squitter Performance in the Los Angeles Basin Region. Paper presented at the *Digital Avionics Systems Conferences, 2000. Proceeding DASC the 19th, 2* 7B1/1-7B1/8 vol.2.

31. Harman, W., Gertz, J., & Kaminsky, A. (1998). Techniques for improved reception of 1090 MHz ADS-B signals. Paper presented at the *Digital Avionics Systems Conference, 1998. Proceedings., 17th DASC. the AIAA/IEEE/SAE, , 2* G25/1-G25/9 vol.2.

32. Nichols, R., Bernays, D. J., Spriesterbach, T., & Dongen, V. (2002). Testing of Traffic Information Service Broadcast (TIS-B) and ADS-B at Memphis International Airport. Paper presented at the *Digital Avionics Systems Conference, 2002. Proceedings. the 21st, , 1* 3A2-1-3A2-13 vol.1.

33. Sampigethaya, K., & Poovendran, R. (2011). Security And Privacy Of Future Aircraft Wireless Communications With Off-board Systems. Paper presented at the *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on,* 1-6.

34. Gilbert, T., & Bruno, R. (2009). Surveillance and Broadcast Services - An Effective Nationwide Solution. Paper presented at the *Integrated Communications, Navigation and Surveillance Conference, 2009. ICNS '09.* 1-19.

35. Garcia, M. A., & Bruno, R. (2009). Ensuring Interoperability Between The Surveillance Broadcast Services System And ADS-B Avionics. Paper presented at the *Integrated Communications, Navigation and Surveillance Conference, 2009. ICNS '09.* 1-7.

36. IATA, Air Traffic Surveillance Views and Expectations of Airspace Users, Gongora, M. Retrieved November 20, 2011 from http://legacy.icao.int/nacc/meetings/2007/SURV_SEMI/Day03_IATA_Gongora.pdf, 2007.

37. ITT, U.S. ADS-B Ground Infrastructure Program, Herndon, Virginia, Retrieved October 3, 2011 from (http://events.aaae.org/sites/091001/assets/files/India%20Aviation%20Summit.pdf), 2009.

38. Babbitt, R.J. (2010). FAA announces performance standards for critical NextGen Avionics. *GPS World, Vol 5.*

39. Powell, J. D., Jennings, C., & Holforty, W. (2005). Use Of ADS-B And Perspective Displays To Enhance Airport Capacity. Paper presented at the *Digital Avionics Systems Conference, 2005. DASC 2005. the 24th,1.*pp. 4.D.4-4.1-9 Vol. 1.

40. Hollinger, K. V., Nickum, J. D., Peed, D. T., & Stock, T. M. (2006). Forecasting Aircraft Owner Equipage Responses To Potential FAA Actions. Paper presented at the *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA,* 1-9.

41. Cotton, W. (1973). Formulation of The Air Traffic System As A Management Problem. *Communications, IEEE Transactions on, 21*(5), 375-382.

42. McHale, J. (2010, December 2010). ADS-B In Brings Air Traffic Control Elements to The Cockpit. *Military & Aerospace Electronics,* 14-19.

43. Hall, T., Mackey, A., Nichols, B., Marksteiner, J., & Volpe, J. A. (2008). Prototype ADS-B System In The Midwest: Description And Lessons Learned. Paper presented at the *Integrated Communications, Navigation and Surveillance Conference, 2008. ICNS 2008,* 1-11.

44. Mozdzanowska, A. L., Weibel, R. E., & Hansman, R. J. (2008). Feedback Model of Air Transportation System Change: Implementation Challenges For Aviation Information Systems. *Proceedings of the IEEE, 96*(12), 1976-1991.

45. Raghavan, R. S. (2002). Performance Analysis Of 1090 Mhz Automatic Dependent Surveillance Broadcast (ADS-B) Using OPNET Modeler [ATC]. Paper presented at the *Digital Avionics Systems Conference, 2002. Proceedings. the 21st,1* 3E6-1-3E6-11 vol.1.

46. Smith, A. P., & Mundra, A. D. (2006). Impact Of ADS-B On Controller Workload: Results From Alaska's Capstone Program. Paper presented at the *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA,* 1-9.

47. Holdsworth, R., Lambert, J., & Harle, N. (2001). In-flight Path Planning Replacing Pure Collision Avoidance, Using ADS-B. *Aerospace and Electronic Systems Magazine, IEEE, 16*(2), 27-32.

48. Bernays, D. J., Drumm, A. C., & Shank, E. M. (2002). Validation Techniques for ADS-B Surveillance Data. Paper presented at the *Digital Avionics Systems Conference, 2002. Proceedings. the 21st, , 1* 3E2-1-3E2-9 vol.1.

49. Hicok, D. S., & Lee, D. (1998). Application of ADS-B For Airport Surface Surveillance. Paper presented at the *Digital Avionics Systems Conference, 1998. Proceedings., 17th DASC. the AIAA/IEEE/SAE, 2* F34/1-F34/8 vol.2.

50. Hammer, J., & Elliott, D. (2010). Stochastic Analysis of ADS-B Integrity Requirements. Paper presented at the *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th,* 3.A.2-1-3.A.2-8.

51. Sampigethaya, K., Poovendran, R., & Bushnell, L. (2010). Assessment And Mitigation Of Cyber Exploits In Future Aircraft Surveillance. Paper presented at the *Aerospace Conference, 2010 IEEE,* 1-10.

52. Sitzabee, William E., Stepaniak, Michael J., Feng, Peter, P. Mission Assurance Issues with t Federal Aviation Administration's Policy to Implement GPS Navigational System. Air Force Institute of Technology, Wright-Patterson, AFB, Ohio.

53. Smith, D. (2006). ADS-B Terrorists' Dream. Retrieved September 8, 2011 from http://www.dicksmithflyer.com.au/Terrorists_dream.php

54. Sampigethaya, K., & Poovendran, R. (2010). Visualization & Assessment of ADS-B Security For Green ATM. Paper presented at the *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th,* 3.A.3-1-3.A.3-16.

55. Smith, A., Cassell, R., Breen, T., Hulstrom, R., & Evers, C. (2006). Methods to Provide System-Wide ADS-B Back-Up, Validation And Security. Paper presented at the *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA,* 1-7.

56. Besada, J. A., Garcia, J., De Miguel, G., Casar, J. R., & Gavin, G. (2000). ADS Bias Cancellation Based On Data Fusion With Radar Measurements. Paper presented at the *Information Fusion, 2000. FUSION 2000. Proceedings of the Third International Conference on, , 2* WEC5/23-WEC5/30 vol.2.

57. Zu Feng, & Zhang Xuejun. (2010). An Application Of Fuzzy Mathematics In ADS-B Data Validation. Paper presented at the *Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on, , 3* 882-886.

58. Ettus, M. (2012). *Ettus Research LLC.* Retrieved August 10, 2011 from http://www.ettus.com

59. Lang, J-P. (2011). *GNU Radio Wiki.* Retrieved August 10, 2011 from http://gnuradio.org/redmine/projects/gnuradio/wiki

60. Foster, N. (2012). *GR-AIR-MODES.* Retrieved August 10, 2011 from https://github.com/bistromath/gr-air-modes

61. Cardew, Edward J. (2010). Decoding ADS-B Position. Retrieved August 10, 2011 from http://www.lll.lu/~edward/edward/adsb/DecodingADSBposition.html

62. Heriot-Watt University (2012). Cyclic Redundancy Check Polynomials Tutorial Retrieved January 15, 2012 from http://www.macs.hw.ac.uk/~pjbk/nets/crc/

REPORT DOCUMENTATION PAGE			*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
22-03-2012	Master's Thesis	August 2010 – March 2012

TITLE AND SUBTITLE Exploiting The Automatic Dependent Surveillance-Broadcast System Via False Target Injection	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Magazu III, Domenic, Captain, USAF	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/ENY) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GCO/ENG/12-07
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Intentionally left blank	**10. SPONSOR/MONITOR'S ACRONYM(S)** Fill in
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
A new aircraft surveillance system, Automatic Dependent Surveillance-Broadcast (ADS-B), is being introduced by the Federal Aviation Administration (FAA) with mandated implementation in the United States by the year 2020. The rapid deployment of the system with current test-beds spread across the U.S. leaves very little chance for anyone to test the abilities of the system and more importantly the flaws of the system.

The research conducted within this thesis explores some of the weaknesses of the system to include the relative ease with which false aircraft targets can be injected. As part of a proof of concept, false ADS-B messages were successfully generated using a system comprised of GNU Radio, a Universal Software Radio Peripheral (USRP), and software developed by the author.

The ability to generate, transmit, and insert spoofed ADS-B messages on the display of a commercial ADS-B receiver, identified and exploited a weakness of the ADS-B system. Four demonstrations, conducted within an experimental environment, displayed the potential uses of the system created through this research and its associated impacts.

15. SUBJECT TERMS
ADS-B, FAA, Aircraft Surveillance, NextGen

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert F. Mills, PhD
U	U	U	UU	101	**19b. TELEPHONE NUMBER** *(Include area code)* 937-255-3636 x4527 Robert.mills@wpafb.af.mil

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

Security of ADS-B: State of the Art and Beyond

Martin Strohmeier*, Vincent Lenders+, Ivan Martinovic*
*University of Oxford, United Kingdom
+armasuisse, Switzerland

***Abstract*—Automatic dependent surveillance-broadcast (ADS-B) is the communications protocol currently being rolled out as part of next generation air transportation systems. As the heart of modern air traffic control, it will play an essential role in the protection of two billion passengers per year, besides being crucial to many other interest groups in aviation. The inherent lack of security measures in the ADS-B protocol has long been a topic in both aviation circles as well as the academic community. Due to recently published proof-of-concept attacks, the topic is becoming ever more pressing, especially with the deadline for mandatory implementation in most airspaces fast approaching.**

This survey first summarizes the attacks and problems that have been reported in relation to ADS-B security. Thereafter, we survey both the theoretical and practical efforts which have been conducted previously concerning these issues, including possible countermeasures proposed in the literature. In addition, the survey seeks to go beyond the current state of the art and gives a detailed assessment of security measures which have been developed more generally for related wireless networks such as sensor networks and vehicular ad hoc networks, including a taxonomy of all considered approaches.

***Index Terms*—ADS-B; aviation; security; wireless; privacy; broadcast**

I. Introduction

The world of air traffic control (ATC) is moving from uncooperative and independent (primary surveillance radar, PSR) to cooperative and dependent air traffic surveillance (secondary surveillance radar, SSR). This paradigm shift holds the promise of reducing the total costs deployment and improving the accuracy. However, it is well known in the aviation community that the ATC system, which is currently being rolled out, called *automatic dependent surveillance-broadcast* (ADS-B), has not been developed with security in mind and is susceptible to a number of different radio frequency (RF) attacks. The problem has recently been widely reported in the press and at hacker conventions. Academic researchers, too, proved the ease of exploiting ADS-B with current off-the-shelf hard- and software [1], [2]. The broad news exposure led the International Civil Aviation Organization (ICAO) to put the security of civil aviation on their agenda of the 12th air navigation conference, identifying "cyber security as a high-level impediment to implementation that should be considered as part of the roadmap development process" [3] and creating a task force to help with the future coordination of the efforts of involved stakeholders.

This shows that there is a widespread concern about the topic, created by the fact that ADS-B will be mandatory for all new aircraft in the European airspace by 2015[1] and has already been embraced by many airlines worldwide. EUROCONTROL approximates that already more than 50 percent of the aircraft worldwide are already equipped with ADS-B transponders. Countries such as Australia have already deployed full continental coverage, with ADS-B sensors being the single means of ATC in low population parts of the country [4].

[1]Older aircraft need to be retrofit by 2017. The FAA mandates ADS-B in the US airspace by 2020.

This paper gives an overview about the research that has been done on the security of ADS-B and describes the potential vulnerabilities identified by the community. Since much relevant security research has been conducted in related fields such as wireless sensor networks or general ad hoc networks, we analyze proposed countermeasures from any of these areas that could be adapted for use in ADS-B or whether they are not applicable for reasons inherent to the system. Furthermore, the present work provides a threat catalogue, analysis and vulnerability categorization of the mainly used data link *Mode S*. We focus primarily on the security of ADS-B and not on other air traffic control (sub-) systems, such as GPS. Among other questions, we seek to answer why existing ideas for securing (wireless) networks such as traditional cryptography cannot simply be transferred and used in the protection of systems such as ADS-B.

While there were a number of reasons behind the switch to a modern air traffic management system, cost has consistently been mentioned as one of the most important ones throughout the process; existing radar infrastructures are simply much more expensive to deploy and maintain [5]. ADS-B, on the other hand, provides significant operational enhancements for both airlines and air traffic managers. The increased accuracy and precision improves safety and decreases the likelihood for incidents by a large margin, unless the system's weak security is exploited by malicious in- and outsiders.

The remainder of the survey is organized as follows: Section 2 gives a detailed overview over the security problems concerning ADS-B and a model of the networking environment. Section 3 broadly outlines solutions proposed in previous works on this topic and looks at the sister protocols ADS-C and military versions of ADS-B. Section IV surveys secure broadcast authentication methods to address the problem while Section V reviews approaches to establish secure location verification with ADS-B. Section 6 summarizes and Section 7 concludes the survey.

II. Problem Statement

This chapter defines the problems related to security in ADS-B more thoroughly. First, we give a short overview over the currently used ADS-B protocol and its existing

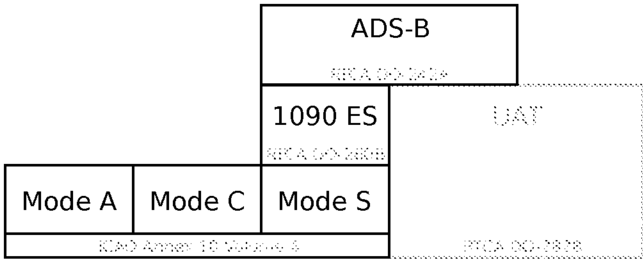


Figure 1. ADS-B hierarchy [1]

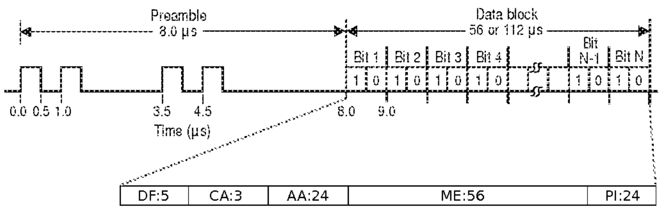


Figure 2. 1090 ES Data Link [1]

vulnerabilities. Building on this, a model of the ADS-B environment is outlined and the required attributes of possible solutions are identified.

