



Network Manager
nominated by
the European Commission



Experience Sharing to Enhance Safety

WS03-2018



**Automation, Digitalisation and Cyber – new challenges for
Human Factors in complex organisations**

"When machine world meets the human world in Air Traffic Management"

27-28 September 2018



University
Politehnica
of
Bucharest



Air Navigation



Faculty
of
Aerospace
Engineering

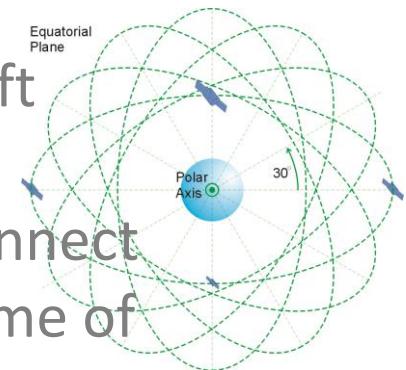
ADS-B and ADS-C communication in the light of digitalisation

Prof. dr. Octavian Thor Pleter, MBA (MBS)

Prof. dr. Cristian Emil Constantinescu, MBA (MBS)

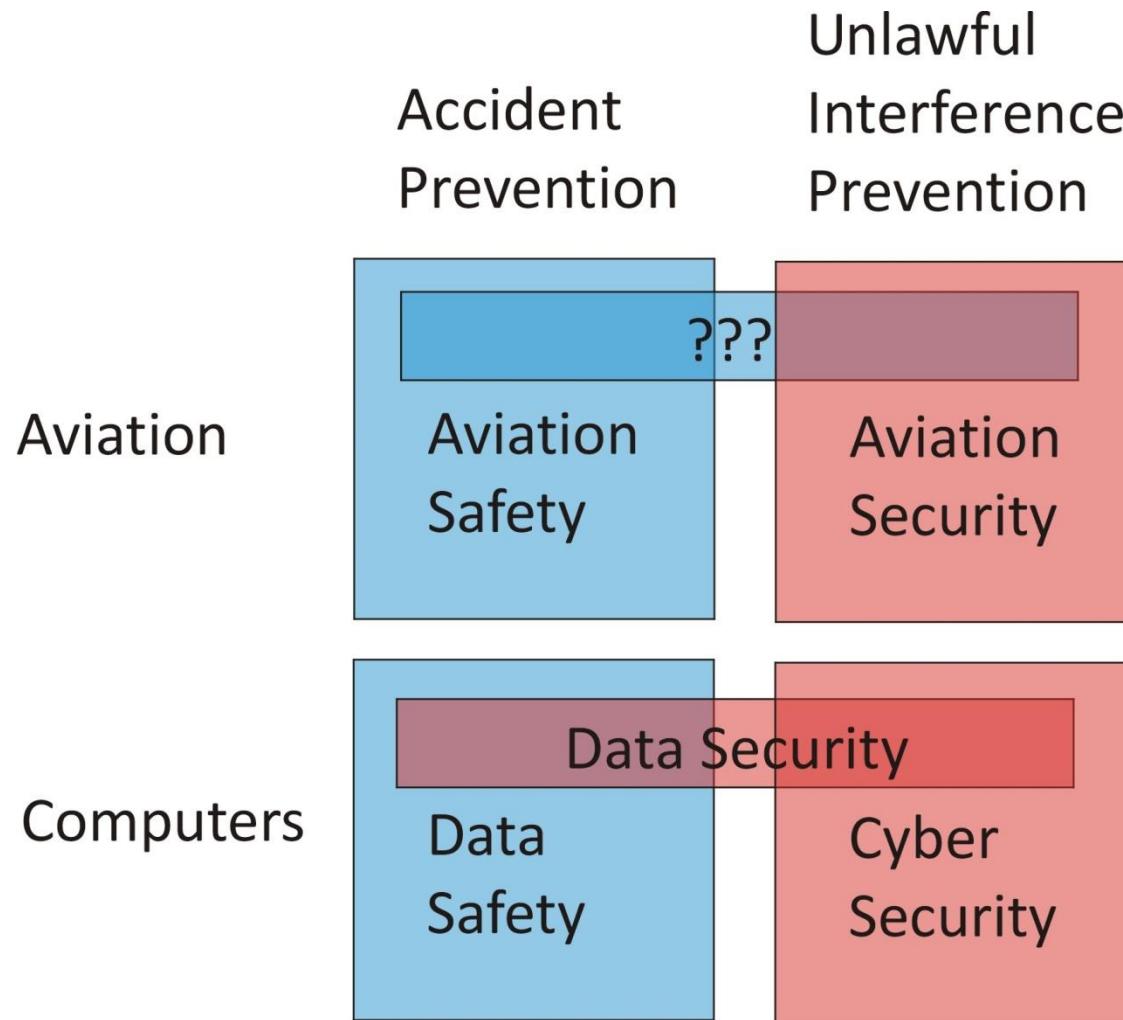
Main Points

- Aircraft are densely packed computer networks flying together everywhere, including some of the most remote / isolated regions of the world **(air segment)**
- ATM systems are part of a global ground based computer network **(ground segment)** + a global satellite network **(space segment)**, in need to communicate in real time with the above aircraft
- ADS/B and ADS/C are those messages which connect the three segments of the network - at least some of the distance is covered by radio transmissions



Main Questions

- How do ADS/B and ADS/C work?
- Do they improve on aviation safety and aviation security?
- Do they bring in new threats, such as data security problems or human factors problems (e.g. over-reliance on automation, mistrust in automation)?
- What could go wrong? What are the vulnerabilities?
- Who owns aviation data? Open / closed system?
- What could the solutions be? Brainstorming session

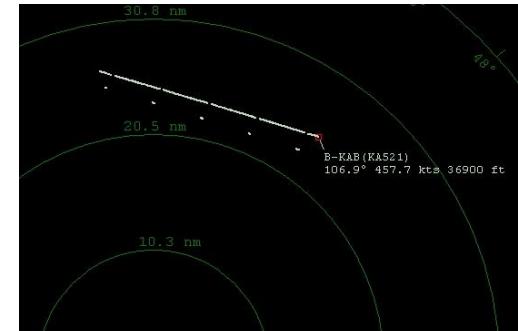
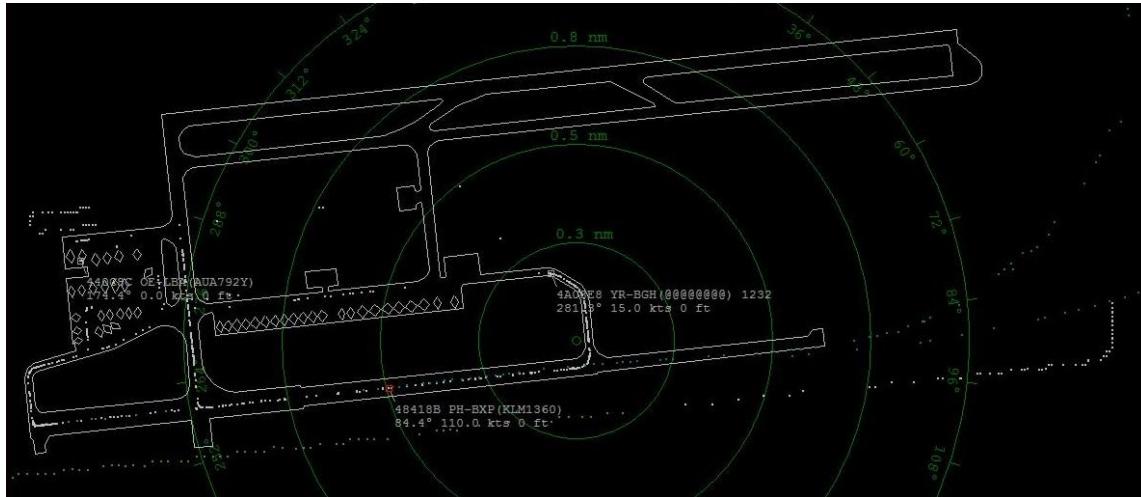


ADS/B Experiments

UPB Faculty of Aerospace Engineering

ADS/B Experiments

Where?	Henri Coanda International Airport Bucharest (LROP) and Aurel Vlaicu International Airport Bucharest (LRBS)
When?	Approx. 400 hours in the 2007-2009 time interval
Purpose	Determine maturity, accuracy, dependability and other issues with ADS/B technology
Method	<ol style="list-style-type: none">1. Compare ADS/B position to the SSR position2. Compare ADS/B position to the runway/taxiway centerline



ADS-B & ADS-C Technology

- Automatic - Always ON and requires no operator intervention;
- Dependent - Depends on accurate GNSS signal for positioning;
- Surveillance - Provides "Radar-like" surveillance services;
- Broadcast - It continuously broadcasts aircraft position and other data to any aircraft, or ground station
- Contract – Provides contractual communications air - ground

Source: ads-b.com

"Broadcast" is by definition:

1: cast or scattered in all directions

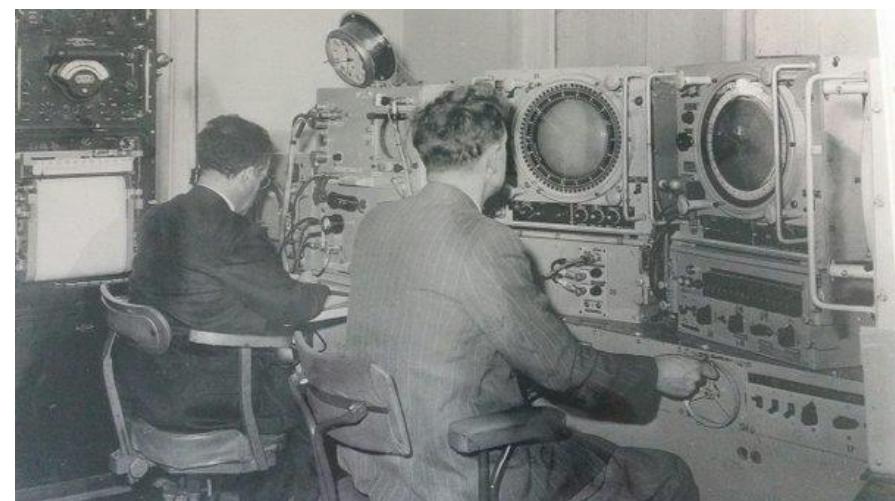
2: made public by means of radio or television