A. ADS-B Protocol Overview

The American Federal Aviation Administration (FAA) as well as its European pendant EUROCONTROL named ADS-B as the satellite-based successor of radar. At its introduction, ADS-B has been a completely new paradigm for air-traffic control. Every participant retrieves their own position and velocity by using an onboard GPS receiver. The position is then periodically broadcasted in a message (typically twice per second) by the transmitting subsystem called ADS-B OUT. The messages then are received and processed by ATC stations on the ground as well as nearby aircraft, if equipped with the receiving subsystem ADS-B IN. Messages can integrate further fields such as ID, intent, urgency code, and uncertainty level.

There are two competing ADS-B data link standards that have been proposed: Universal Access Transceiver (UAT) and 1090 MHz Extended Squitter (1090ES). UAT has been created specifically for the use with aviation services such as ADS-B, utilizing the 978MHz frequency with a bandwidth of 1Mbps. Since UAT requires fitting new hardware, as opposed to 1090ES, it is currently only used for general aviation in EUROCONTROL and FAA-mandated airspaces. Commercial aircraft, on the other hand, employ SSR Mode S with Extended Squitter, a combination of ADS-B and traditional Mode S known as 1090ES (see Fig. 1). In other words, the ADS-B function can be integrated into traditional Mode S transponders. From here on, we focus on the commercially used 1090ES data link. The complete overview over the ADS-B protocol can be found in the specification documents [6], [7], [8], various other works give succinct, higher level descriptions of the protocol (e.g. [9], [2], [1]).

The 1090ES Data Link: As the name suggests, the 1090ES data link predominantly uses the 1090MHz frequency for communication sent out by aircraft, to both other aircraft and ground stations (Mode S also uses ground to air communication at 1030MHz for interrogations and information services). Figure 2 provides a graphical view of a 1090ES transmission, which starts off with a preamble of two synchronization pulses. The data block is then transmitted by utilizing pulse position modulation (PPM). With every time slot being 1µs long, a bit is indicated by either sending a 0.5µs pulse in the first half of the slot (1-bit) or in the second half (0-bit). It is important to note that PPM is very sensitive to reflected signals and multipath dispersion as this can play a major role in security and protocol considerations.[2]

There are two different possible message lengths specified in Mode S, 56 bit and 112 bit [6], whereas ADS-B solely uses the longer format. The downlink format field DF (alternatively UF for uplink messages) assigns the type of the message. 1090ES uses a multipurpose format as shown in Fig. 2. When set to 17, it indicates that the message is an extended squitter, enabling the transmission of 56 arbitrary bits in the ME field. The CA field indicates information about the capabilities of the employed transponder, while the 24 bit AA field carries the unique ICAO aircraft address which enables aircraft identification. Finally, the PI-field provides a 24 bit CRC to detect and correct possible transmission errors. It is possible for recipients to correct up to 5 bit errors in 1090ES messages using a fixed generator polynomial of degree 24.

This quick overview shows that only the 56 bit ME field can be used to transmit arbitrary data, i.e. utilized for a secure ADS-B solution. However, not only is it very limited in size but also typically occupied by positional and other data. Thus, the format as currently in practical use is intuitively very limiting to most types of security solutions as we will explain in more detail in this work.

B. Data Link Vulnerabilities

In this section, we discuss the vulnerabilities inherently stemming from the broadcast nature of RF communication when used without additional security measures. Contrary to wired networks, there are no practical obstacles for an attacker trying to access a wireless network such as buildings or security guards, making access control mechanisms very challenging. In [9], McCallie et al. defined a taxonomy for various possible attacks, even though their difficulty estimations have become somewhat dated with the widespread availability of cheap software-defined radios as recently illustrated in [1]. Despite this, the described attacks are ordered in increasing order of difficulty here, providing a comprehensive attacker model.

Eavesdropping: The most straightforward form among the many security vulnerabilities present in ADS-B is the act of listening in to the unsecured broadcast transmissions. This passive attack is called *Aircraft Reconnaissance* in [9]. As ADS-B is using unsecured messages over an inherently

[2]See [10] for more information on PPM and multipath.

broadcast medium, the possibility to eavesdrop is not surprising and has been mentioned since the early stages of development. Many non-adversarial services use this obvious privacy concern, e.g., to visualize air-traffic on the Internet,[3] yet eavesdropping also forms the basis for a number of more sophisticated active attacks. Furthermore, it is not only difficult to stop without full encryption but also is practically impossible to detect. A small number of countries (such as the United Kingdom) have long-standing, very general laws against listening in on unencrypted broadcast traffic which is not intended for the recipient[4] even though the technical realities render such legal approaches all but obsolete.

Jamming: Almost equally simple is the jamming attack, where a single node (both ground stations or aircraft) or an area with multiple participants is effectively disabled from sending/receiving messages by an adversary sending with sufficiently high power on the 1090MHz frequency of Mode S. It has generally also been proven feasible to do reactive jamming in real time, targeting only packets which are already in the air as assessed in [11]. While jamming is a problem common to all wireless communication, the impact is severe in aviation due to the system's inherent wide open spaces which are impossible to control as well as the importance and criticality of the transmitted data.

Message Injection: On the next higher level of difficulty, it is also possible to inject non-legitimate messages into the air-traffic communication system. Since no authentication measures are implemented at the data link layer, there is no hurdle at all for an attacker to build a transmitter that is able to produce correctly modulated and formatted ADS-B messages. See [1] for more details on how to conduct an attack with limited knowledge and very cheap and simple technological means which have been easily and widely available for some time. As another direct consequence of missing authentication schemes, a node can deny having broadcasted any (false) data and/or claim having received conflicting data, making any kind of liability impossible. Concrete attack instances that use message injection include [9]:

- Ground Station Flood Denial
- Aircraft Flood Denial
- Ground Station Target Ghost Inject
- Aircraft Target Ghost Inject

Message Modification: Modifying messages during transmission is typically done via two different approaches, overshadowing and bit-flipping. Overshadowing means that the attacker sends a high-powered signal to replace part or all of the target message. Bit-flipping on the other hand has the attacker superimposing the signal converting any number of bits from 1 to 0 (or the other way around). In both cases arbitrary data can be injected without the knowledge of any of the participants. Message modification can be regarded as even more sinister than the injection of a completely new message, since the manipulated message was originally legitimate. The feasibility of such message manipulation has recently been shown in [12] and [13]. Concrete attack examples are [9]:

- Virtual Aircraft Hijacking
- Virtual Trajectory Modification

Message Deletion: Legitimate messages can be physically "deleted" from the wireless medium by utilizing destructive or constructive interference. Destructive interference means transmitting the inverse of the signal broadcast by a legitimate sender. Due to superposition, the resulting signal should be erased or at least highly attenuated but in practice this approach has very precise and complex timing requirements, making it extremely challenging.

Constructive interference on the other hand does not require synchronization but simply causes a large enough number of bit errors. Since Mode S extended squitters' CRC can correct a maximum of 5 bit errors per message, if a message exceeds this threshold, the receiver will drop it as corrupted. While effectively destroyed, the receiver might at least be able to verify that a message has been sent, depending on the implementation and the circumstances. In any case, it is more subtle than complete jamming of the 1090MHz frequency. Message deletion is key to the following attacks [9]:

- Aircraft Disappearance
- Aircraft Spoofing

C. Identification of System Requirements

There are a number of demands on a security approach for ADS-B, stemming from the way it is needed to work in practical real-world aviation settings and the characteristics of the broadcast approach. We first codify the model and then follow up with an analysis of what we need to have as security primitives in air traffic control systems.

Network Properties:

- The assumed network model consists purely of unidirectional broadcasts. Although there is a growing body of research on Aeronautical Ad hoc Networks (AANETs) that provide multi-hop communication [14], the present real-world implementation is based on **single-hop unidirectional broadcast links**. Aircraft broadcast their position, velocity and direction in plain-text periodically every few hundred milliseconds, a concept called beaconing. Thus, in the following we concentrate mainly on the so-called beacon-based security.
- We **do not consider any type of energy constraints** in association with ADS-B devices.

[3]Prominent examples are flightradar24.com and radarvirtuel.com among many others.

[4]Section 48 of the Wireless Telegraphy Act of 2006 states that (1) "A person commits an offence if, otherwise than under the authority of a designated person— (a) he uses wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of a message (whether sent by means of wireless telegraphy or not) of which neither he nor a person on whose behalf he is acting is an intended recipient, or (b) he discloses information as to the contents, sender or addressee of such a message."

- Furthermore, there are **no significant computational constraints** with neither ground stations nor ADS-B units employed in aircraft.
- **Reliability has not been a major concern** yet, as some lost packets do not normally cause a problem. Indeed, the protocol does have no means to prevent collisions, the sender will not retransmit any packets and no guarantees are given. Loss is dealt with on higher layers. This is also reflected in [1], which shows that the packet error rate tends to hover around a mean of 33 %, independent of the channel. This means that there is some substantial packet loss on the physical layer that is likely to increase when the channel utilization rises over the next decades due to the mandatory ADS-B roll-out. This will be reinforced by the ever-increasing flight traffic,[5] especially in high-density airspaces.
- **The network is ad hoc and highly mobile.** Many nodes are moving at a velocity of up to 1,000 km/h or more. It is therefore extremely dynamic and communication between two nodes may last only a few seconds. Aircraft trajectories are principally not physically restricted, although there are often common routes and also air spaces restricted due to policies do exist.
- **The network is long range**, typically ADS-B is considered to be feasible at distances of 100 NM and more.[6]
- In contrast to other, independently deployed wireless (sensor) networks the **undetected physical capture of legitimate nodes is not the most important concern.** Legally having access to a legitimate ADS-B node, however, is not considered very difficult, at least when taking general aviation into account.

Security Attributes: Perrig and Tygar [16] identify two large themes around which secure broadcast revolves: First, make sure that receivers know that any received information comes from the appropriate sender, and second that senders can freely limit the recipients of broadcasted information. In light of the recently exploited inherent vulnerabilities of the ADS-B system with cheap off-the-shelf hardware [2], [1], this is quickly becoming the most important topic in ADS-B research. Based on the model defined above, any security scheme for ADS-B would have to satisfy the following properties:

- *Data integrity*: Ensures that the data is the same as has been provided by the sender and has not been modified by any third party.
- *Source integrity:* Ensures that a message originates from the participant that claims to have sent it.
- *Data origin authentication*: Ensures that a message originates from the location claimed in a message.
- *Low impact on current operations:* A scheme should be compatible with the current ADS-B installations and not overly affect both hard- and software standards.
- Sufficiently *quick and correct detection* of incidents.

[5]Growth rate forecasts from market analysts suggest a 5.1% increase per year between 2010 and 2030. Cargo traffic is expected to grow even more at 5.6% per year in the same time frame [15].

[6]Aviation typically uses the nautical mile, also abbreviated as nmi, as a distance measure which is 1,852m.

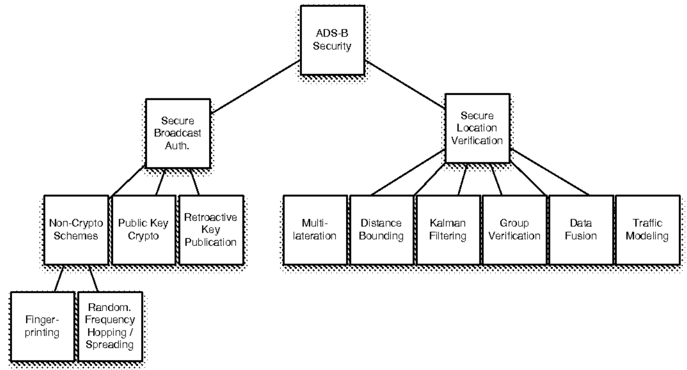


Figure 3. Taxonomy of ADS-B Security

- Needs to be *secure against DoS-attacks* against computing power.
- Any approach *needs to be easily scalable*. This is in respect to both a locally rising aircraft density and globally increasing aircraft traffic. The strain on the heavily used 1030 MHz channel should not measurably increase (e.g. due to an increased number and/or larger packets).
- *Robustness to packet loss.* A jammed wireless channel should decrease neither security nor reliability of the scheme.
- Achieving *non-repudiation* is seen as nice to have but not very high on the priority list for immediate air traffic security and is more of a legal topic.

III. Outlining Solutions

Substantial work has already been done on ADS-B security over the last decade and several approaches have been proposed in the literature to enhance ADS-B security in particular. Furthermore, a large amount of research has been done in related fields such as vehicular ad hoc networks (VANETs) or wireless sensor networks where broadcast authentication and security also play an important role. While some ideas may not be directly applicable to the aforementioned model and requirements of ADS-B, it might be possible to adapt them to the changed use case at hand. If not, besides the advantages and disadvantages of every approach we also list the major obstacles.

The remainder of this section first presents overview works in the community concerned with the security of ADS-B as a whole. We then consider ADS-B's sister protocols ADS-C and military versions of ADS-B in our context before analyzing all collected ideas in detail in the following sections.

As shown in the taxonomy in Fig. 3, we identified two distinct approaches to securing ADS-B: **Secure Broadcast Authentication** and **Secure Location Verification**. Consequently, Section IV examines the various schemes that apply asymmetric properties (cryptographic and non-cryptographic) to directly authenticate broadcast communication while Section V reviews several different methods that seek to verify the authenticity of location claims made by aircraft and other ADS-B participants.

A. Previous Works on ADS-B Security

Securing ADS-B communication was not a very high priority when it was specified to be the new standard in civilian secondary surveillance. Neither the RTCA standards [6], [7], [8] nor other requirements documents [17], [18] mention security in this context. However, security problems in ADS-B have been well-known for a long time, mostly because they are relatively obvious to the interested researcher.[7] For instance, weak ADS-B security has recently got very broad reporting in the mainstream press[8] due to two talks at the DEFCON and Black Hat security conferences.[9]

Sampigethaya and Poovendran [19], [20] first analyse the security and privacy of ADS-B and other related and unrelated communication systems which are part of the so-called "e-enabled aircraft". McCallie et al. [9] provide a current security analysis, focused on the nature of possible attacks and their difficulty. They give a systematic high-level overview and propose general recommendations for addressing ADS-B's problems. Costin and Francillon [2] as well as Schaefer et al. [1] analysed ADS-B security, too, focusing on the ease of exploiting ADS-B with current hard- and software and offering some possible countermeasures.

Kovell et al. [21] mention data fusion with other systems, multilateration and various cryptographic schemes as state of the art research on ADS-B security. They further conduct a more thorough analysis on Kalman filtering and group validation concepts and proposed mitigation methods. Nuseibeh et al. conduct an example of a formal security requirements analysis of ADS-B [22], proposing multilateration to deal with possible attack scenarios. Burbank et al. [23] present general concepts for communications networking to meet the requirements of future airspace systems, i.e. a vision of a mobile ad hoc and wireless networking concept for use in both the terminal area and in the en-route airspace. Li and Kamal [24] analysed the security of the whole FAA's Next Generation Air Transportation System (NextGen) of which ADS-B is a core component.[10] They develop a high-level defense-in-depth framework for analyzing NextGen and mention general secure communication approaches such as encryption, authentication and spread spectrum as part of the ADS-B security layer.

B. ADS-C

A theoretical, currently already available, way to deal with suspicious ADS-B participants would be to ask them to switch to the connection-oriented ADS-C (ADS-Contract, also known as ADS-Addressed). However, ADS-C also has a number of very severe inherent shortcomings, some of which are described by the ICAO: [26]

- It requires the installation of additional avionics (for data communications): FANS 1/A or ATN.
- Performance may be determined by the limitations of the communications media.
- A cost may be associated with the transmission of each report since the data is carried by a data link service provider:
- It does not support ASA because the messages are not directly available to other aircraft.

Overall, the current implementation of ADS-C over the outdated ACARS network[11] considerably limits its usefulness. It is also violating the basic assumptions of ADS-B, being a system that sends on demand instead of periodically broadcasting without being requested, which is why it is not considered any further.

C. Communication in Military Avionics

There is undoubtedly a much stronger need and motivation to implement stringent security in a military communications context. Though it is not the primary focus of this work, anything in practical use by military forces could naturally be of interest for civil security solutions as well. There are various standards currently in use by the US and NATO military, among them the cryptographically secured Mode 4 and Mode 5 as defined in the STANAG 4193 specification. Mode 4, which employs a 3-pulse reply to a challenge, has been in use for decades and according to the forecasts of the NATO Minimum Military Requirements is to be superseded by Mode 5 in 2015 (initial operational capability) and 2020 (full operational capability), respectively [27].

While the legacy Mode 4 indeed only allows airplanes to respond to challenges, Mode 5 adopts the ADS-B broadcast capability, so participants can announce their presence without a prior query, very useful in identification, friend or foe (IFF) [28]. On the security side, Mode 5 uses proprietary hardware and encryption algorithms with a black key concept;[12] it furthermore offers time-of-day authentication, automatic switchovers and a longer period [29]. The signal modulation is done via spread spectrum and operation requires a platform identification number (PIN). Mode 5 hardware is equipped with a unique identifier that informs about national origin and the platform number. Mode 5 has two different levels: Level 1 is the interrogation response mode, providing time, position and identification based on both GPS and traditional means. Level 2 is the broadcast mode and entirely based on GPS. There are currently no further available details on the security mechanisms, including the applied cryptography, of Mode 4 and 5 since this information is classified.

The ADS-B specification itself also mentions the message types/downlink formats Military Extended Squitter (DF19) as well as Military Use Only (DF22) without detailing them further, although it is known for example that DF19 makes ample use of bursts instead of regular beacon messages only [30].

[7] Especially on the Internet broad warnings have been floating around as early as 1999, e.g. http://www.airsport-corp.com/adsb2.htm, http://www.dicksmithflyer.com.au/cat_index_36.php

[8] E.g. http://www.forbes.com/sites/andygreenberg/2012/07/25/next-gen-air-traffic-control-vulnerable-to-hackers-spoofing-planes-out-of-thin-air/

[9] http://www.blackhat.com/usa/bh-us-12-briefings.html#Costin

[10] Although certainly not the only safety-critical wireless module. See e.g. [25] for concerns about the impact of GPS integrity on aviation safety.

[11] The Aircraft Communications Addressing and Reporting System (ACARS) will be superseded by the Aeronautical Telecommunications Network (ATN) and IP communication over the next decade.

[12] Black keys are safe to transmit since they are encrypted with a key encryption key. Red keys on the other hand are unencrypted and classified as highly sensitive.

Format #	DF					Military Extended Squitter
19	1 0011	AF : 3	Military Application : 104			

Figure 4. DF19 data format [30]

IV. Secure Broadcast Authentication

Secure Broadcast Authentication is one possible means to prevent and/or detect attacks in a unidirectional broadcast network such as ADS-B. This section will describe the various methods that have been proposed in the literature, typically for wireless sensor networks or VANETs and analyse their applicability to ADS-B.

Authentication of messages on a broadcast medium is hard, compared to point-to-point communication. A symmetric property is only useful in point-to-point authentication where both parties trust each other. Thus, an asymmetric mechanism is inherently required so that receivers can *verify* messages but are not able to *generate* authentic messages themselves [31]. For a good overview over secure broadcast communication in general, the reader is referred to [16].

The goal is to keep the open nature of ADS-B intact while offering a potential authentication mechanism. This could be done either globally or only selectively in cases where suspicious behaviour has been detected. Such reactive authentication could lessen the strain on the network by only requiring additional security (and thus computational and communicational overhead) at times when incidents seem more likely.

Furthermore, there is a distinction between broadcast schemes that are user-based vs. those that are node-based, or possibly both. Node-based (also known as host-based) schemes ensure the authenticity of a given node, i.e. the hardware. User-based schemes on the other hand look to authenticate a human user, regardless of the underlying hardware [32]. This work focuses mainly on node-based schemes.

A. Non-Cryptographic Schemes on the Physical Layer

Non-cryptographic schemes such as fingerprinting comprise various methods for wireless user authentication and device identification techniques, either based on hardware or software imperfections or characteristics of the wireless channel which are hard to replicate. The goal is to identify suspicious activity in a network. Finding a signature for legitimate beacons in a network, possibly being able to tell apart ground stations from aircraft, identifying the type of aircraft or even individual machines provides data useful for the development of an intrusion detection system [33]. If there are tangible differences between legitimate and non-legitimate packets on the physical layer, then machine learning techniques could be employed to develop a model for predictions of normal behaviour and also statistical thresholds beyond which an activity is considered suspicious. Even if it is only feasible to identify classes of devices instead of singular participants, this could prove to be valuable information in detecting intruders. Yet, fingerprinting does not provide surefire security in any way, and various attacks and concerns have been brought forward [34].

Currently, there have been no attempts at applying any kind of non-cryptographic schemes to boost the security of ADS-B. A common counter-argument has been the fact that contrary to e.g. the 802.11 markets the commercial airplane market is divided into two big players (Boeing and Airbus) which in the long run makes significant differences at least between ADS-B vendors unlikely. Still, fingerprinting has also been successfully employed to tell apart the exact same models from the same vendor. For a good overview of the state of the art in physical-layer identification of wireless devices, see [33].

Zeng et al. [35] broadly identified three different techniques that can be employed to enhance or even replace traditional cryptographic measures: Software, hardware and channel-based fingerprinting.

a) Software-Based Fingerprinting: This type of fingerprinting techniques tries to exploit distinctly different patterns or behaviour of software operating on wireless equipment. Depending on the specification of a protocol, there is a lot of leeway for manufacturers and developers when implementing software on a given device. If there is enough entropy in information about the combination of chip sets, firmware, drivers to tell apart different wireless users, this approach can be used to verify their continuity up to a certain degree. As a downside, it seems likely that large fleets of airline operators are fitted with very similar or same hardware, making them harder or even impossible to differentiate and on the other hand easier to study and copy for a potential attacker.

b) Hardware-Based Fingerprinting: A number of techniques have been proposed to identify devices based on unique hardware differences. Some of these differences can be used for *radiometric fingerprinting*, exploiting differences in the turn-on/off transient or the modulation of a radio signal to build unique signatures. While this works well for non-mobile cases and attackers with standard, off-the-shelf hardware, it can break down against more powerful adversaries employing software defined radios and be subjected to signal/feature replay attacks [33]. Furthermore, the existing research captured signals very closely to the fingerprinting antenna (15m or less) and in non-mobile settings, making it very improbable to work in the highly-dynamic, large-distance ADS-B setting.

Another unique hardware feature amongst wireless devices is *clock skew*. As no two clocks run precisely the same, this can be used to create signatures and enable identification. Unfortunately, to exploit this, we would require timestamps included in ADS-B messages. Also, it is possible for an attacker to eavesdrop on the communication and mimic the appropriate clock skew [36].

Recently reviewed options for future systems include the use of so-called physically unclonable functions (PUFs), which essentially exploit specifically implemented circuits to create unique and secure signatures, thus abandoning the scope of non-cryptographic solutions.[13] Furthermore, besides

[13] For a good overview on PUFs, see [37]

requiring new hardware, this approach also necessitates an overhauled messaging protocol, including a challenge and response model [38], making it a difficult fit for the requirements of the ADS-B protocol.

c) Channel/Location-Based Fingerprinting: Exploiting natural characteristics of the physical layer has been a hot research topic in relation with security in wireless networks. Various approaches have shown that this can be a viable alternative to more traditional authentication and verification measures, typically based on received signal strength (RSS, e.g. [39]), channel impulse response (CIR, e.g. [40]) or the carrier phase (e.g. [41]). They are comparably easy to implement in wireless systems and can offer reasonable security without requiring much overhead.

Any such concept requires bidirectional communication, however. One practical example is the retroactive authentication of data packets via an RSS list as proposed by Zeng et al. in [35]. As this temporal RSS variation authentication (TRVA) requires an ACK packet in a given coherence time, it is not compatible with current ADS-B protocols. Furthermore, it is doubtful if this could work with reasonable efficiency in a highly dynamic environment such as airborne MANETs. The coherence time T_C in which the channel stays stable in a wireless network where only one sender moves at 800km/h is roughly 0.6188ms. At a 1090ES bandwidth of 1 symbol/μs it is obvious that such protocols are impossible to deploy. This physical property also effectively denies the application of many other more sophisticated physical-layer schemes such as SecureAngle [42], which aims at securing wireless networks by using multiple antennas capturing the angle of arrival information of nodes to built signatures and detect anomalies. Similarly, practical indoor location-based geo-tags, built with surrounding radio frequency signals such as done in [43] are not applicable.[14]

Laurendeau and Barbeau [44], [45] exploit RSS similar to time difference of arrival concepts (see V-A) to localize malicious insiders in a vehicular ad hoc network with the help of various receivers. Taking into account that an attacker will not be inclined to cooperate and can even actively fake the signal strength he utilizes, their proposition enables the receivers of a message to at least identify a given area where it must have originated from.

d) Randomized/Uncoordinated Frequency Hopping / Spreading: A physical-layer scheme different from fingerprinting, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are both used in wireless systems to improve protection against malicious narrow band and pulse jamming as well as eavesdropping. In their usual form they both require a pre-shared spreading code or hopping pattern between sender and receiver which makes it hard to follow or hinder the communication for anyone without access to the code/pattern. This is also exploited in military

[14]Although one advantage is that many legacy Mode S systems use several directional rotating antennas to pick up ADS-B signals. The extracted information about the angle-of-arrival could conceivably be used to raise red flags, as described in Section V-F.

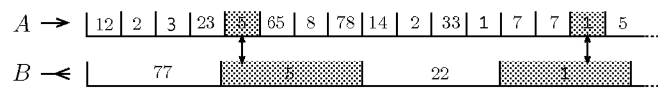


Figure 5. Uncoordinated Frequency Hopping after [46]. Both A and B regularly change their communication frequencies without having pre-established a common pattern. By statistical chance they will communicate on the same channel every so often.

communications (see Section III-C) but is not a viable option for world-wide civil and commercial ATC where such secret codes would presumably not stay secret for long.

The need for a pre-established code can be relinquished by employing random, uncoordinated versions of FHSS and DSSS. Strasser et al. [46] propose such a physical layer approach to counteract jamming in wireless broadcast scenarios. Uncoordinated Frequency Hopping (UFH) provides a viable way to broadcast initial messages without an attacker being able to jam the transmission in an efficient way. The key insight to these approaches is that, contrary to normal frequency hopping mechanisms, sender and receiver(s) rely on the statistical chance to be on the same channel at the same time. The obvious downside of UFH is its low bandwidth due to the fact that many times receivers will not listen on the correct channel. More concretely, the probability with UFH that a packet will be received at a node without an attacker being involved is $p_m \geq 1 - (1 - \frac{c_s}{c})^{c_r}$ (c being the number of possible channels, c_s and c_r the number of channels a sender/receiver is using simultaneously).

Based on the same principle are Uncoordinated Direct-Sequence Spread Spectrum (UDSSS) [47] and Randomized Differential DSSS [48]. Both these techniques rely on the statistical chance that spread codes randomly chosen by sender and receiver(s) will happen to be the same every so often.

While the proposed methods can effectively defeat jamming and modification attacks, the inherently lower performance and a prolonged transmission time make them difficult to use in a large-scale system such as ADS-B. Furthermore, authentication and security against replay attacks is only achieved by adding a private/public key infrastructure and timestamps, respectively.

B. Public Key Cryptography

Cryptographic measures have been a tried and tested means to secure communication in wireless networks and must subsequently also be considered in the ADS-B setting. One question to examine is if the current implementation of ADS-B can be encrypted. The first possibility would be to distribute the same encryption keys to all ADS-B participants worldwide, or at least to aircraft and ground stations in a given area. Such a vast group encryption scheme, including even general aviation, would be considered extremely insecure to both inside and outside attacks. This inherent weakness is non-fixable even with very frequent key updates (which also would again increase the complexity of the encryption deployment). In short, such a scheme would fulfill none of the required criteria listed in Section II-C. Finke et al. [49] examine various encryption schemes, including the possibility to do the key management for symmetric encryption out of band, for example through the controller-pilot data link communication (CPDLC) which they consider worth exploring further. The authors also give an analysis of the security and practicability of asymmetric, symmetric and format preserving encryption. In their conclusion, they support a symmetric cipher using the FFX algorithm which can encrypt non-standard block sizes (i.e. ADS-B's 112 bit messages) with sufficient entropy. However, the difficulties concerning key management and distribution are widely acknowledged.

As mentioned before, if broadcast authentication is needed, one requires an asymmetric property, a characteristic fulfilled by public key cryptography. Samuelson and Valovage [50] report on an implementation of authentication and encryption in UAT using a public key infrastructure (PKI). Their method uses a hash to create a message authentication code (MAC) that can be used to authenticate the message and can be extended to full encryption but no further details are publicly available. There are related patents filed under the names "Secure ADS-B Authentication System and Method" [51] and "Automatic Dependent Surveillance System Secure ADS-S" [52] by Sensis Corporation.[15] The general idea is to use a challenge/response format with an authenticator ground station, who authenticates every participant in its reach and notifies a higher authority and/or all other participants of any failed authentication. This concept requires the station to have access to a worldwide database of secure keys that is both hard to maintain globally as well as subject to possible security breaches. if this is the case, the system can be used to not only identify ADS-B participants but also pilots and various other people/systems taking part in the flight process. Furthermore, ADS-S includes a changed modulation and complete overhaul of the messaging system, making it incompatible with ADS-B and as such very costly and extremely doubtful to be deployed widely in the future.