3: of or relating to radio or television broadcasting

(Myriam-Webster Dictionary)

ADS-B & ADS-C Technology

- ADS-B/C are new technologies enabled by a **very old setup of the radio spectrum**, established in 1950!
- ADS-B/C are **civilian** technologies **without any security** feature, easy to decode, easy to fake, based on old modulation types on some very crowded narrowband frequencies, easy to jam
- The only protection: fear of legal consequences -> attacks on aviation safety are punished by the Criminal Code (radio police)

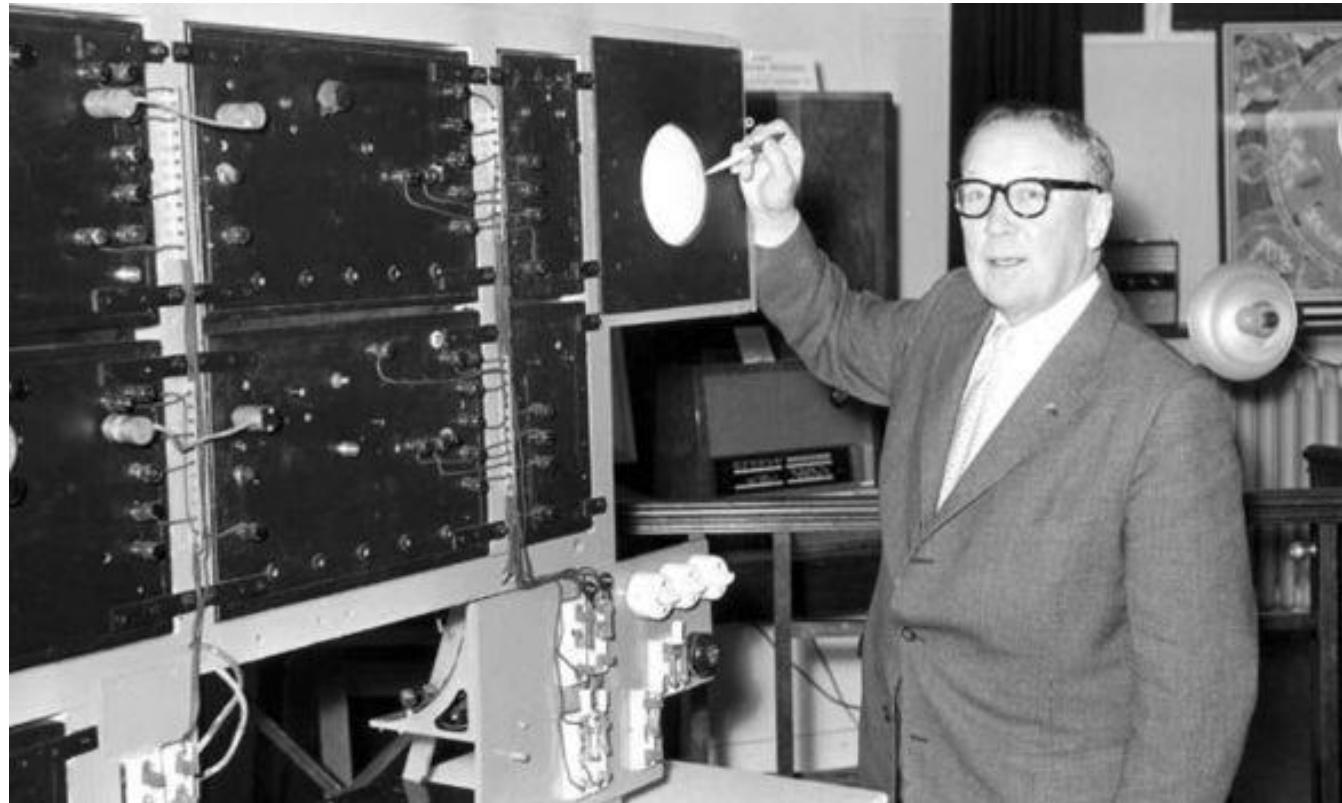


What can go wrong when tampering with ADS-B/C?

- ATC Surveillance malfunction (**lost targets, false targets, targets jumping** around the screen) and consequent wrong decisions by ATCOs
- ATC Services **capacity overload** (aircraft denied airspace entry)
- False contractual CPDLC messages sent to aircraft **to descend, to climb, to turn**
- False TCAS targets causing unnecessary **TCAS descents / climbs**
- Loss of confidence in the systems – users **panic**

Sir Robert Watson-Watt

Invented SSR and XPDR in 1935, Modes 1-4, A/C and IFF



Picture: Daily Express

Mode A/C Classic SSR Transponder (1950)



1030/1090 MHz

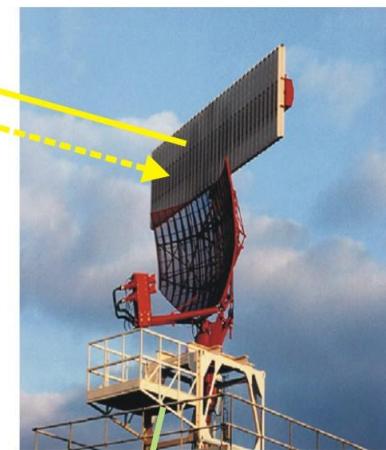
Mode A Interrogation (1030 MHz)
"Who are you?"

Mode C Interrogation (1030 MHz)
"What is your altitude/flight level?"

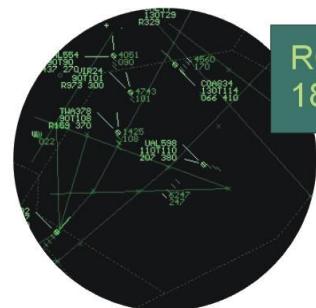
Mode A Reply (1090 MHz)
"My squawk alpha is 3471"

Mode C Reply (1090 MHz)
"My ALT/FL is FL180"

SSR



ATC SCREEN



ROT140
180

TARGET
AIRCRAFT
LABEL



squawk 3471 = ROT140
(from current database)

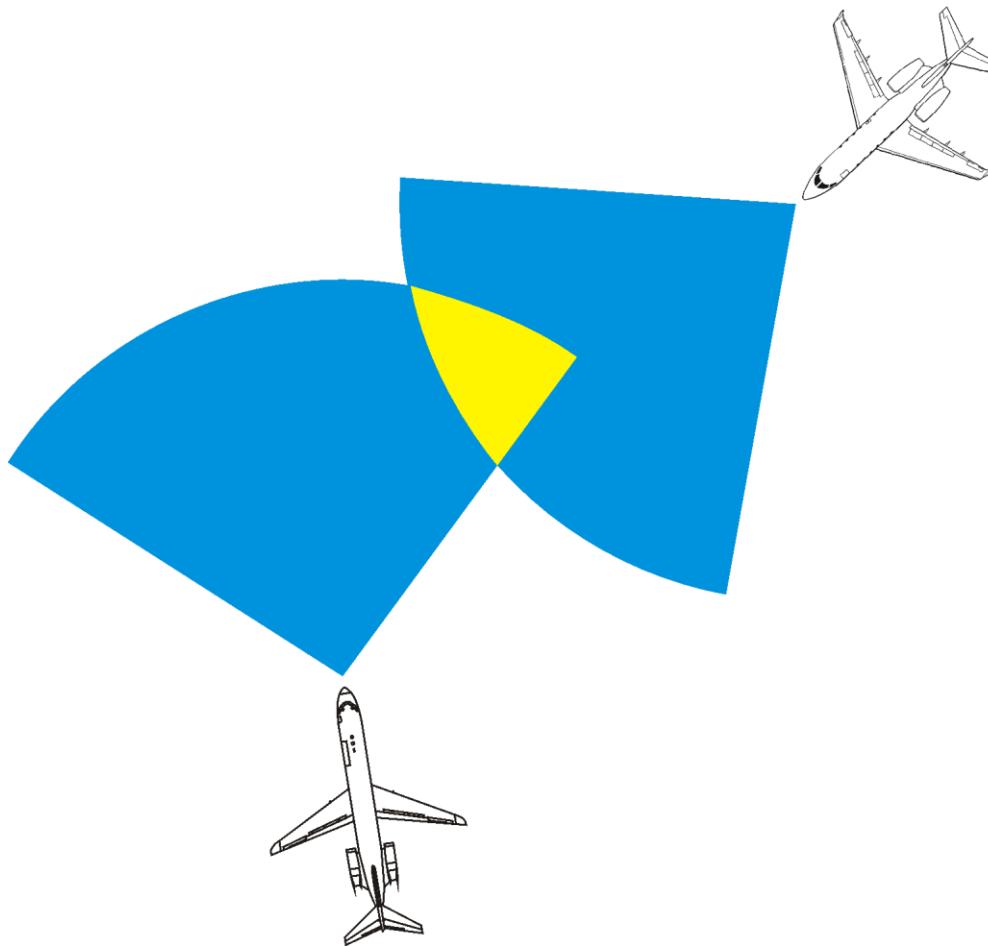
SSR Mode S Information Link (1980)