Costin et al. [2] suggest a "lightweight" PKI solution which essentially amounts to a retroactive part publication of the key as discussed in Section IV-C: Aircraft A transmits the signature distributed over a number N of ADS-B messages, so that after every N messages the surrounding participants have received A's signature. The recipients keep the messages until the full signature has been transmitted, at which point they can authenticate the buffered messages. The authors suggest that the PKI key distribution necessary for this scheme could be done during an aircraft's regular check-ups.

Ziliang et al. [53] present a concrete PKI solution for data authentication in ADS-B/UAT based on Elliptic Curve Cipher and X.509 certificates. The authors try to tackle a number of problems involved with cryptography such as key size length and keeping the broadcast nature of ADS-B. UAT offers much longer messages than 1090ES, with payloads of 16 or 32 bytes when transmitted from aircraft and even 464 bytes in ground message bursts [54]. Yet, their conclusion is that the data block format needs to be changed, no matter which type of cryptography is used. Consequently, they propose and implement their authentication scheme with a slightly changed UAT message type. In 1090ES, this scheme would require not only using the DF24 Extended Length Messages available in the Mode S standard but still need 5 messages to divide and accommodate the signature data and timestamps, a solution that hardly looks scalable in an already crowded frequency. On top of this, the description leaves very much open the question of an efficient certificate distribution scheme.

[15]Now owned by defense contractor Saab AB.

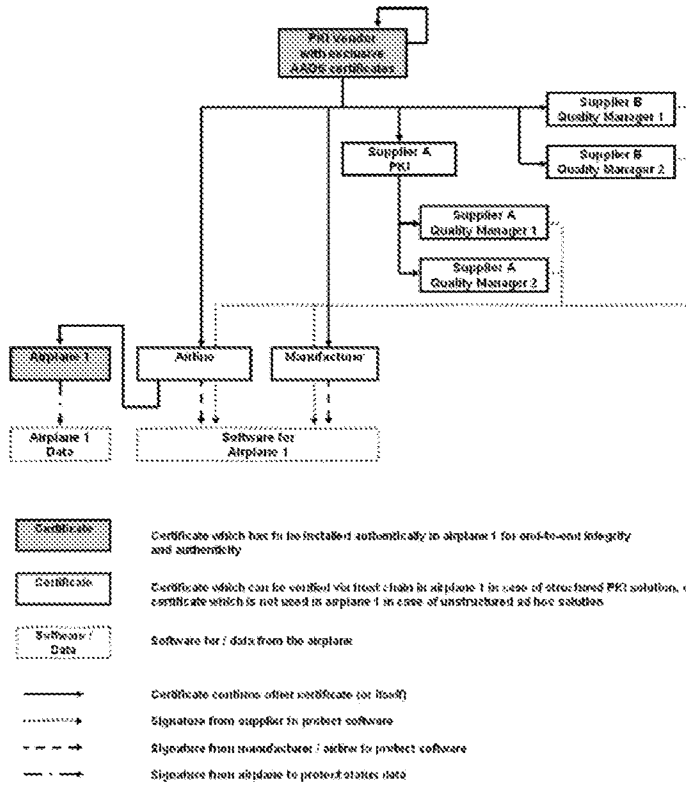


Figure 6. Outline of a public key infrastructure from [57]. A PKI vendor supplies airlines, manufacturers and external suppliers with the required certificates.

Raya and Hubaux [55], [56] discuss using Public Key Cryptography in VANETs. In short-range scenarios with beacons sent every 100-300ms and up to 120 mobile nodes in a 300m communication range, they calculated with message sizes from 294 to 791 bytes (depending on the system) and found the performance to be acceptable in simulations.

Robinson et al. [57] analyse various different solutions to create PKI infrastructures for a general airplane assets distribution system (AADS). Although, the work is not discussing the ADS-B protocol but instead focusing on the distribution of software and data on the ground, the authors identify the airline industry's needs and requirements from a PKI infrastructure, and it seems plausible that the same system could be used to secure air traffic control data. According to their analysis, an ad hoc approach employing pre-loaded trust certificates and without a central authority could be used as a short-term solution until a more structured, long-term public key infrastructure has been developed (see Fig 6 for an outline of their proposal).

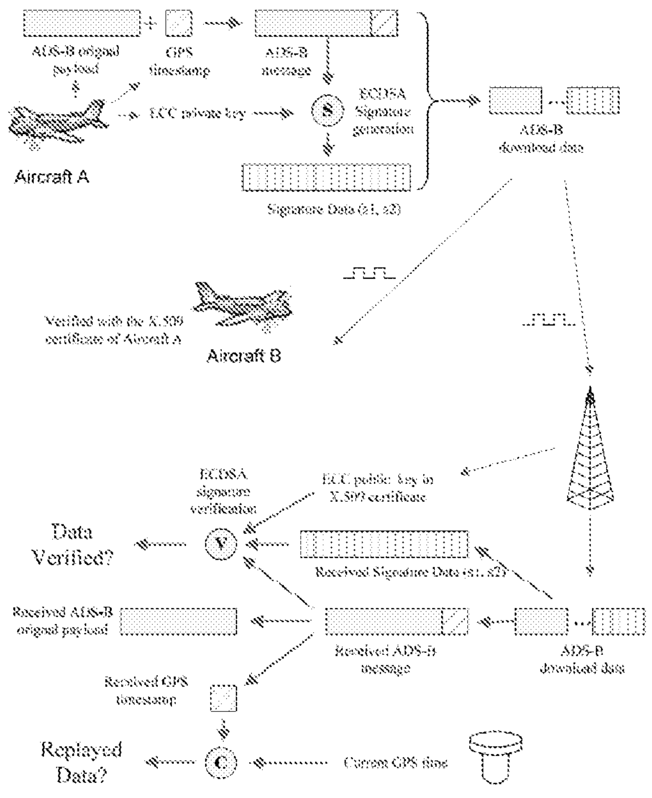


Figure 7. Example of a typical encryption scheme adapted for ADS-B from [53]. It employs elliptic curve cryptography to generate signatures which can be verified with the responding certificate by other aircraft and ground stations. An additional GPS timestamp prevents replay attacks.

The obvious idea for a centralised key distribution would be to have aviation authorities such as the FAA act as a certificate authority (CA). But assuming the role of a CA is no easy task, even many specialized institutions had to report numerous security breaches over the last decades. Furthermore, if this problem is sufficiently solved, there remains the question of how aircraft from airspaces mandated by different authorities can securely communicate with each other. These challenges are somewhat analog to the same approach in vehicular networks as discussed in [58] but arguable even worse due to the large internationalization of the ADS-B network.

There are certain natural disadvantages to using an encryption solution that cannot be overcome (or only with great difficulty) as mentioned in [59]:

- Despite the encryption of data frames, management and control frames are not protected.
- It immediately and unmitigatably breaks compatibility with the installed base.
- Key exchange is notoriously difficult in ad hoc networks, which are by definition without a centralized institution. They are often too dynamic, requiring constant adaptation. This would result in too much overhead in both the number as well as the size of messages.
- The open nature of ADS-B is widely seen as a feature. A cryptographic system implemented in a way comparable to ADS-S does not offer public broadcast communication.
- One-time signatures even using advanced techniques such as Merkle-Winternitz prove infeasible due to their overhead of 80 bytes and more, simply to sign 60 bits [31].

To conclude this section, it is generally difficult to build any kind of encryption scheme with the currently accepted 1090ES data link. Approaches have been shown to be theoretically possible with the higher bandwidth UAT, although practical proof of scalability and practicability have not been given yet. Furthermore, at this point in time it does not seem likely that UAT will play a role apart from general aviation in the FAA-mandated airspace. So, while UAT offers more technical possibilities not only for security and encryption, and even combined UAT/1090ES transmitters are neither a technical nor a regulatory problem,[16] traditional cryptography in conjunction with the current installment of ADS-B does not seem like a worthwhile route for further research at the present.

C. Retroactive Key Publication

A variation on traditional asymmetric cryptography is the technique of having senders retroactively publishing their keys which are then used by receivers to authenticate the broadcast messages. This approach that has been proposed for use in various fields [60], [16]. The key concept is simple: Any broadcasting entity produces an encrypted message authentication code (MAC) which is then sent along with every message. After a set amount of time or messages, the key to decrypt this MAC is published. All listening receivers, who have buffered the previous messages, can now decrypt the messages and ensure the continuity of the sender over time.

The TESLA (Timed Efficient Stream Loss-Tolerant Authentication) protocol [61], standardized in RFC 4082,[17] can provide efficient broadcast authentication on a large scale, while being able to cope with packet loss and real-time applications. The µTESLA broadcast authentication protocol is the adaptation of TESLA for wireless sensor networks [62].

Both TESLA and µTESLA use one-way key chains as shown in Fig. 8: The broadcaster chooses a random key K_n and applies a public pseudo-random function F as often as required to acquire the keys: $K_i = F(K_{i+1}),\ 0 \leq i \leq n-1$. Subsequently, every secret $K_i, i > 0$ is used for sending in the i-th interval and disclosed to the public after a number of time intervals d. As every previous key K_i with $i < j$ can be recovered by the receiver(s) by applying the one-way function F, the receiver needs to do two things to authenticate a message: [48]

1) Authenticate the key K_i against previously received keys to ensure they are from the same key chain.

[16] "There is nothing in the regulations and there are no technical hurdles that would prevent a manufacturer from building a combination UAT/1090ES box, one that would eliminate the different-technology blind spots while allowing high-flying aircraft the ability to get FIS-B through UAT." http://www.flyingmag.com/technique/proficiency/ins-and-outs-ads-b

[17] "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", http://www.ietf.org/rfc/rfc4082.txt

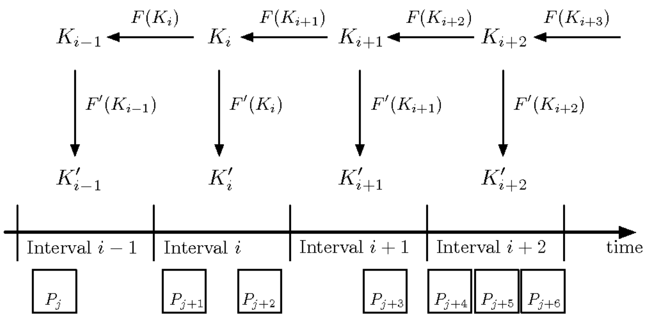


Figure 8. The Figure illustrates TESLA's utilization of one-way chains after [61]. The first one-way function F generates the chain, following that the second one-way function F' derives the MAC keys. Time is divided into separate intervals i, all having the same length. The packets P_j are each sent during one specific interval. For every such packet, the sender computes a MAC with the key that is in accordance with that interval. E.g. P_{j+2}'s MAC is calculated based on its data and key K'_i. Disclosing the keys of previous intervals can be done either by attaching the key to sent packets or in separate messages.

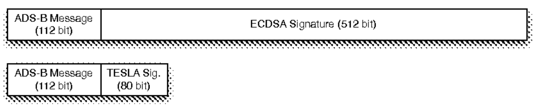


Figure 9. TESLA signatures vs. ECDSA signatures. Tesla signatures cost significantly less overhead compared to many other cryptographic solutions.

2) Ensure that the message with key K_i could only have been sent before the key has been published (requiring loose time synchronization), i.e. before interval $i + d$.

The fact that µTESLA uses symmetric cryptography in connection with time as its asymmetric property makes it an interesting idea for adaptation to ADS-B since sufficiently good time synchronization could be provided via GPS (this would require sending the GPS timestamps in a new protocol field since this is not currently the case). The advantages of µTESLA are obvious: ADS-B keeps its open and broadcast nature and a complex PKI infrastructure is not required to ensure a sender's continuity, although it could be added if identification and source integrity are required (e.g. solely for well-connected ground stations). Nonetheless, it enables a participant to protect itself against impersonation attacks. In areas well-served by ground stations any break in continuity detected by any single one of them would immediately set off red flags.

Another advantage of µTESLA is that lost packets on the notoriously jammed 1090 MHz frequency (there is no medium access control in place) are not an integral problem for authentication. Furthermore, the overhead for communication as well as required modifications to the ADS-B protocol are significantly less than with traditional asymmetric cryptographic methods.[18]

On the other hand, µTESLA also has some disadvantages when applying it to AANETs. There is a need to reinitialize it (if used for identification) and it can be susceptible to memory-based DoS (depending on the setup of the receiver). To counter this, Eldefrawy et al. [63] propose an approach that utilizes forward hashing using two different nested hashes and the Chinese Reminder Theorem, resulting in a system that does not need to be reinitialized.

Haas and Yu [64] compare TESLA and ECDSA-based authentication by simulating their performance in a real-world VANET scenario (although not including certificate distribution). Regarding channel congestion and MAC layer delay they found that the TESLA protocol with keys attached to a following broadcasts performed significantly better than ECDSA or a TESLA-scheme that publishes keys in separate packets.

Hu and Laberteaux [65] discuss a combination of a full-blown PKI infrastructure with CAs distributing 512 bit signatures to bootstrap 80 bit TESLA signatures for short-term authentication in VANETs. Such a system offers comparably lightweight integrity and possibly on-demand authentication, if needed and requested.

V. Secure Location Verification

Besides securing the communication - and thus the location data - of ADS-B, there are other approaches to ensure the integrity of air traffic management. The general idea of secure location verification is to double check the authenticity of location claims made by aircraft and other ADS-B participants. This is inherently different to the verification of the broadcast sources and messages. The baseline is to establish means to find the precise location of a sender, effectively offering some redundancy and thus the ability to double check any claims made. As an additional advantage any such approach creates more location data, which can be merged with ADS-B and radar and offer a back-up system in case of failure of these primary navigation systems or GPS.

A. Multilateration

Multilateration, or hyperbolic positioning, is a popular form of *Co-operative Independent Surveillance* and has been successfully employed for decades in military and civil applications. If the precise distance between three known locations and an unidentified location can be established, it is a purely geometric task to find the unknown point. We can, for example, use the received ADS-B signals which travel at the speed of light to estimate the distance. Since we do not know the absolute time a message needed to travel from an airplane to a receiver, we have to employ the time difference of arrival (TDOA) .[19]

Thus, multilateration requires a number of antennas in different locations that receive the same signal at different times. From the TDOA, hyperboloids can be calculated on which the aircraft's position must lie. With four or more measured antennas a 3D position can be estimated by finding the intersection of the hyperbolas.

[18] The original µTESLA requires a 6 byte MAC.

[19] For a full explanation of the multilateration process in aviation see e.g. [66] or [67].

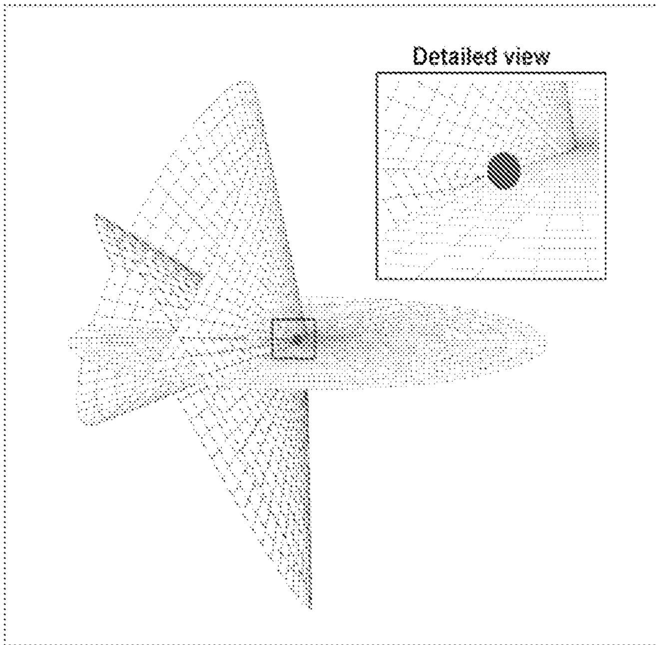


Figure 10. Intersection of three hyperboloids from [68]. With four receivers in a 3D setting, one can specify the origin of the message as the red point where the computed hyperboloids intersect.

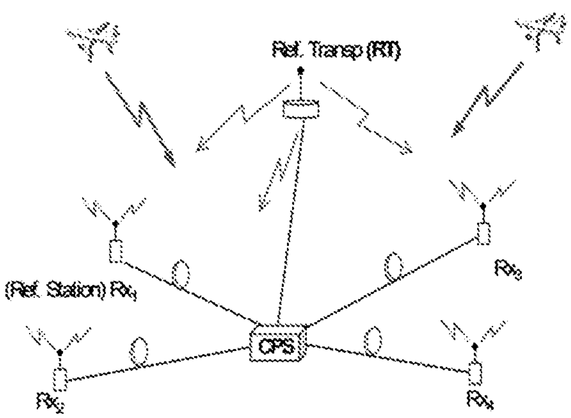


Figure 11. Basic multilateration architecture from [69]. Four (or more) receiver stations (Rx) measure the time at which they receive the same message from an aircraft. They send this data to the central planning station which can calculate the aircraft's position from from the time difference of arrival between the receiver stations.

Performing multilateration by utilizing TDOA is currently the preferred solution for location verification on the ground. It is used in the field (e.g. by the ASDE-X system [70]) at various US airports[20] and also being rolled out in Europe in connection with the CASCADE project.[21] One major advantage of multilateration is the fact that it can utilize aircraft communication that is already in place. Thus, there are no changes required to the currently existing infrastructure in aircraft, while on the ground receiver stations and central processing stations have to be deployed (see Fig. 11).

While currently used mainly in comparably short distances (taxiway and runway on airports, up to about 60 m height), Wide Area Multilateration (WAMLAT) has also been a popular research topic. Compared to primary radar systems, WAMLAT is relatively easy and cost-effective to install and use on the ground but can also be successfully employed in an airborne MANET.[22] Using an estimated distance of a target between four or more receivers, it is possible to tell the 3D position of a sender with roughly 30 m accuracy (at 90 NM distance) compared to 20 m for ADS-B [71]. However, in comparison to ADS-B the accuracy of multilateration in practice deteriorates over long distances (see Fig. 12).

There have been various practical studies of multilateration using ADS-B signals. For example, [5] examines it as a method to provide a means to backup and validate ADS-B communication. Johnson et al. [72] describe their proof of concept work in a war-zone in Afghanistan. Kaune et al. [73] built a proprietary low cost test bed to do multilateration with ADS-B signals. Thomas [74] presents findings from two controlled helicopter flights in the North Sea.

Daskalakis and Martone [75] give a technical assessment of the possibility of using ADS-B and WAMLAT in the Gulf of Mexico, testing a single controlled flight with good accuracy.

A recent work at MITRE Corporation [76] analyzes the attempt to build an alternative navigation system with WAMLAT in the FAA-mandated US airspace. The authors discuss the potential use of already deployed sensors for multilateration around three airports with flat terrain, also noting that the challenge is greater in more mountainous areas. Further, they provide some sensor placement discussion, determining the optimal choice and number from a given database concerning requirements such as accuracy and low dilution of precision.

Despite its successful use in the field, multilateration leaves a number of open problems in terms of secure location verification, for example the estimation of aircraft altitudes with ground-based receivers is known to be very difficult. Galati et al. [77] discuss the theoretical application secondary surveillance radar as basis for multilateration in airport surveillance. They analyze a case study of Marco Polo airport in Venice and look at technical details such as dilution of precision and multilateration algorithms and conduct simulations with five sensors in a 25 km radius around the airport. They propose angle-of-arrival measurements to improve the unsatisfying height estimates provided by wide area multilateration.

The International Civil Aviation Organization also names a few of the known limitations of multilateration: [26]

1) Aircraft have to be equipped with a functioning transponder.
2) It is susceptible to multi-path.
3) The transmitted signal has to be correctly detected at multiple receiving stations.
4) Communication links are needed between remote receiver/transmitter sites and the master processing station.

Essentially, some of the limitations stem from cost and logistic reasons as it can be difficult and expensive to deploy enough sensors and stations in very remote and inaccessible areas.

[20]See the manufacturer's description: http://www.saabsensis.com/docs/128/

[21]http://www.cascade-eu.org

[22]Although vast open spaces such as found in e.g. Australia or over oceans can prove infeasible for the use of multilateration and have been one of the very reasons driving the development and deployment of ADS-B.

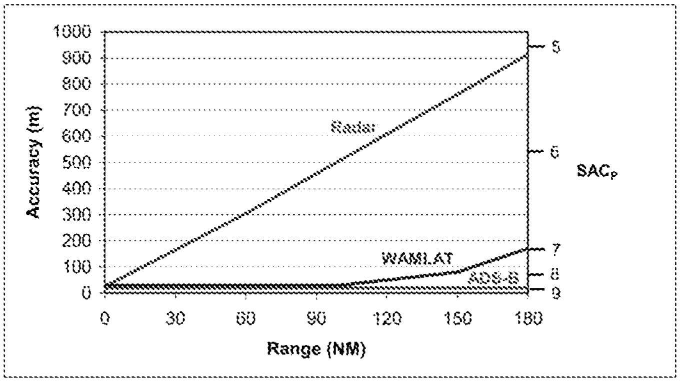


Figure 12. Comparison of location estimation accuracies when utilizing primary radar, wide area multilateration and ADS-B [5]. SAC_p denotes the Surveillance Accuracy Category for Position as defined in [5].

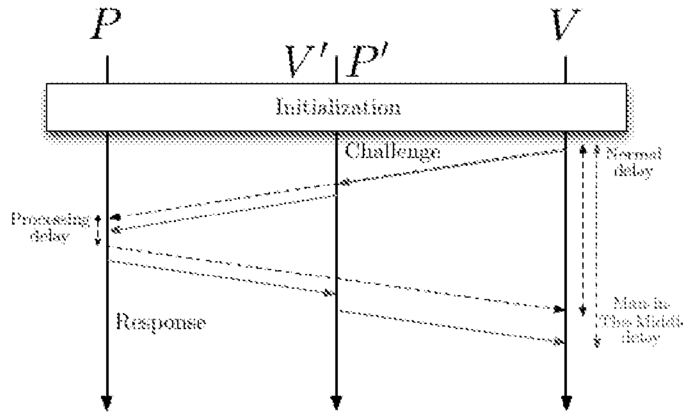


Figure 13. Principle of distance bounding protocols. The verifier V sends a challenge to the prover P who then, after processing, sends his response (black dashed arrows). A man in the middle (V'/P') can only increase the distance by adding further processing delays, but not decrease it (red arrows).

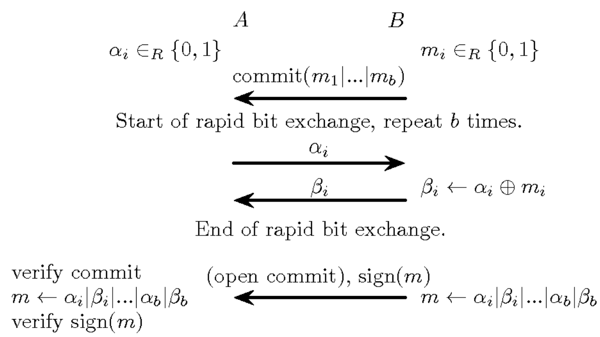


Figure 14. Original untrusting distance bounding protocol by Chaum and Brands [79]. A is the verifier, B the prover. After the protocol exchange A can verify that B is within a given distance.

Furthermore, [52] mentions an attack vector for an adversary trying to fool a receiver system utilizing multilateration for location verification. An attacker would need to purchase and modify four traffic-collision avoidance system (TCAS) receivers and use a GPS/WAAS time transfer unit between the units to ensure relative timing accuracy. Furthermore, he needs to engineer an algorithm similar to the one the TCAS uses to determine aircraft's tracks. As this involves both a certain cost and non-zero engineering knowledge the difficulty of exploiting this threat is relatively high, certainly when compared with the simplicity of spoofing ADS-B messages.

In principle, there always remains the question of how to secure the communication needed to perform multilateration and relay the localisation information to the other participants. If it is not properly secured, Sybil attacks, where a number of dishonest nodes deceive their environment, are entirely possible [78].

B. Distance Bounding

Distance bounding is another method that has been employed in wireless networks to partly localize other participants and ensure secure transaction e.g. for RFID communication. First presented by Brands and Chaum in 1993 [79], the idea behind distance bounding is to establish a cryptographic protocol with the goal to have a prover P show to a verifier V that P is within a certain physical distance (see Fig. 14 for the concrete protocol). The universally valid fact that electromagnetic waves travel roughly at the speed of light c, but never faster, builds the foundation of all distance bounding protocols.[23] This enables the computation of a distance based on the time of flight between the verifier's challenge and the corresponding response by the prover. The determined distance serves as an upper-bound, an additional piece of information that can subsequently be used as a means to verify and authenticate a node by checking the truth of its claims. When distance-bounding is performed by various trusted entities (such as ground stations) these can collaborate and find the actual location of the prover via trilateration.[24] There are various practical attacks on distance bounding schemes given in the literature, among them a number of relay attacks such as the so-called distance fraud, mafia fraud and terrorist fraud [80] as well as the newer distance hijacking attack [81].

Consequently, an abundance of protocols have been suggested to deal with these various deficiencies. Song et al. [82] give an example of a secure distance bounding mechanism for VANETs, comprising three steps:

1) Traditional distance bounding is used to find the lower bound of the distance between V and P. P can only increase the time to respond to V's challenge and as such only appear further away than it really is.
2) The verifier then checks the claimed location of P for plausibility (also see Section V-F):
    a) Transmission range-based verification: There are limits on the maximum distance of wireless transmission in practice. Test runs can help to find practical upper bounds for ADS-B users in a certain location/path. If the prover claims to be further

[23]This is in contrast to e.g. distance estimation via received signal strength, which can be influenced and faked by a malicious node.

[24]Triangulation is not to be confused with the previously described multilateration. The former uses the absolute measurements of three or more distance circles to determine positions, while the latter uses the *difference* in distance between the measurements.

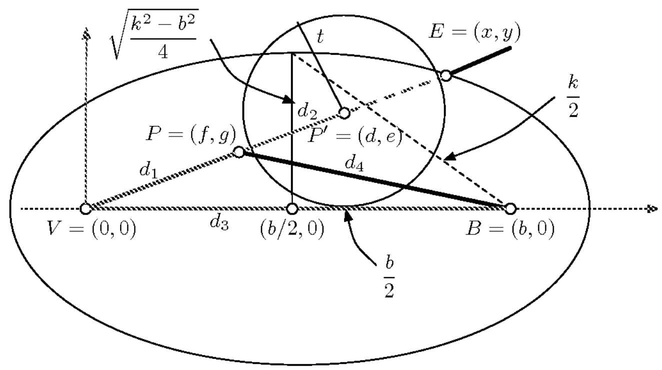


Figure 15. Network topology for a minimum distance guarantee after [82]. V is the verifier, P the prover, P' its claimed location. B is a common neighbour of both V and P who gives an estimate E of P's position. Considering the ellipse and a certain error distance, B can detect the distance enlargment of P.

away, it can be considered malicious.

b) Speed-based verification: Considering the fact that the typical speed of a given airplane in differing flight stages is known (certainly the physically possible minimum and maximum velocity), consecutive position claims have to be in a given window.

3) To further improve the security, after all plausibility checks have been passed, the verifier chooses a common neighbour B. That neighbour of both P and V then gives its location estimation E for P as shown in Fig. 15. Whenever the estimate lies outside the error margin, B knows that P enlarged its distance.

While in the literature distance bounding has been used mostly for close-up, indoor communication, it has been modeled for use in VANETs up to a distance of 225 m between prover and verifier [82], [83]. Tippenhauer and Capkun [84] also considered the impact of moving targets on distance bounding protocols and verifiable multilateration. In their original implementation, it takes about 600ms to perform a full localization, which, at a speed of only 500 km/h means that a target already moves 75 m during the process. The authors propose Kalman filters (see Section V-C) to smoothly keep track of the prover's location and detect any malicious tampering by outsiders.

Besides its current unsuitability for the long distances and high velocities present in air-traffic control, another main disadvantage of distance bounding is the fact that it inherently requires a response by the prover to the verifier's challenge and thus from an ADS-B point of view enforces an entirely new protocol paradigm. As an additional, on-demand feature it could still provide crucial information about the legitimacy of nodes in areas where PSR is not present (or is phased out due to cost reasons) .

C. Kalman Filtering and Intent Verification

Kalman filters (also known under the technical term linear quadratic estimation) [85] have already seen extensive use in broader ATC applications, e.g. to filter and smoothen GPS position data in messages. It is used to observe noisy time series of measurements and tries to statistically optimally predict future states of the measured variables of the underlying system.

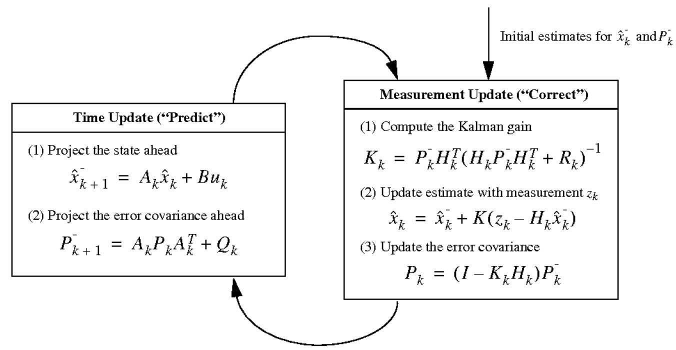


Figure 16. Basic concept of Kalman filtering from [86]. The time update step projects the measured variables and the error covariances. The measurement update step computes the Kalman gain and updates the estimates and error covariances with the actual measurements.