1030/1090 MHz



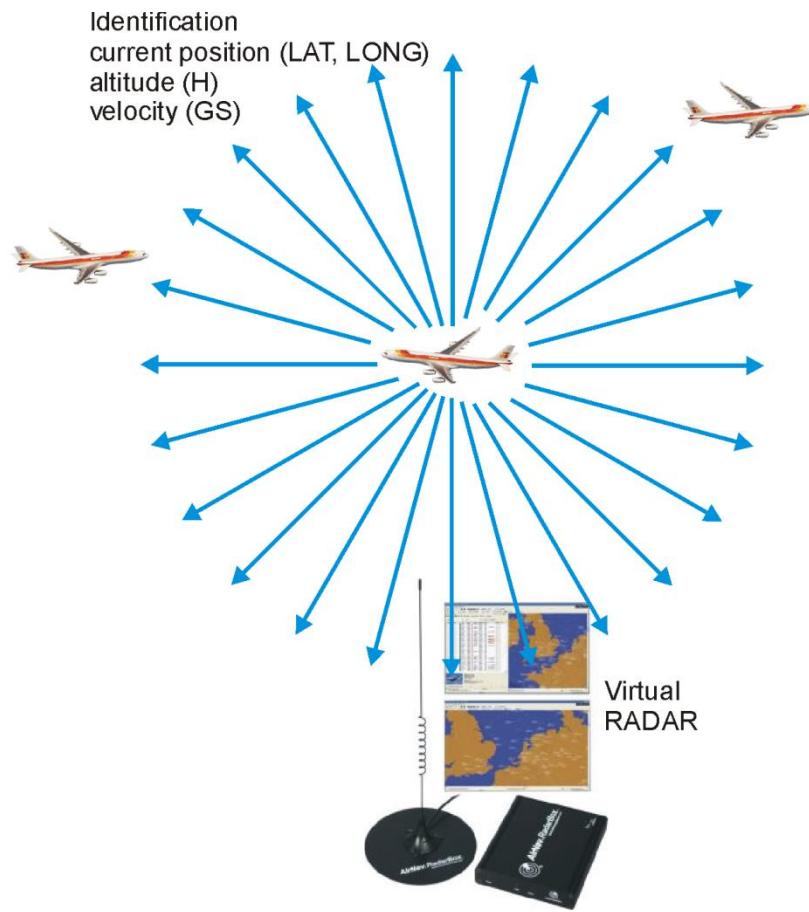
TCAS - Mode S interrogation (1992)

1030/1090 MHz



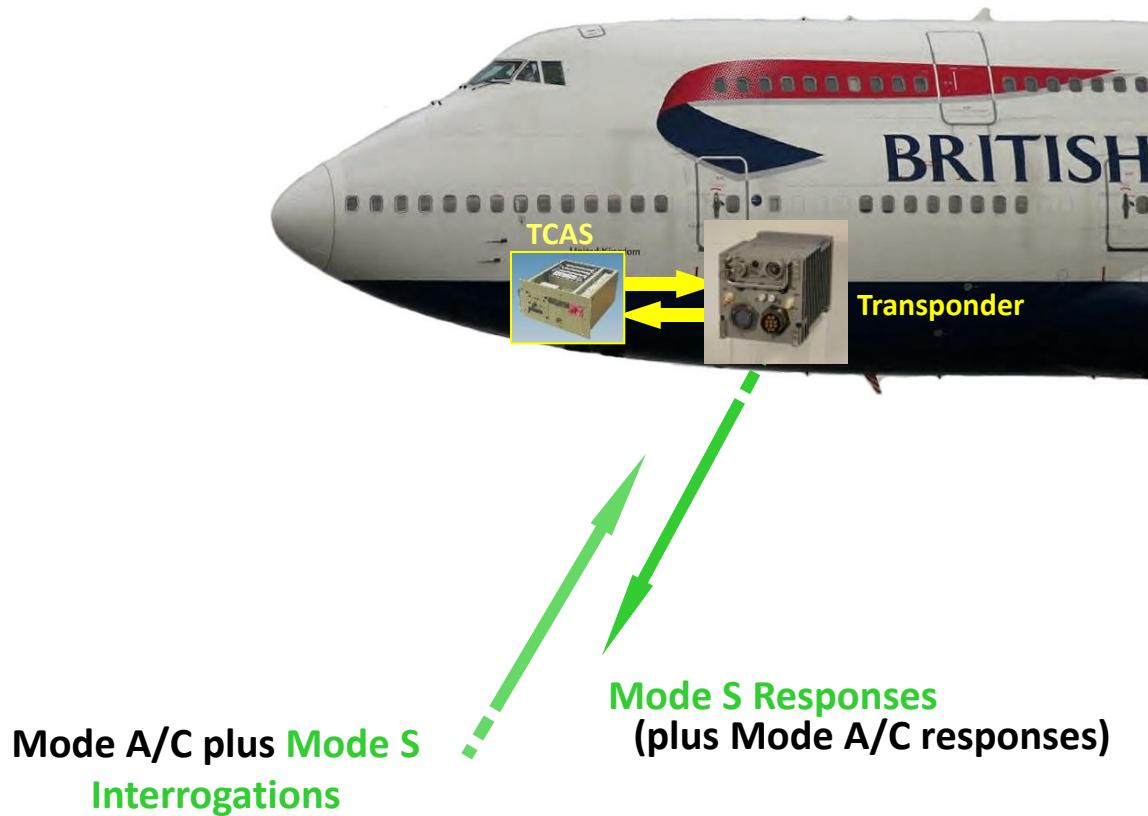
Automatic Dependent Surveillance / Broadcast (ADS/B - 2003)