A high level overview of the Kalman filtering algorithm comprises two distinct steps, a prediction step and an update step (see Fig. 16). As the procedure is recursive it can easily be used and updated in real time, without having to save more than the last state.

- Prediction step: In the first step, the current state variables are predicted as well as the connected uncertainties.
- Update step: For every following step, the previously obtained estimates are then updated with a weighted average. During this process, the estimates with higher certainty are assigned higher weight.

The theory behind Kalman filtering requires the observed system to be linear and the underlying measuring variables and errors to follow a normal distribution, although there have been developments to adapt the approach to non-linear systems, too.

Kalman filtering plays a crucial role in the multilateration approach, sorting out noisy signals and smooth over missing data (Fig. 17). It is also a useful tool in general to predict the future values of a feature based on collected historical data. More concretely, it is used in ground systems to filter and verify the state vectors and trajectory changes reported by ADS-B aircraft and conduct plausibility checks on these data [87]. Krozel et al. [88] then go on further to verify the intent of the aircraft by first defining local and global correlation functions to evaluate the correlation between aircraft motions and the ADS-B intent (Fig. 16). Then the authors compute geometric conformance, i.e. if the aircraft is in given horizontal and vertical limits and intent conformance, i.e. analyzing the aircraft motion and comparing it to a plausible intent model in several dimensions (in this case horizontal, vertical and velocity).

Kovell et al. [21] note that since Kalman filtering is used in a number of ADS-B related systems, it is essential to distinguish between Kalman filters dealing with an aircraft's GPS position, with received signal strength of packets and the angle of arrival at a recipient's antenna and their proposed use for real time

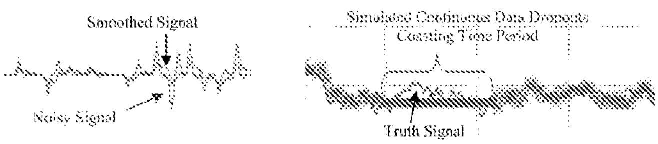


Figure 17. Example of Kalman filtering from [88]. Noisy signals are being smoothed (left), dropped data being coasted over below a given cutoff point (right).

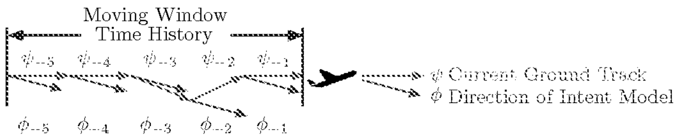


Figure 18. Practical application of intent verification in ADS-B from [88]. The example analyzes the horizontal aircraft motion with a global correlation function as a moving window over local correlation functions.

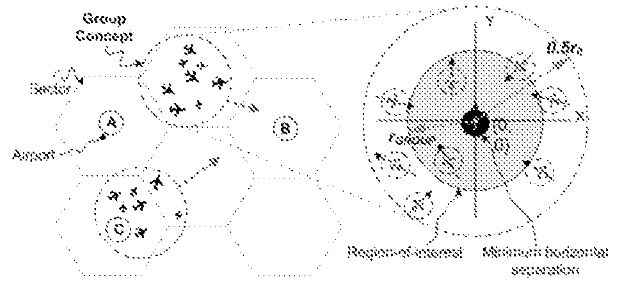


Figure 19. Illustration of the group concept from [19]. Four or more aircraft V are in any group G. Each group then can internally use multilateration to verify each other's location claims as well as those of outsiders in range. r_0 is the wireless communication range, $0.5r_0$ considered geographically proximate and thus acceptable for group establishment, given sufficient communication quality. To lower group overhead, the region of interest for a group can be restricted to r_{group}.

positional claim verifications of an aircraft onboard of other aircraft. Kalman filtering of positional claims is slightly more difficult in aircraft-to-aircraft systems but there are no inherent impossible obstacles to it.

From an attacker's point of view, Kalman filters can be tricked by a so-called frog boiling attack [89]: The adversary is jamming the correct signal, while continuously transmitting an ever-so-slightly modified position. If this is done slowly enough, the Kalman filter will see the injected data as a valid trajectory change. This exposes a general weakness of Kalman filtering as the approach is based on comparatively little historical data. But it is still of great use since obviously bogus manoeuvres, speeds, features can be detected (see also Section V-F) and the complexity of any attack is greatly increased. Another general downside is that it opens up more DoS-possibilities due to the largely increased computational complexity at every receiver, although this is not a major problem with comparably powerful installations in ground stations and airplanes. A possible threshold time after which sufficient trust has been established between two participants based on data validated by Kalman filtering is still open research [21].

D. Group Verification

Group verification is another concept proposed to mitigate security and privacy concerns over the use of ADS-B [19]. It aims at securing the airborne ADS-B IN communication by employing multilateration done by a group to verify location claims of non-group members in-flight. A given authenticated group with 4 or more aircraft having established trust can communicate with each other to utilize multilateration (based on TDOA or RSS) just as ground stations can (see Section V-A). If a forged position report is detected, the sensible reaction would be to increase the circle of avoidance around nearby airplanes since their position cannot anymore be regarded as precisely known and thus safe.

Kovell et al. [21] conducted a study about the applicability of the group concept in commercial aviation in the United States airspace. Examining the vast differences in traffic density over the US, they found that around 91% of aircraft at a given time could be part of a sufficiently large group of 4 aircraft or more.

Group verification has a number of downsides. First of all, it requires many additional messages to implement the verification and trust process. As ADS-B is purely unidirectional broadcast, a new protocol is needed to support the group concept. Concerning the question of which protocol to use, the authors mention the L-Band Digital Aeronautical Communication System (L-DACS) as one possibility. L-DACS is being developed by EUROCONTROL as a future IP technology for air-to-air communication but unfortunately there is no specification in sight in the medium term.[25] If such a protocol can be successfully implemented, there remains the central problem of how to manage the secure authentication of members that are to be accepted into the group in the first place. It is very complicated to establish trust in new groups of MANETs and to reliably avoid malicious aircraft. Furthermore, the performance of the system in reaction to intelligent intentional jamming of some or all communication would have to be considered.

On the other hand, even without a perfectly secure solution, the group concept would raise the difficulty and engineering effort of certain attacks on airborne aircraft by orders of magnitude.

E. Data Fusion and Trust Management

Data fusion is quickly becoming a cornerstone of modern intelligent transport systems (ITS). The concept can be used at various stages of data processing, Baud et al. [90] e.g. describe the fusion of radar and ADS-B data and show that this approach can improve the quality of tracking in practice. Concerning ADS-B security, the literature proposes to

[25]"In addition to the air/ground capability, some of the assessed technologies could also support additional features such as air/air (point to point and/or broadcast) communications and digital voice. However the support of these capabilities needs further investigation." http://www.eurocontrol.int/communications/public/standard_page/LDACS.html

check positional data obtained from within the system against data coming in from other, independent sources. Adequate data can e.g. stem from multilateration (see Section V-A), traditional primary radar systems or even flight plan data. Such verification can provide a way of knowing if some of the involved systems work outside normal parameters, be it from a malicious source or not. Subsequently, automated technical or non-technical procedures can be carried out, identifying the problem and reacting accordingly. This process comprises an analysis of the trust-worthiness of the data, if it has been vulnerable to tampering depending on the system and the precision/measurement uncertainty of the respective technologies (as given e.g. in [5]). The trust-worthiness can then be calculated by looking at the correlations and further features deduced through machine learning processes which aim to expose anomalies in received information and thus to enable more automated detection of attacks.

An example of this is given in [91]. The authors use the cosine similarity between claimed and estimated positions to judge the trustworthiness of a participant's claims and maintain historical beacon trust information :

$$Sim_{Cos}(\vec{E},\vec{O}) = \frac{\vec{E}\cdot\vec{O}}{|\vec{E}|\cdot|\vec{O}|} = \frac{x_E \times x_O + y_E \times + v_E \times v_O}{\sqrt{x_E^2 + y_O^2 + v_E^2} \times \sqrt{x_O^2 + y_O^2 + v_O^2}} \quad (1)$$

x_O, y_O are the coordinates, v_O the velocity as claimed in the last received message. x_E, y_E are the estimated coordinates of the claimant, based on the previously received message. As a further step they calculate the time-based weighted trustworthiness of a beacon message, taking into account the cosine similarity of the last I beacon messages and their respective estimates:

$$T_{beacon} = \frac{\sum_{i=1}^{I} Sim_{Cos}(\vec{E},\vec{O})(w_i)^n}{\sum_{i=1}^{I}(w_i)^n} \quad (2)$$

It is easy to make a case for data fusion, since many of the required components are already available and a two-out-of-three (2oo3) approach is widely accepted best practice in many industries dealing with processes that are crucial to safety and security. It has even been suggested to equip the average car with primary surveillance radar, to secure vehicular ad hoc networks [92].

There are already a number of integrated systems being deployed (such as ASDE-X) that are inherently fusing the data of various sub-systems (ADS-B, multilateration, flight plan information, radar data) to increase both security and accuracy in airport proximity. The clear advantage of data fusion is the compatibility with legacy systems, including the fact that the ADS-B protocol does not need to be amended to provide these additional features. The downsides include increased cost for additional systems to provide the necessary redundancy.

F. Traffic Modeling and Plausibility Checks

Traffic modeling could provide a mechanism to detect deviations from normal ADS-B behaviour. By utilizing historical data as well as machine learning methods it is possible to create a model of a map for each ground station, providing a means to verify location claims made by aircraft via ADS-B. Figure 20 shows how a typical heat map based on RSS values looks from the point of view of a ground station. Such models can provide hints about non-matching location claims of a message send by an aircraft. Other potential considerations include checking for a certain number of consecutive packets of the same - or different - aircraft with the same RSS/angle-of-arrival, or otherwise suspicious absolute values which could indicate a stationary, ground-based attacker (e.g. RSS/AoA values outside typically observed thresholds).

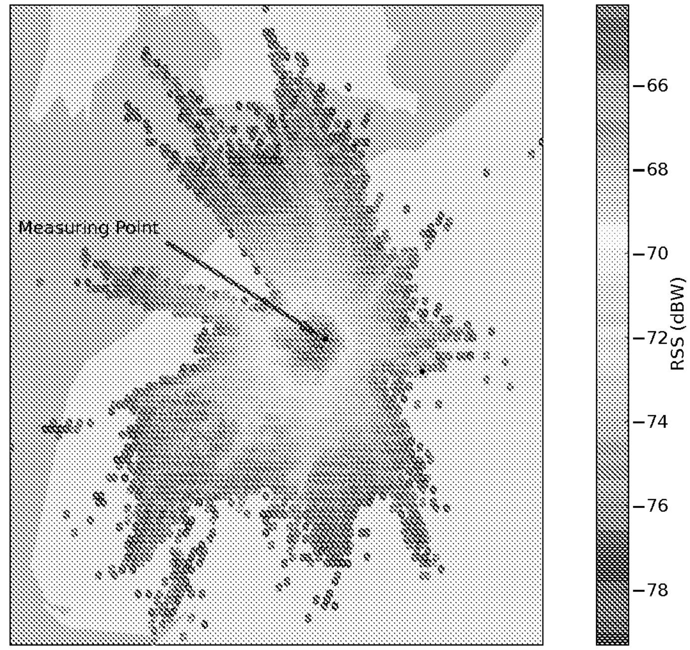


Figure 20. Example of an RSS heat map used for traffic modeling from [1]. The colors indicate the received signal strength at a single measuring point which correlates strongly with the distance. Though it is relatively easy for an attacker to manipulate the RSS, it becomes increasingly difficult the more measuring points have to be deceived.

Xiao et al. [93] used a similar statistical approach for the detection of Sybil nodes in VANETs. They propose an algorithm that could be performed by any node that has received enough measurements of e.g. signal strength from nearby witnesses. While a single estimated position of a node may not be an accurate representation of the real location, a larger sample of estimated positions would have to be very similar to the node's position claims over a given period of time.

More formally, if in a period Δt_o there are n sequential positions $l_1, ..., l_n$ claimed by an airplane and the corresponding estimated positions $l_1^{'}, ..., l_n^{'}$, then the difference between the two can be treated as a random error. That means that a large enough sample of differences is distributed normally with a mean μ_d and a variance σ_0^2. Under these assumptions, it is sufficient to test against the hypotheses:

$$H_0 : \mu_d = 0 \;\; H_1 : \mu_d \neq 0$$

$$H_0^{'} : \sigma^2 \leq \sigma_0^2 \;\; H_1^{'} : \sigma^2 > \sigma_0^2$$

If both H_0 as well as $H_0^{'}$ are true than it can be assumed that the claimant has given valid positional reports within the chosen level of significance (see [93] for further explanations and simulation results in VANETs). As this method is only really practical for fixed receivers, the goal is to use ground stations to detection of unusual behaviour. They are also more likely to be able to collect enough samples to make the verification process as sound as possible.

On top of this, there are numerous comparably simple rules that can be utilized as potential red flags by an intrusion detection system without resorting to more complex measures. Neither of these rules are necessary nor sufficient by themselves to detect an ongoing attack. But depending on the scenario and the attacker's savvy, they can indicate unusual behaviour that should be further investigated either by a human or handled through additional technical means. For example, it is very plausible to outright drop a number of packets where either the data or the meta data is technically or physically impossible. Doing so can significantly reduce the strain on the ADS-B system and even prevent both spoofing and DoS attacks which are not crafted carefully enough. If a large number of potential red flags are checked for an intrusion detection system, not only the risk for an attacker to cause an alert increases significantly, but also the cost and complexity of an attack rise. While this does not constitute theoretical perfect security, plausibility checks can be very useful in practice.

Mitigating factors exist across various layers, from the physical to the application layer. Some are available to ground stations/air traffic control only, others also to aircraft-to-aircraft (A2A) ADS-B IN communication. Such cases include but are not limited to:

- Investigating **airplanes which suddenly appear** well within the maximum communication range of a receiver.
- Dropping **aircraft which are violating a given acceptance range threshold**, producing impossible locations [94].
- **Aircraft violating a given mobility grade threshold**, producing impossible minimum or maximum velocities [94].
- **Maximum Density Threshold**: If too many aircraft are in a given area, ATC software will typically alarm the user [94].
- **Map-based Verification**: Aircraft in unusual places such as no-fly areas or outside typical airways (this might possibly be better handled at the ATC software layer) [94].
- **Flight plan-based Verification**: Flooded/attacked ground stations are able to check ADS-B messages against the existing flight plan.
- Obvious **discontinuities in one of the 9 ADS-B state vector data fields** (also see the related Section V-C) .

As explained before, such potential red flags need to be handled with utmost care and can typically not be automated but require much additional scrutiny before any action is taken (e.g., the packet/flight is considered an attack and dropped from ATC monitors). Yet, they also enable the opportunity to follow up and activate further means to secure the airspace. For example, when using such centralized detection at the ground stations, these same stations could then destroy messages sent by the detected offenders as outlined in [95], [96].

VI. Summary and Further Discussion

Tables I-III provide a compact overview over the effectiveness of all examined solutions in combating the various proposed attacks as well as offering advantages and disadvantages concerning the feasibility to implement each approach in the real world. As has been laid out, there is no single optimal or even good solution when considering means that have no or little impact on the currently employed ADS-B software and hardware. Table I shows the attacks the discussed approaches can counteract. We see that most security schemes focus on attacks of the message injection/modification class. This has two main reasons that have been mentioned throughout this work: First of all, the open nature of ADS-B has been considered a desirable feature in most scenarios. So unless there is a major paradigm shift in the way air traffic communication and control is handled currently, there is no interest in protecting against passive listeners, despite this being the first stepping stone for more sophisticated and problematic attacks. Second, passive attacks such as eavesdropping are simply much more difficult to protect against without having a full cryptographic solution. Similarly, attacks on the physical layer, such as continuously jamming the well-known frequency or the more surgical message deletion are hard to defend against, with measures on the same layer (e.g. uncoordinated spread spectrum) providing some of the only approaches to this general wireless security problem. All discussed approaches do however address message insertion and tampering, either by protecting outright against it through verification (cryptographic methods) or by detecting anomalies in the data (e.g. Kalman filtering, multilateration).

	Injection / Modification	Eavesdropping	Jamming / Deletion
Physical Layer Authentication	+	-	-
Uncoordinated Spread Spectrum	-	+	+
(Lightweight) PKI	+	+	-
µTESLA	+	-	-
Wide Area Multilateration	+	-	-
Distance Bounding	+	-	-
Kalman Filtering	+	-	-
Group Verification	+	-	-
Data Fusion	+	-	-
Traffic Modeling	+	-	-

Table I
Overview of capabilities of various security approaches against feasible attacks on ADS-B.

	Data Integrity	Source Integrity	Location Integrity	DoS
Physical Layer Authentication	No	Yes	Possibly	Partly
Uncoordinated Spread Spectrum	No	No	No	Yes
(Lightweight) PKI	Yes	Yes	Yes	Partly
µTESLA	No	Yes	No	No
Wide Area Multilateration	No	No	Yes	No
Distance Bounding	No	No	Partly	No
Kalman Filtering	No	Partly	Partly	No
Group Verification	No	Possibly	Yes	No
Data Fusion	No	Partly	Yes	Backup
Traffic Modeling	No	No	Yes	No

Table II
OVERVIEW OF SECURITY FEATURES OF VARIOUS APPROACHES FOR USE WITH ADS-B.

	Difficulty	Cost	Scalability	Compatibility
Physical Layer Authentication	Variable	Variable	Variable	Requires additional hard-/software. No modifications to the ADS-B protocol.
Uncoordinated Spread Spectrum	Medium	Medium	Medium	Requires new hardware. No modifications to the ADS-B protocol.
(Lightweight) PKI	High	High	Medium	Distribution infrastructure and changes in protocol and message handling needed.
µTESLA	Medium	Medium	High	New message type required for key publishing, MAC added.
Wide Area Multi-lateration	Low	Medium	Medium	No change to ADS-B required. Separate hardware system.
Distance Bounding	High	Medium	Low	New messages and protocol needed.
Kalman Filtering	Low	Low	High	No additional messages needed. Separate software system.
Group Verification	High	Medium	Low	New messages and protocol needed.
Data Fusion	Low	Medium - High	Medium	No change in ADS-B required. Separate system.
Traffic Modeling	Medium	Low	High	Additional, separate entities for ground stations needed.

Table III
OVERVIEW OF FEASIBILITY ATTRIBUTES OF VARIOUS APPROACHES FOR USE WITH ADS-B.

Table II takes a look at the security features the discussed schemes can provide. As discussed before, only a full cryptographic public key infrastructure can guarantee the integrity of received data. All other approaches either aim to secure the integrity of the source (e.g. µTESLA, many of the discussed physical layer schemes) or seek to verify the provided location data independently. Additional protection against flood denial of service attacks against ATC systems can be directly provided by spread spectrum approaches and cryptography, while other methods rely on higher layers to sort out false aircraft claims.

Table III provides an overview over the feasibility of the different approaches in practical settings, especially considering the current state of air traffic control in the aviation industry. As is to be expected, the difficulty and cost columns are mostly correlated. The difficulty to overcome technical challenges is particularly high for distance bounding, which is yet in its beginnings and a full-blown public key infrastructure. In contrast, we see wide-area multilateration, Kalman filters and data fusion techniques already in use in the field. This naturally translates to the cost factor which plays an important role in industry decisions. One can choose between a completely new protocol which addresses the security question better than the current installment of ADS-B does, slight modifications such as new message types, or a transparent, parallel system which requires new software and/or new hardware in different scales. This touches also on the question of scalability. For example, the fusion of various ATC systems and their data (PSR, SSR, ADS-C, WAMLAT, FANS) is an obvious and necessary idea. Yet, it is common knowledge in the aviation community that a "major part of the business case for Automatic Dependent Surveillance - Broadcast (ADS-B) is attributed to the savings generated by decommissioning or reducing reliance on conventional radar systems" [5]. Thus, it seems inefficient and unlikely to have legacy and/or new backup systems around on a broad scale, simply to fix the inadequateness of ADS-B related to security.

Considering the fact that the invention, certification and large-scale deployment of air-traffic systems takes decades, as currently seen in the example of ADS-B, it seems equally non-sensible to present a completely overhauled ATC-system at this point in time. In practice this means that incremental changes with backwards compatibility as a main factor kept in mind are more likely to be successful than a completely new proposal. On the other hand, cost and complexity of deployment cannot be the only factors taking into consideration - not having security is famously even much more expensive.[26] As mentioned throughout this work, it can be a useful dichotomy to distinguish between attack detection, attack prevention and dealing with suspected attacks. In this paper, we focused mainly on attack detection and prevention, leaving attack reaction for future research.

VII. CONCLUSION

This survey sought to review the available research on the topic of securing the ADS-B protocol in particular and air traffic control communication in general. We provided an in-depth overview of the existing work, both specific to ADS-B as well as ideas brought in from related fields such as VANETs. After reviewing the literature, it seems that the solutions currently under consideration (and in use in practice such as multilateration) can only be a fill-in, providing a quick

[26]"If you think safety is expensive, try an accident", an insight by easyJet owner Stelios Haji-Ioannou that came after facing manslaughter charges for the deaths of employees in a shipping disaster at a former company.

improvement to the security of the current system. For all-encompassing security (and possibly privacy), new message types and/or completely new protocols would need to be defined. Taking this into account for the creation of a long-term security solution in dependent air traffic surveillance, it makes sense to consider the impact of both secure broadcast authentication approaches as well as secure location verification. This should include a thorough breakdown of future traffic density, including upper bounds on wireless communication not only on current navigation channels, as well as the possible impact of communication and message overhead of a new protocol to not run into hard challenges again in the foreseeable future.

References

[1] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic, "Experimental analysis of attacks on next generation air traffic communication", in *Applied Cryptography and Network Security*. Springer, 2013, pp. 253–271.

[2] Andrei Costin and Aurelien Francillon, "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices", in *Black Hat USA*, 2012.

[3] ICAO, "Cyber Security for Civil Aviation", in *Twelfth Air Navigation Conference*, 2012, pp. 1–4.

[4] EUROCONTROL, "Cascade news 9 - update on developments", October 2010.

[5] A Smith, R Cassell, T Breen, R Hulstrom, and C Evers, "Methods to Provide System-wide ADS-B Back-Up, Validation and Security", in *25th Digital Avionics Systems Conference*, 2006, pp. 1–7.

[6] RTCA Inc., "Minimum aviation system performance standards for automatic dependent surveillance broadcast (ads-b)", DO-242A (including Change 1), December 2006.

[7] RTCA Inc., "Minimum operational performance standards for 1090 mhz extended squitter automatic dependent surveillance – broadcast (ads-b) and traffic information services – broadcast (tis-b)", DO-260B with Corrigendum 1, December 2011.

[8] RTCA Inc., "Minimum operational performance standards for universal access transceiver (uat) automatic dependent surveillance – broadcast", DO-282B with Corrigendum 1, December 2011.

[9] Donald McCallie, Jonathan Butts, and Robert Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system", *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, August 2011.

[10] John R. Barry, *Wireless Infrared Communications*, Kluwer Academic, Boston, 1994.

[11] Matthias Wilhelm and Ivan Martinovic, "Short paper: reactive jamming in wireless networks: how realistic is the threat?", *Proceedings of the fourth ACM conference on Wireless network security*, pp. 47–52, 2011.

[12] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Čapkun, "Investigation of signal and message manipulations on the wireless channel", in *ESORICS'11 Proceedings of the 16th European Conference on Research in Computer Security*, 2011.

[13] Matthias Wilhelm, Jens B Schmitt, and Vincent Lenders, "Practical message manipulation attacks in IEEE 802.15.4 wireless networks", in *MMB & DFT 2012 Workshop Proceedings*, 2012.

[14] Hua Li, Bo Yang, Cailian Chen, and Xinping Guan, "Connectivity of Aeronautical Ad hoc Networks", in *2010 IEEE Globecom Workshops*. December 2010, pp. 1788–1792, Ieee.

[15] Boeing Commercial Airplanes Market Analysis, "Boeing current market outlook 2011-2030", 2011.

[16] Adrian Perrig and Doug Tygar, *Secure Broadcast Communication in Wired and Wireless Networks*, Springer, 2003.

[17] Patrick J Martone and George E Tucker, "Candidate requirements for multilateration and ADS-B systems to serve as alternatives to secondary radar", in *Digital Avionics Systems, 2001. DASC. 20th Conference*, 2001, pp. 1–12.

[18] Christos Rekkas and Melvyn Rees, "Towards ADS-B implementation in Europe", *2008 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles*, pp. 1–4, September 2008.

[19] Krishna Sampigethaya and Radha Poovendran, "Security and privacy of future aircraft wireless communications with offboard systems", *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, pp. 1–6, January 2011.

[20] Krishna Sampigethaya and Linda Bushnell, "A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance", in *AIAA Proceedings*, 2009, pp. 1–10.

[21] Brandon Kovell, Benjamin Mellish, Thomas Newman, and Olusola Kajopaiye, "Comparative Analysis of ADS-B Verification Techniques", 2012.

[22] Bashar Nuseibeh, Charles B Haley, and Craig Foster, "Securing the Skies: In Requirements We Trust", *Computer*, vol. 42, no. 9, pp. 64–72, 2009.

[23] Jack Burbank, Robert Nichols, Sunita Munjal, Robert Pattay, and William Kasch, "Advanced communications networking concepts for the National Airspace System", in *2005 IEEE Aerospace Conference*. 2005, pp. 1905–1923, IEEE.

[24] Winston Wenhua Li and Pan Kamal, "Integrated Aviation Security for Defense-in-Depth of Next Generation Air Transportation System", in *IEEE Conference on Technologies for Homeland Security*, 2011, pp. 136–142.

[25] Washington Y. Ochieng, Knut Sauer, David Walsh, Gary Brodin, Steve Griffin, and Mark Denney, "GPS Integrity and Potential Impact on Aviation Safety", *Journal of Navigation*, vol. 56, no. 1, pp. 51–65, January 2003.

[26] Julio C. Siu, "ICAO Concepts and References Regarding ADS-B, Multilateration and Other Surveillance Techniques", in *ICAO/FAA Workshop on ADS-B and Multilateration Implementation*, 2011, number September.

[27] Richard Wagner, "IFF, Combat ID and the Information Domino Effect", Tech. Rep., Canadian Department of National Defence, 2009.

[28] Office of Technology Assessment U.S. Congress, *Who Goes There: Friend or Foe?*, U.S. Government Printing Office, Washington, DC, 1993.

[29] Larry Kenney, Joe Dietrich, and Jerry Woodall, "Secure ATC surveillance for military applications", *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pp. 1–6, November 2008.

[30] RTCA Inc., "Proposed change to do-181d and ed-73c for higher squitter rates at lower power", Special Committee 209 ATCRBS / Mode S Transponder MOPS Maintenance, April 2007.

[31] Mark Luk, Adrian Perrig, and Bram Whillock, "Seven cardinal properties of sensor network broadcast authentication", *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks - SASN '06*, p. 147, 2006.

[32] Thomas YC Woo and Simon S Lam, "Authentication for Distributed Systems", *Computer*, vol. 25, no. 1, pp. 39–52, 1992.

[33] Boris Danev, Davide Zanetti, and Srdjan Capkun, "On physical-layer identification of wireless devices", *ACM Computing Surveys*, vol. 45, no. 1, pp. 1–29, November 2012.

[34] Boris Danev, Heinrich Luecken, Srdjan Capkun, and Karim El Defrawy, "Attacks on physical-layer identification", in *Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 89–98.

[35] Kai Zeng, Kannan Govindan, and Prasant Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks", *IEEE Wireless Communications*, pp. 1–8, 2010.

[36] Suman Jana and Sneha Kumar Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews", *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, March 2010.

[37] Roel Maes and Ingrid Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions", *Towards Hardware-Intrinsic Security*, , no. 71369, pp. 3–27, 2010.

[38] Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications", *2008 IEEE International Conference on RFID*, pp. 58–64, April 2008.

[39] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel", in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 128—-139.

[40] Junxing Zhang, Sneha K. Kasera, and Neal Patwari, "Mobility Assisted Secret Key Generation Using Wireless Link Signatures", in *2010 Proceedings IEEE INFOCOM*. March 2010, pp. 1–5, IEEE.