1030/1090 MHz



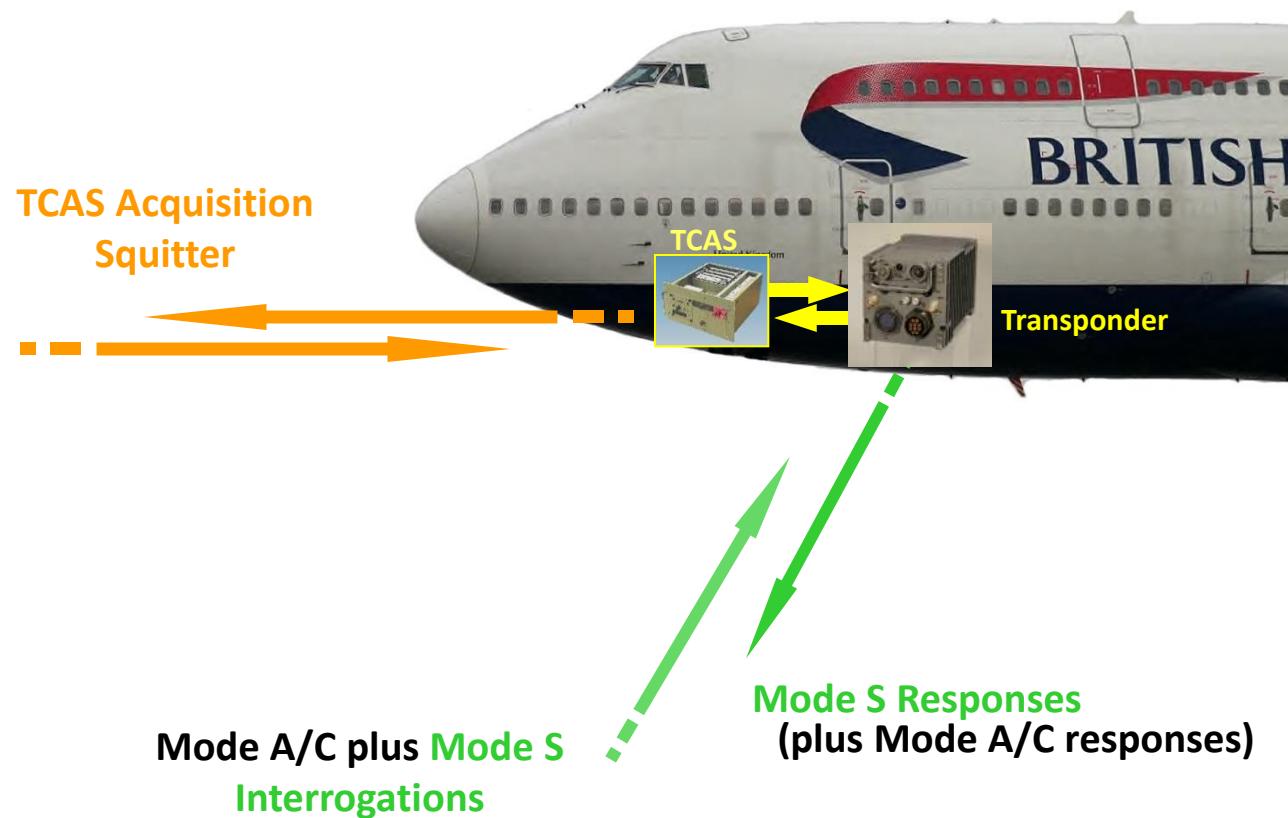
1090 MHz
Extended Squitter

Mode S Transponder



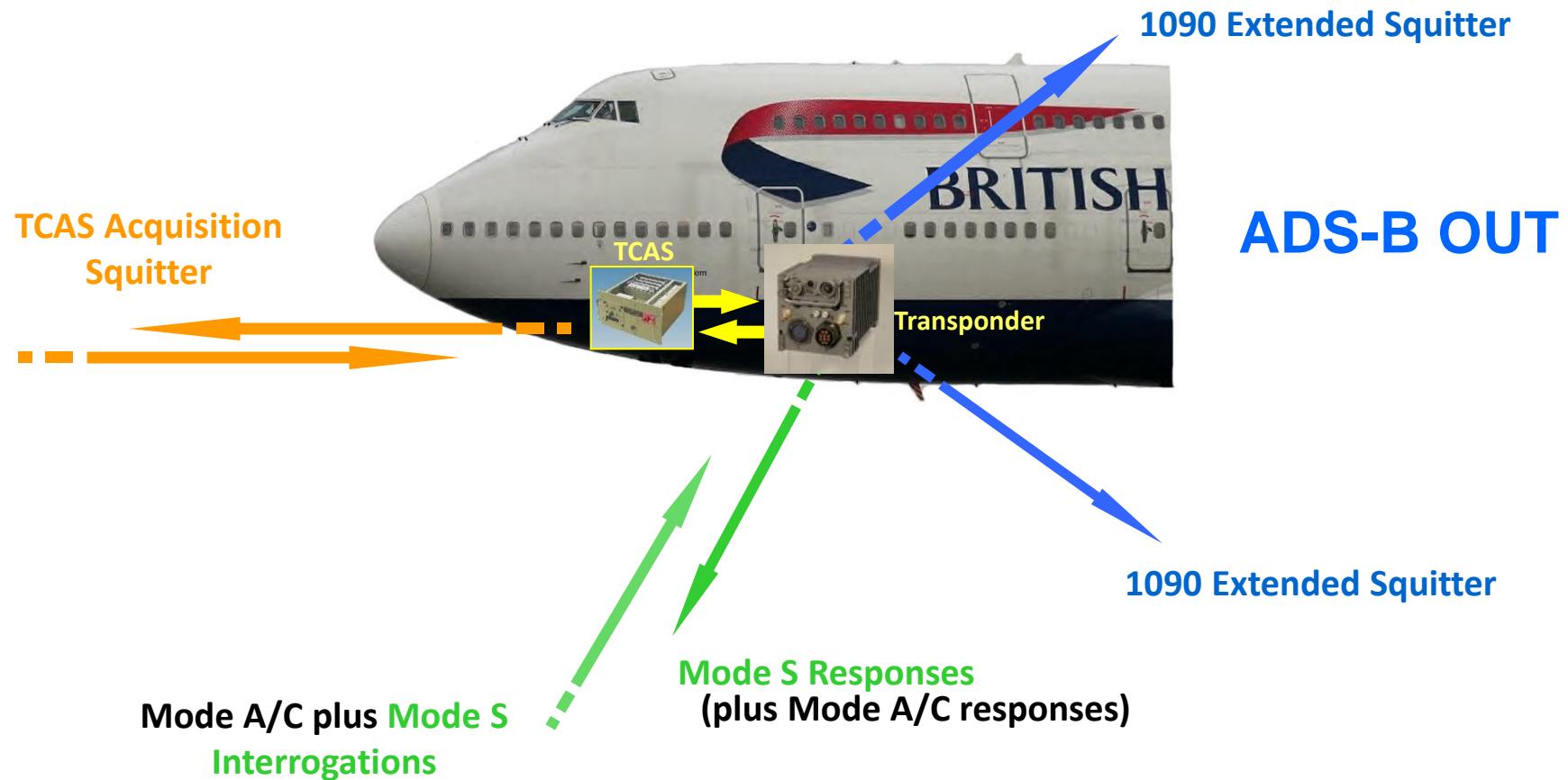
Source: Raytheon

Mode S Transponder (Level 2)



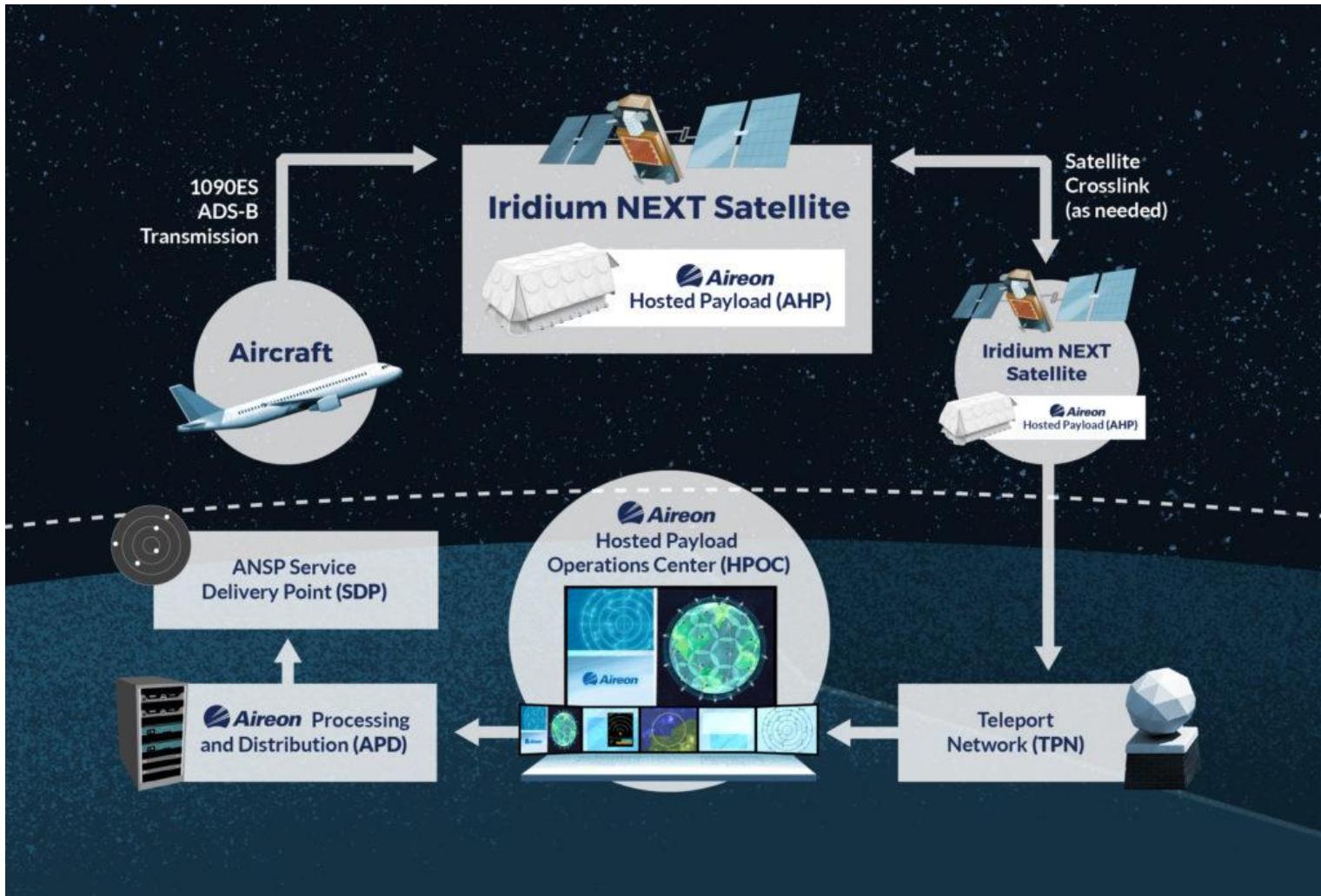
Source: Raytheon

Mode S Transponder (Level 2e)



Source: Raytheon

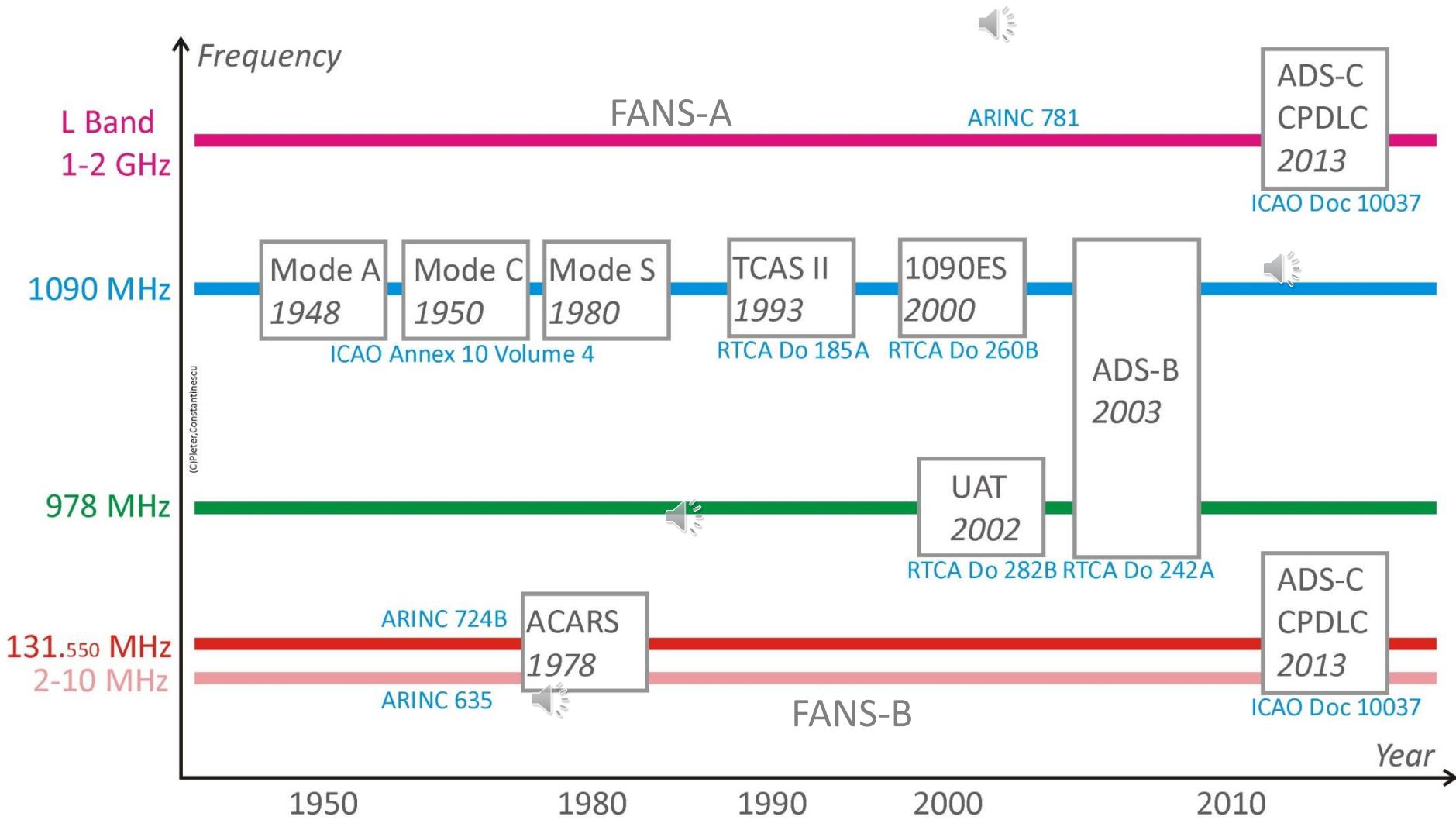
Global ADS/B Tracking by Aireon



Source: Aireon

ADS-B and ADS-C

FANS Future Air Navigation Systems Data Link



Global Data Center Datalink Coverage

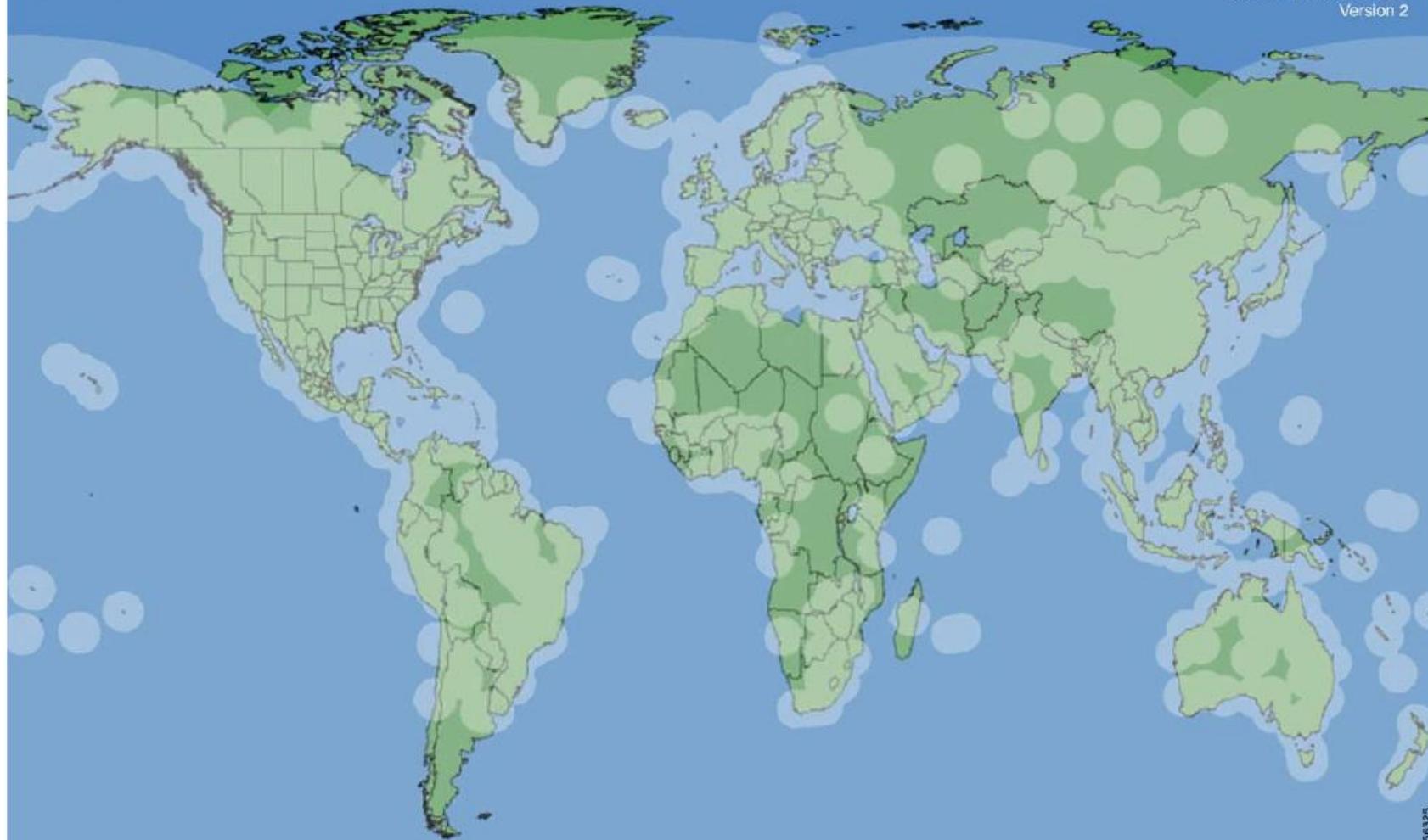
Honeywell

-  VHF Coverage at FL300
-  Satellite Coverage

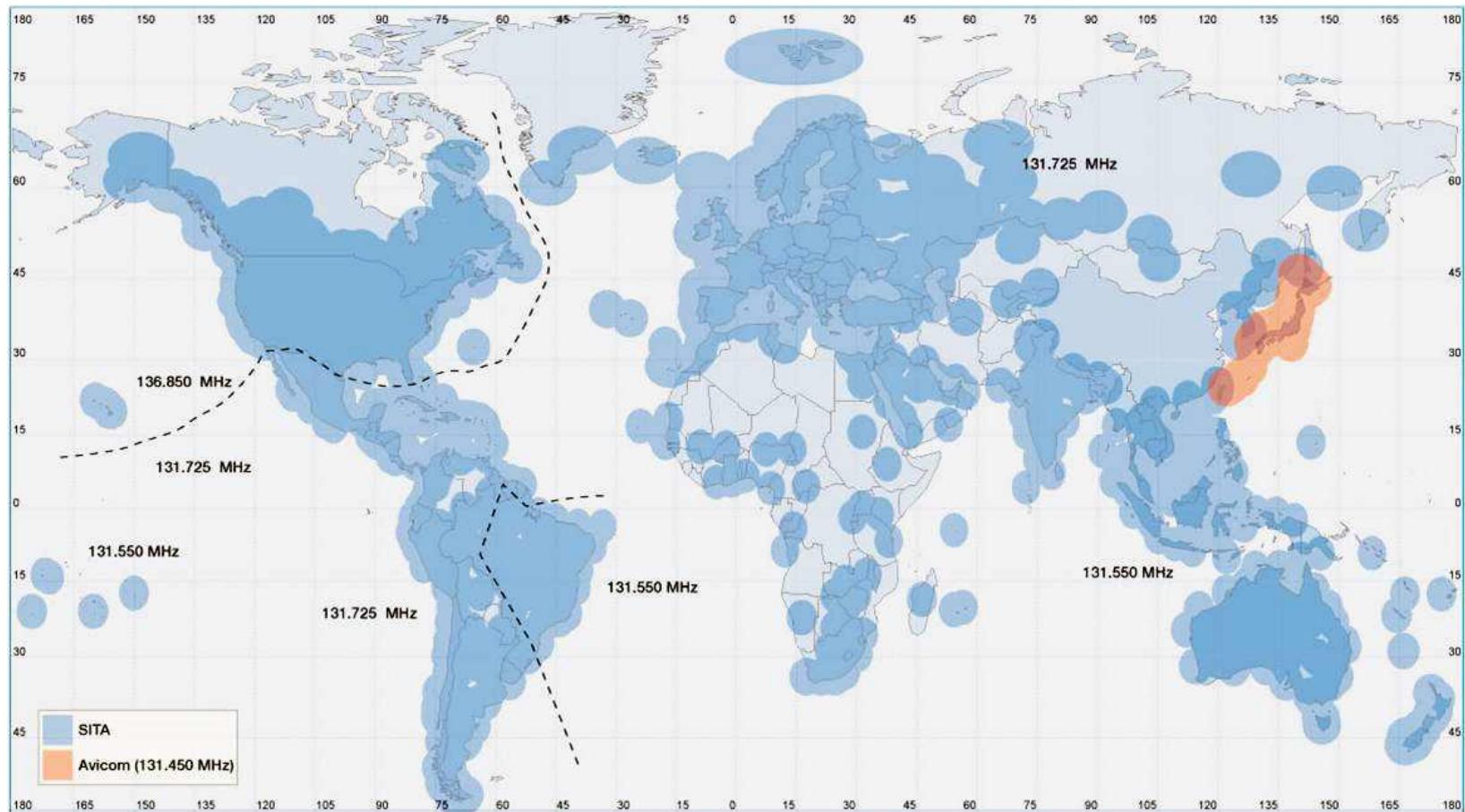
All datalink transmissions require line of sight to a VHF ground station or satellite.

888.634.3330 telephone
425.885.8100 telephone
425.885.8930 facsimile
www.mygdc.com
gdc@honeywell.com