[41] Qian Wang, Hai Su, Kui Ren, and Kwangjo Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless

networks", *2011 Proceedings IEEE INFOCOM*, pp. 1422–1430, April 2011.
[42] Jie Xiong and Kyle Jamieson, "SecureAngle: Improving Wireless Security Using Angle-of-Arrival Information", in *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, p. 11.
[43] Di Qiu, Dave De Lorenzo, Sherman Lo, Dan Boneh, and Per Enge, "Physical Pseudo Random Function in Radio Frequency Sources for Security", in *Proceeding of ION ITM*, 2009, pp. 26–28.
[44] Christine Laurendeau and Michel Barbeau, "Insider attack attribution using signal strength-based hyperbolic location estimation", *Security and Communication Networks*, vol. 1, no. July, pp. 337–349, 2008.
[45] Christine Laurendeau and Michel Barbeau, "Probabilistic Localization and Tracking of Malicious Insiders Using Hyperbolic Position Bounding in Vehicular Networks", *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 128679, 2009.
[46] Mario Strasser, Christina Pöpper, Srdjan Capkun, and Mario Cagalj, "Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping", *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 64–78, May 2008.
[47] Christina Pöpper, Mario Strasser, and Srdjan Capkun, "Jamming-resistant Broadcast Communication without Shared Keys", in *Proceedings of the USENIX Security Symposium*, 2009, pp. 231–247.
[48] Donggang Liu, Peng Ning, Sencun Zhu, and Sushil Jajodia, "A Tree-Based μTESLA Broadcast Authentication for Sensor Networks".
[49] Cindy Finke, Jonathan Butts, Robert Mills, and Michael Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system", *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3–11, March 2013.
[50] Ken Samuelson, Ed Valovage, and Dana Hall, "Enhanced ADS-B Research", *2006 IEEE Aerospace Conference*, pp. 1–7, 2006.
[51] Marc Viggiano, Edward Valovage, Ken Samuelson, Dana Hall, et al., "Secure ads-b authentication system and method", 2010, US Patent 7,730,307.
[52] Leonard Schuchman, "Automatic dependent surveillance system secure ads-s", 2011, US Patent 7,876,259.
[53] Feng Ziliang, P A N Weijun, and Wang Yang, "A Data Authentication Solution Of ADS-B System Based On X .509 Certificate", in *27th International Congress of the Aeronautical Sciences*, 2010.
[54] Chris Moody, "System Description for the Universal Access Transceiver", Tech. Rep. November, FAA, 2000.
[55] Maxim Raya and Jean-Pierre Hubaux, "The security of vehicular ad hoc networks", *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks - SASN '05*, p. 11, 2005.
[56] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.
[57] Richard V Robinson, Mingyan Li, Scott A Lintelman, Krishna Sampigethaya, Radha Poovendran, David Von Oheimb, and Jens-Uwe Bußer, "Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes", in *AIAA Aviation Technology Integration, and Operations (ATIO) Conference*, 2007.
[58] Bryan Parno and Adrian Perrig, "Challenges in Securing Vehicular Networks", in *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005, pp. 1–6.
[59] Junqi Zhang and Vijay Varadharajan, "Wireless sensor network key management survey and taxonomy", *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, March 2010.
[60] Adrian Perrig, Ran Canetti, J. D. Tygar, and Dawn Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels", in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 56–73.
[61] Adrian Perrig, Dawn Song, and Ran Canetti, "The TESLA Broadcast Authentication Protocol", 2005.
[62] Adrian Perrig, Robert Szewczyk, J D Tygar, Victor Wen, and David E Culler, "SPINS : Security Protocols for Sensor Networks", *Wireless networks 8*, vol. 8, no. 5, pp. 521–534, 2002.
[63] Mohamed Hamdy Eldefrawy, Muhammad Khurram Khan, Khaled Alghathbar, and Eun-Suk Cho, "Broadcast authentication for wireless sensor networks using nested hashing and the Chinese remainder theorem.", *Sensors*, vol. 10, no. 9, pp. 8683–95, January 2010.
[64] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux, "Real-World VANET Security Protocol Performance", *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–7, November 2009.
[65] Yih-Chun Hu and Kenneth P Laberteaux, "Strong VANET Security on a Budget", in *Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, 2006, vol. 06, pp. 1–9.
[66] Andreas Savvides, Heemin Park, and Mani B. Srivastava, "The bits and flops of the n-hop multilateration primitive for node localization problems", *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications - WSNA '02*, p. 112, 2002.
[67] WHL Neven, TJ Quilter, R Weedon, and RA Hogendoorn, "Wide Area Multilateration Report on EATMP TRS 131/04 Version 1.1", Tech. Rep., 2005.
[68] Ning Xu, Rick Cassell, and Carl Evers, "Performance assessment of Multilateration Systems - A solution to nextgen surveillance", in *Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2010, pp. 2–9.
[69] Gaspare Galati and Mauro Leonardi, "Wide area surveillance using SSR mode S multilateration: advantages and limitations", in *European Radar Conference (EURAD)*, 2005, pp. 225–229.
[70] J.G. Herrero, J.A. Besada Portas, F.J.Jimenez Rodriguez, and J. R Casar Corredera, "ASDE and multilateration mode-S data fusion for location and identification on airport surface", in *Radar Conference, 1999. The Record of the 1999 IEEE*, 1999, number 34, pp. 315–320.
[71] Leon Purton, Hussein Abbass, and Sameer Alam, "Identification of ADS-B System Vulnerabilities and Threats", in *Australian Transport Research Forum, Canberra*, 2010, pp. 1–16.
[72] Jerry Johnson, Holger Neufeldt, and Jeff Beyer, "Wide area multilateration and ADS-B proves resilient in Afghanistan", in *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2012 IEEE*, 2012.
[73] Regina Kaune, Christian Steffes, Sven Rau, Wolfgang Konle, and Juergen Pagel, "Wide area multilateration using ADS-B transponder signals", in *Information Fusion (FUSION), 2012 15th International Conference on*, 2012, pp. 727–734.
[74] Paul Thomas, "North sea helicopter ADS-B/MLat pilot project findings", in *Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), 2011 Tyrrhenian International Workshop on*, 2011, pp. 53–58.
[75] Anastasios Daskalakis and Patrick Martone, "A technical assessment of ADS-B and multilateration technology in the Gulf of Mexico", in *Proceedings of the 2003 IEEE Radar Conference.* 2003, pp. 370–378, Ieee.
[76] Frederick A Niles, Robert S Conker, M Bakry El-Arini, Daniel G O'Laighlin, and Dmitri V Baraban, "Wide Area Multilateration for Alternate Position, Navigation, and Timing (APNT)", Tech. Rep. 1, 2012.
[77] Gaspare Galati, Mauro Leonardi, Pierfrancesco Magarò, and Valerio Paciucci, "Wide area surveillance using SSR mode S multilateration: advantages and limitations", in *Radar Conference, 2005. EURAD 2005. European*, 2005.
[78] John R. Douceur, "The sybil attack", *Peer-to-peer Systems*, pp. 251–260, 2002.
[79] Stefan Brands and David Chaum, "Distance-bounding protocols", *Advances in Cryptology - EUROCRYPT'93*, pp. 344–359, 1994.
[80] Jolyon Clulow, Gerhard P Hancke, Markus G Kuhn, and Tyler Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks", in *Security and Privacy in Ad-hoc and Sensor Networks*, 2006, pp. 83–97.
[81] Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, and Srdjan Capkun, "Distance Hijacking Attacks on Distance Bounding Protocols", *2012 IEEE Symposium on Security and Privacy*, pp. 113–127, May 2012.
[82] Joo-Han Song, Vincent W. S. Wong, and Victor C. M. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks", *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, pp. 1–5, 2008.
[83] Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Škorić, Dave Singel, and Srdjan Čapkun, "Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System", in *Computer Security–ESORICS 2012*, 2012, pp. 415—-432.
[84] Nils Ole Tippenhauer and Srdjan Čapkun, "ID-Based Secure Distance Bounding and Localization", in *Computer Security–ESORICS 2009*, 2009, pp. 621–636.
[85] Rudolph Emil Kalman, "A new approach to linear filtering and prediction problems", *Journal of basic Engineering*, vol. 82, no. Series D, pp. 35–45, 1960.
[86] Greg Welch and Gary Bishop, "An introduction to the Kalman filter", pp. 1–16, 1995.
[87] Dieter Fox, Jeffrey Hightower, Lin Liao, and Dirk Schulz, "Bayesian Filters for Location Estimation", *Pervasive Computing*, vol. 2, no. 3, 2003.

[88] Jimmy Krozel, Dominick Andrisani, Mohammad A Ayoubi, Takayuki Hoshizaki, and Chris Schwalm, “Aircraft ADS-B Data Integrity Check”, in *AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum*, 2004, pp. 1–11.

[89] Eric Chan-Tin, Victor Heorhiadi, Nicholas Hopper, and Yongdae Kim, “The Frog-Boiling Attack: Limitations of Secure Network Coordinate Systems”, *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 3, pp. 27, 2011.

[90] O Baud, N Honore, and O Taupin, “Radar / ADS-B data fusion architecture for experimentation purpose”, in *9th International Conference on Information Fusion*, 2006, pp. 1–6.

[91] Yu-chih Wei, Yi-ming Chen, and Hwai-ling Shan, “Beacon-based Trust Management for Location Privacy Enhancement VANETs”, in *13th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2011.

[92] Gongjun Yan, Stephan Olariu, and Michele C. Weigle, “Providing VANET security through active position detection”, *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, July 2008.

[93] Bin Xiao, Bo Yu, and Chuanshan Gao, “Detection and Localization of Sybil Nodes in VANETs”, in *International Conference on Mobile Computing and Networking: Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006, pp. 1–8.

[94] Tim Leinmuller, Elmar Schoch, and Frank Kargl, “Position verification approaches for vehicular ad-hoc networks”, *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, October 2006.

[95] Ivan Martinovic, Paul Pichota, and Jens B Schmitt, “Jamming for Good: A Fresh Approach to Authentic Communication in WSNs”, in *WiSec ’09: Proceedings of the second ACM conference on Wireless network security*, 2009, pp. 161–168.

[96] Matthias Wilhelm and Ivan Martinovic, “WiFire: A Firewall for Wireless Networks”, *ACM SIGCOMM Computer Communication Review*, vol. 4, no. 4, pp. 456–457, 2011.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Filer:	Jed Margolin
Attorney Docket Number:	

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**730**

Electronic Acknowledgement Receipt

EFS ID:	17800483
Application Number:	14146202
International Application Number:	
Confirmation Number:	7721
Title of Invention:	ADS-B Radar
First Named Inventor/Applicant Name:	Jed Margolin
Customer Number:	23497
Filer:	Jed Margolin
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	02-JAN-2014
Filing Date:	
Time Stamp:	14:22:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$730
RAM confirmation Number	901
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Application Data Sheet	jm_adsb2_ads_aia0014.pdf	1565346 8351bab7673d0635172b0457df4ed675a4e2ea1a	no	7
Warnings:					
Information:					
2	Transmittal of New Application	jm_adsb2_transmittal_aia0015.pdf	275238 a2004b4515f6d6825c329e99be6b0269b71c5193	no	2
Warnings:					
Information:					
3	Oath or Declaration filed	jm_adsb2_declaration_aia0001_s.pdf	83978 072c0c1c86ea52b16e6ef05df8b61baf3645fda4	no	1
Warnings:					
Information:					
4	Miscellaneous Incoming Letter	jm_adsb2_fees_sb17.pdf	256250 4f77a3823f6b125f839f56880e69c40d0fca6109	no	2
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	jm_adsb2_ids.pdf	149919 031365502b09f4877f94c00d3f17980d549eaa78	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Specification	jm_adsb2_spec.pdf	77230 bf85b09e7361f42d91f53d3b6b002a003d908486	no	12
Warnings:					
Information:					
7	Claims	jm_adsb2_claims.pdf	29624 c0e15c99045a4ed47c8a064d874ec82102e7d9c1	no	9
Warnings:					
Information:					
8	Abstract	jm_adsb2_abstract.pdf	8786 4ee0f3c82fce321ea307a4533308e3a7b3d53311	no	1
Warnings:					
Information:					
9	Drawings-only black and white line drawings	jm_adsb2_figures.pdf	68146 8ce167abc3e8b8ec40e4915815a2f3d003d845bf	no	4

Warnings:					
Information:					
10	Foreign Reference	fpd_07_EP2136222.pdf	1322390 43af1491b0bafb6a2a970523ffb03a940ad84084	no	21
Warnings:					
Information:					
11	Non Patent Literature	npl_02_cfr1.pdf	40168 fa2bdd11ef1ba816b1373bba8e74b56b304e80a5	no	1
Warnings:					
Information:					
12	Non Patent Literature	npl_03_cfr2.pdf	38688 b635ea7d9dc99f6a40e304a50413cd32972955df	no	1
Warnings:					
Information:					
13	Non Patent Literature	npl_05_helo_ops.pdf	60845 3b7aae851203f51c1a925e7cbd1fbbe9e77fb599	no	3
Warnings:					
Information:					
14	Non Patent Literature	npl_09_afrl.pdf	176784 dca5ad308360f47dac6d5ae2f24dadb84478c13d	no	3
Warnings:					
Information:					
15	Non Patent Literature	npl_10_access5.pdf	2520004 dbdae2f0475c5b28f193a4189bf782586901f912	no	19
Warnings:					
Information:					
16	Non Patent Literature	npl_11_faa.pdf	3264175 d3ac1855142544d9fee267ed965a673e69b46b62	no	8
Warnings:					
Information:					
17	Non Patent Literature	npl_12_zone.pdf	476572 53795d0b631b121b6aafc24997b4b45dfee84b76	no	2
Warnings:					
Information:					
18	Non Patent Literature	npl_13_QRMFinalReport_v26Jan.pdf	3577602 a31d1a061e622b39c08b4646e6bf42df5107f7b9	no	48

Warnings:					
Information:					
19	Non Patent Literature	npl_14_FAST47_5-adsb2.pdf	2105976 f6527e29a714b71bc2358e69e93a5328ffa7c172	no	6
Warnings:					
Information:					
20	Non Patent Literature	npl_15_magazu_usaf2.pdf	6693611 c3b2785ffe590bb3fd003da8a38ff9b06b7bb228	no	101
Warnings:					
Information:					
21	Non Patent Literature	npl_16_adsb_security.pdf	2100152 73b631095c4ff10a70f71195e93a39d999a39fba	no	20
Warnings:					
Information:					
22	Fee Worksheet (SB06)	fee-info.pdf	31967 a11c83d1d7645ae6df7ff49b9488b89e881bdd81	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	24923451		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	

Title of Invention	ADS-B Radar

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 [Remove]

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jed		Margolin	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	VC Highlands	State/Province	NV	Country of Residence i	US

Mailing Address of Inventor:

Address 1	1981 Empire Rd		
Address 2			
City	Reno	State/Province	NV
Postal Code	89521-7430	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. [Add]

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	23497
Email Address	jm@jmargolin.com [Add Email] [Remove Email]

Application Information:

Title of the Invention	ADS-B Radar		
Attorney Docket Number		Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	Suggested Figure for Publication (if any)	1

Filing By Reference :

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	

Title of Invention	ADS-B Radar

Only compete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country i

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	23497		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Claims benefit of provisional	61887338	2013-10-05

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	

Title of Invention	ADS-B Radar

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country	Filing Date (YYYY-MM-DD)	Access Code (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	

Title of Invention	ADS-B Radar

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee ◯ Legal Representative under 35 U.S.C. 117 ◯ Joint Inventor

◯ Person to whom the inventor is obligated to assign. ◯ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	

Title of Invention	ADS-B Radar

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	ADS-B Radar	

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Jed Margolin/			Date (YYYY-MM-DD)	2014-01-02
First Name	Jed	Last Name	Margolin	Registration Number	
Additional Signature may be generated within this form by selecting the Add button.					

Add

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.