Document 176-9001-999
Version 2



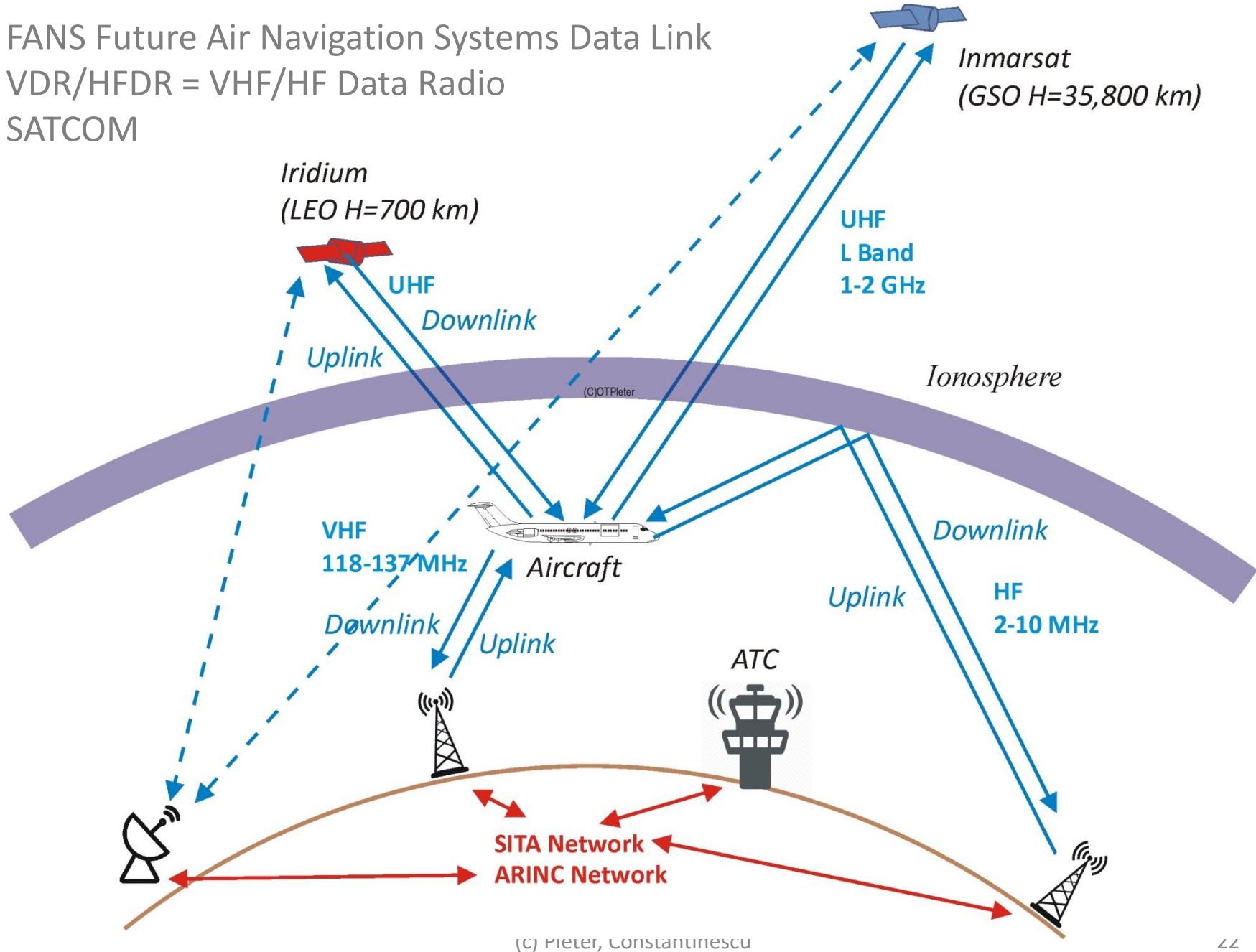
SITA VHF Coverage



FANS Future Air Navigation Systems Data Link

VDR/HFDR = VHF/HF Data Radio

SATCOM



FANS Future Air Navigation Systems Data Link

HF	VHF	SATCOM Inmarsat	SATCOM Iridium
Sky Wave	Line of sight	Line of sight	Line of sight
Long range	Short range	Global except poles	Global
Poor quality (interference fading)	Good quality	Good quality	Good quality
Slow speed	Medium speed	High speed	High speed
Low cost	Low cost	Expensive	Very expensive

VDL-M2 VHF Data Link Mode 2

VDL-M2 or VDL2 is a means of sending information between aircraft and ground stations

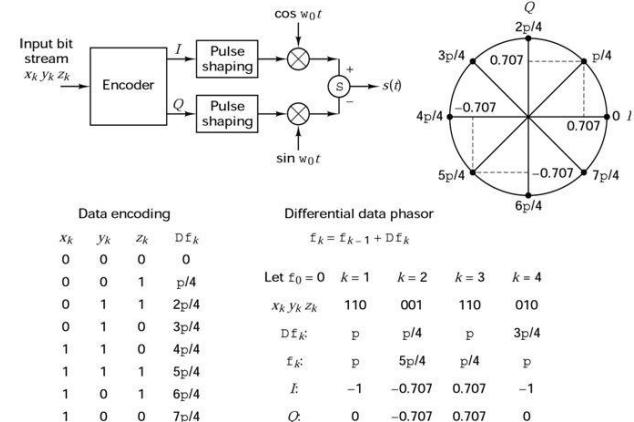
- ICAO Annex 10 Vol III Communication Systems
- EUROCONTROL Manual on VHF Digital Link (VDL) Mode 2

VDL-M2 is the only VDL mode being implemented operationally to support Controller Pilot Data Link Communications (CPDLC).

An extension to the AVLC* protocol permits ACARS over AVLC (AOA) transmissions.

D8PSK (Differentially Encoded 8-Phase Shift Keying) 31.5 kbps speed at 25 kHz bandwidth and 10500 Bd

D8PSK Modulator



Dept. of EE, NDHU

23

*) AVLC = Aviation VHF Link Control

Controller Pilot Data Link Communications (CPDLC)

CPDLC is an electronic communication link between air traffic controllers and pilots. The messages are digitally displayed in the cockpit.

CPDLC messages air-to-ground may follow a standard phraseology or may be free-text.

CPDLC messages ground-to-air normally follow a standard format. Response is required to most messages.

Communication procedures are detailed in ICAO Annex 10 Volume III Part 1 Chapter 3. The CPDLC message set is contained in ICAO Doc 4444: PANS-ATM, Annex 5.

CPDLC use FANS A/B as data link

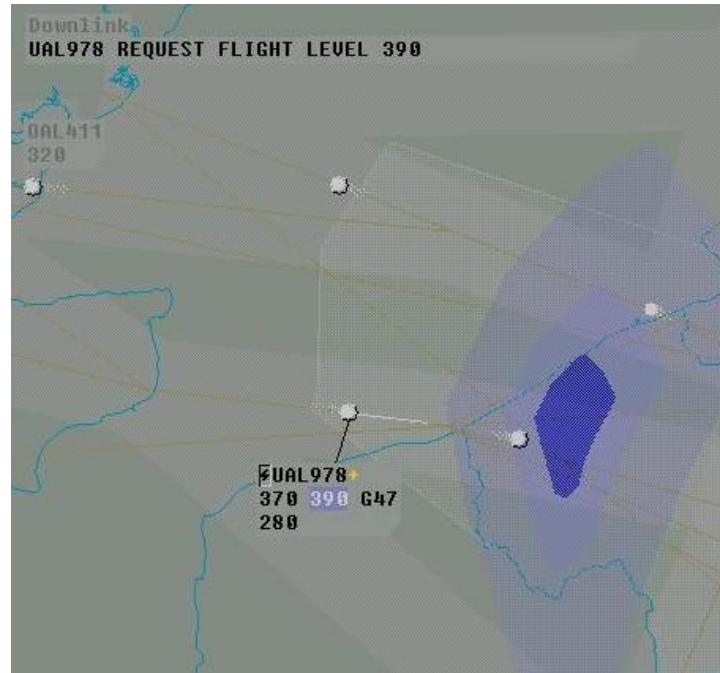
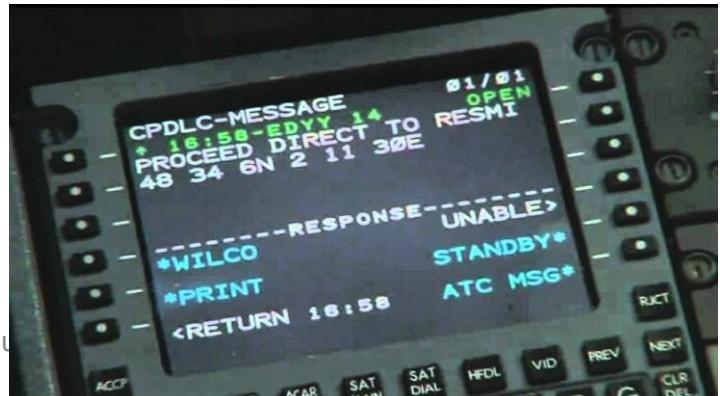
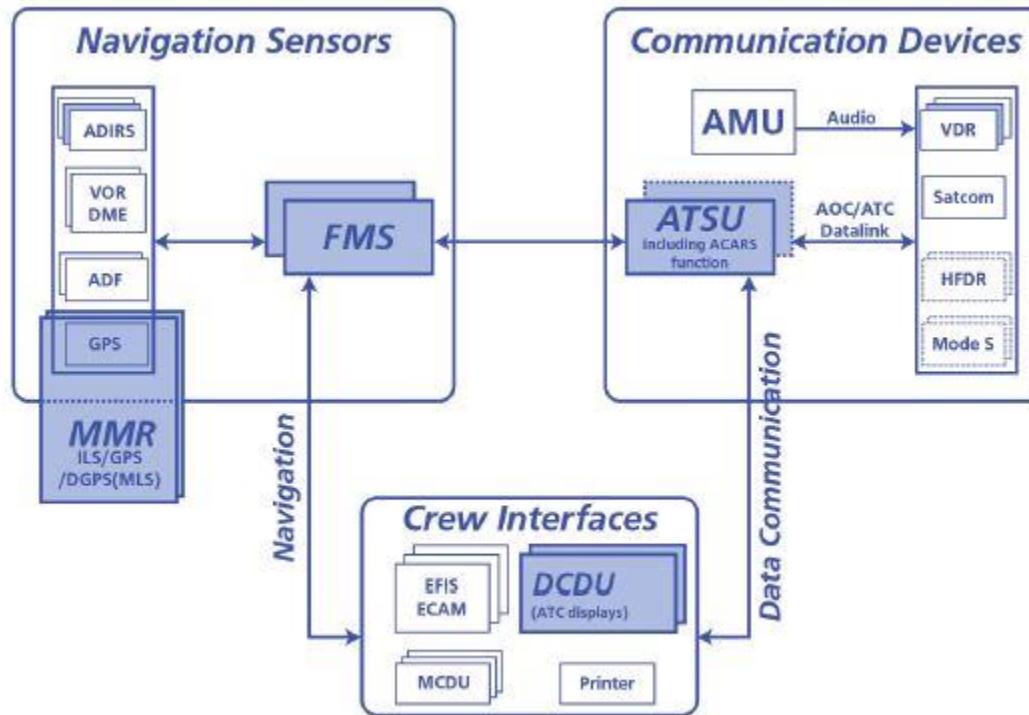


Photo: Telenet.be / CPDLC



CPDLC Architecture



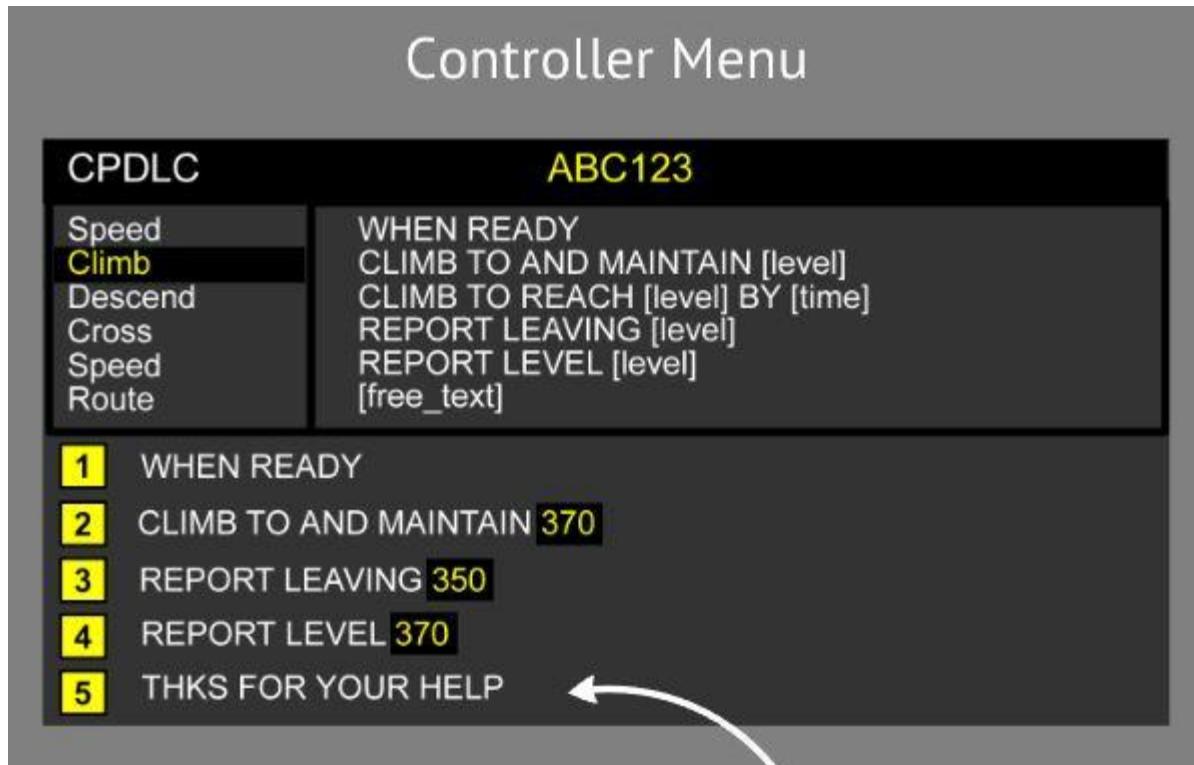
MMR = Multi Mode Receiver

AMU = Audio Management Unit

ATSU = Air Traffic Service Unit

Source: Oxford Aviation ATPL Instrumentation

CPDLC – Controller Interface

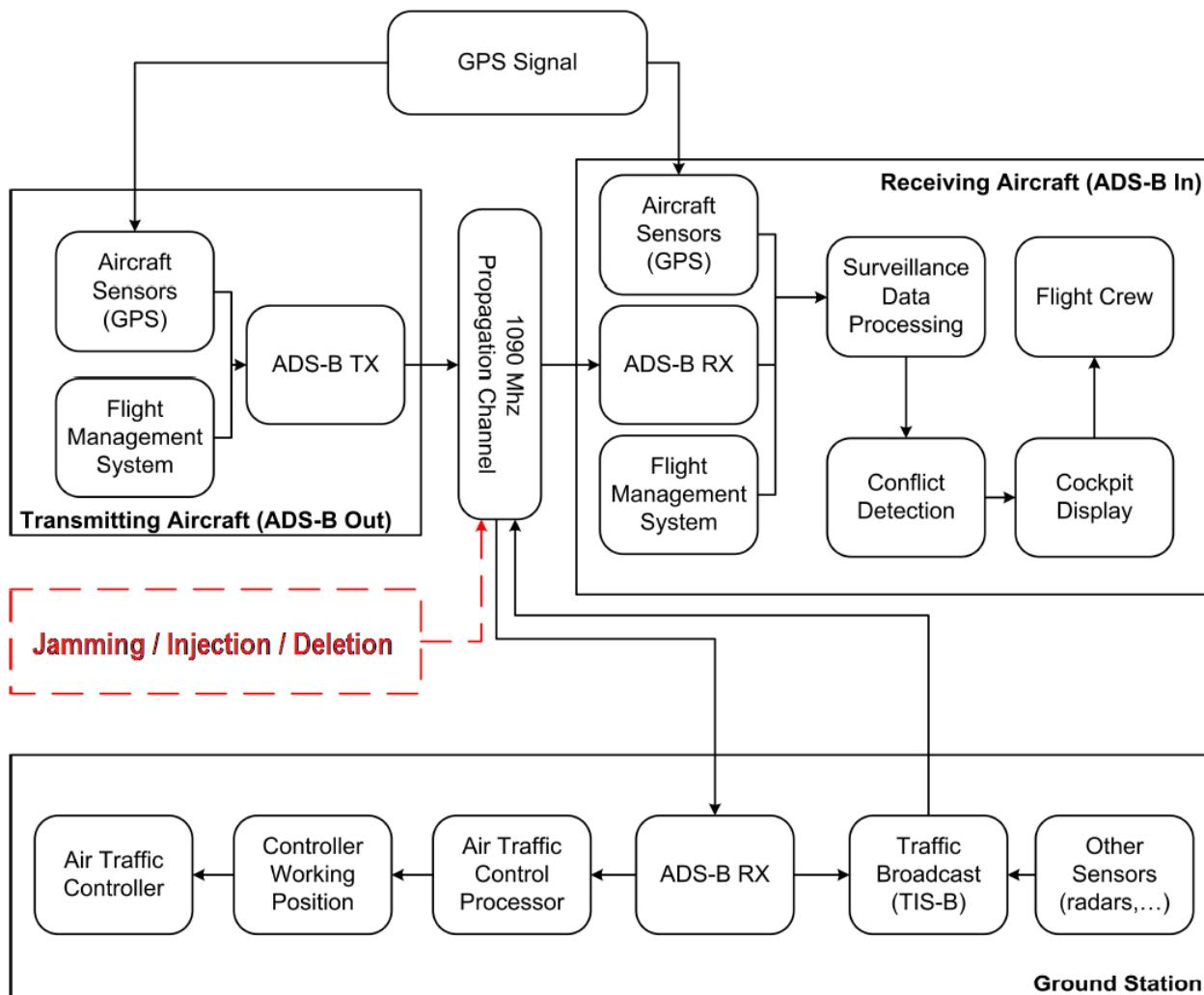


CPDLC – Pilot Interface



Photo: Oxford Aviation ATPL Instrumentation

ADS-B and ADS-C Vulnerabilities

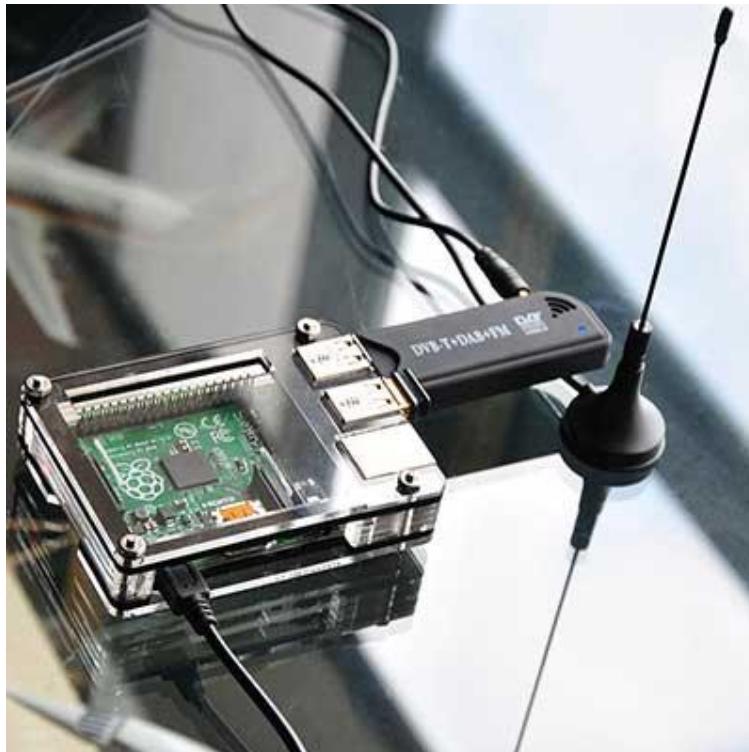


ADS-B and ADS-C Vulnerabilities

- **Eavesdropping**, i.e., listening to the unsecured broadcast transmissions: it is impossible to be prevented without applying encryption and, of course, it is impossible to be detected;
- **Jamming**, i.e., the intentional transmission of high power harmful signals in the RF channel in order to disable the air–ground communication: for a single receiver or in a particular geographical area, this type of attack may create denial-of-service problems at any ATC;
- **Message injection (or spoofing)**, i.e., the intentional transmission of signals with the same protocol but with misleading information;
- **Message deletion** by SSR reply garbling / PI violation: legitimate messages can be “deleted” or manipulated by the superposition of false message with relative higher power.

~~Eavesdropping~~

Reception of 1090ES was made possible by development in software defined radio (SDR) on very cheap generic hardware.



Piaware hardware

Receiving a radio message intended for another person is a legal offence in many countries (including Romania)

Since ADS-B is a reception-only operation it is untraceable

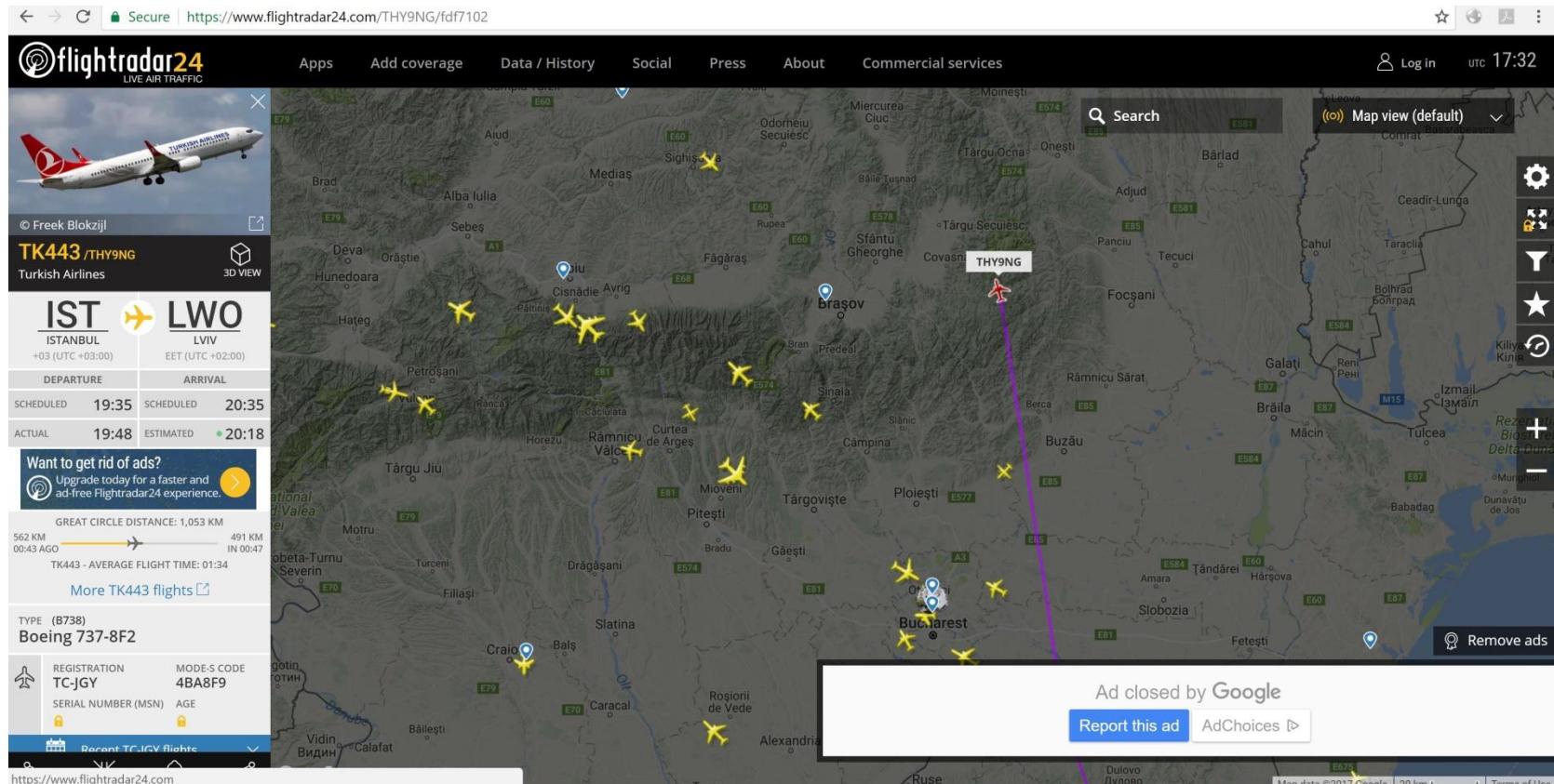
“Broadcast” is by definition:

- 1:** cast or scattered in all directions
- 2:** made public by means of radio or television
- 3:** of or relating to radio or television broadcasting

(Myriam-Webster Dictionary)

FlightRadar24

<https://www.flightradar24.com>



(c) Piepter, Constantinescu

Global ADS-B Exchange

<https://www.adsbexchange.com/>

https://global.adsbexchange.com/VirtualRadar/desktop.html

TC-JGY
Turkish Airlines
Turkey
Boeing 737NG 8F2/W

4BA8F9

Altitude: 38000 ft Speed: 464.0 kts Heading: 352.0° Vertical Speed: 0 ft/m Squawk: 6335 Species: Landplane Transponder: ADS-B Latitude: 45.39569° Longitude: 26.54377°

Route:
LTBA Atatürk, Istanbul, Turkey
UKLL Lviv, Ukraine

Interesting: No User Tag: 0 Flights Count: 1,378 MLAT: No Message Count: 1,378 Time Tracked: 40:44 Avg. Signal Level: Operator Code: THY

Image Search :: FlightAware :: airport-data.com :: airliners.net :: airframes.org :: PlaneLogger.com :: Update Database :: Past Flights
Show on map :: Enable auto-select

Tracking 13 aircraft (out of 7,535)

Flag	Silhouette	Type	Callsign	Reg.	Altitude	Speed	Squawk	Civ/Mil	Country	Model	M
BRITISH AIRWAYS		B789	BAW35	G-ZBK6	37000 ft	507.0 kts	2716	Civil	United Kingdom	Boeing 787 9	N
QATAR		B773	QTR5ML	A7-BEG	35975 ft	470.0 kts	2211	Civil	Qatar	Boeing 777 3DZER	N
Emirates		B773	UAE125	A6-EGJ	38000 ft	463.0 kts	2363	Civil	United Arab Emirates	Boeing 777 31HER	N
TURKISH AIRLINES		B738	THY9NG	TC-JGY	38000 ft	464.0 kts	6335	Civil	Turkey	Boeing 737NG 8F2/W	N
RYANAIR		B738	RYR5TF	EI-DYV	37000 ft	448.0 kts	6426	Civil	Ireland	Boeing 737NG 8AS/W	N
blue		B738	BMS3102	YR-BMI	27000 ft	409.0 kts	4044	Civil	Romania	Boeing 737NG 8K5/W	N
Emirates		A388	UAE23E	A6-EDV	37000 ft	518.0 kts	3440	Civil	United Arab Emirates	Airbus A380 861	N
Emirates		A388	UAE4CK	A6-EEE	38000 ft	484.0 kts	3242	Civil	United Arab Emirates	Airbus A380 861	N
AEGEAN		A320	AEE963	SX-DVS	14025 ft	307.3 kts	5407	Civil	Greece	Airbus A320 232	N
		A320	W771SF	HA-IVA	28425 ft	406.0 kts	5420	Civil	Hungary	Airbus A320 232SI	N

Flight Aware

<https://flightaware.com/>

Join FlightAware (Why Join?) Login English (USA) 12:33PM EST

All Search for flight, tail, airport, or city Track FORGOT THE FLIGHT NUMBER?

LIVE FLIGHT TRACKING PRODUCTS ADS-B PHOTOS SQUAKWS DISCUSSIONS ABOUT CONTACT

 FlightAware

Turkish Airlines 443 THY443 / TK443

EN ROUTE AND ON TIME
Landing in 46 minutes

IST
ISTANBUL, TURKEY
took off from
[Istanbul Ataturk Int'l - IST](#)

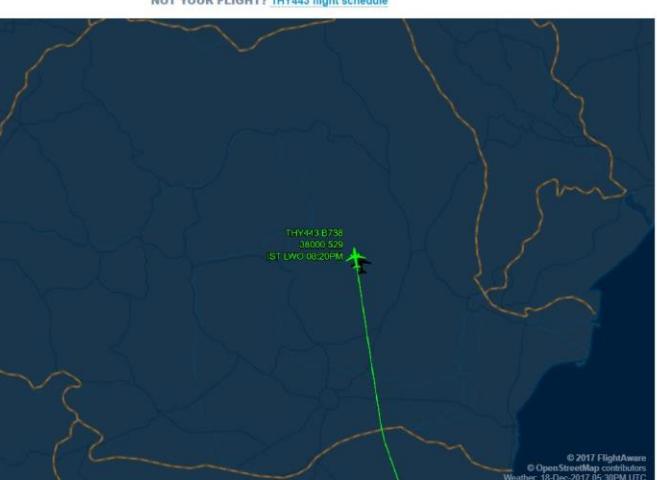
MONDAY 18-DEC-2017
07:35PM +03 (on time)

59m elapsed 358 mi flown

1h 45m total flight time

46m remaining 297 mi to go

NOT YOUR FLIGHT? [THY443 flight schedule](#)



THY443 B738
IST LWO 08:20PM

© 2017 FlightAware. All rights reserved. Weather: 18-Dec-2017 05:30Z in UTC

En Route Replay Speed 10x

ALTITUDE (ft) 40,000 20,000 0 38,000 ft 529 mph

IST 07:48PM +03 LWO 06:48PM EET

08:30PM +03 07:30PM EET

09:00PM +03 08:00PM EET

09:20PM +03 08:20PM EET

0 500 1,000 (feet)
Speed (ft/min)

File Speed

Activity Log

EN ROUTE FLIGHT

Date	Departure	Arrival	Aircraft	Duration
Monday 18-Dec-2017	07:35PM +03 Istanbul Ataturk Int'l - IST	08:20PM EET Lviv Int'l - LWO	B738	1h 45m

Flight Details updated 30 seconds ago

[View track log](#) [Track inbound plane](#)

DEPARTURE TIMES

	Gate Departure	Taxiing	Takeoff
Actual	07:35PM +03	13 minutes	07:48PM +03
Scheduled			07:35PM +03

Average Delay Less than 10 minutes

ARRIVAL TIMES

	Landing	Taxiing	Gate Arrival
Estimated	08:20PM EET	-----	
Scheduled	08:07PM EET ⓘ		

Average Delay Less than 10 minutes

AIRCRAFT INFORMATION

Aircraft Type **Boeing 737-800 (twin-jet) (B738)** [Photos](#)

AIRLINE INFORMATION

Airline **Turkish Airlines "Turkair"** [all flights](#)

FLIGHT DATA

Speed **529 mph (Planned: 394 mph)** [graph](#)

Altitude **38,000 ft** [graph](#)

Distance **Direct: 665 mi**

Route —

TOP BOEING 737-800 (TWIN-JET) PHOTOS

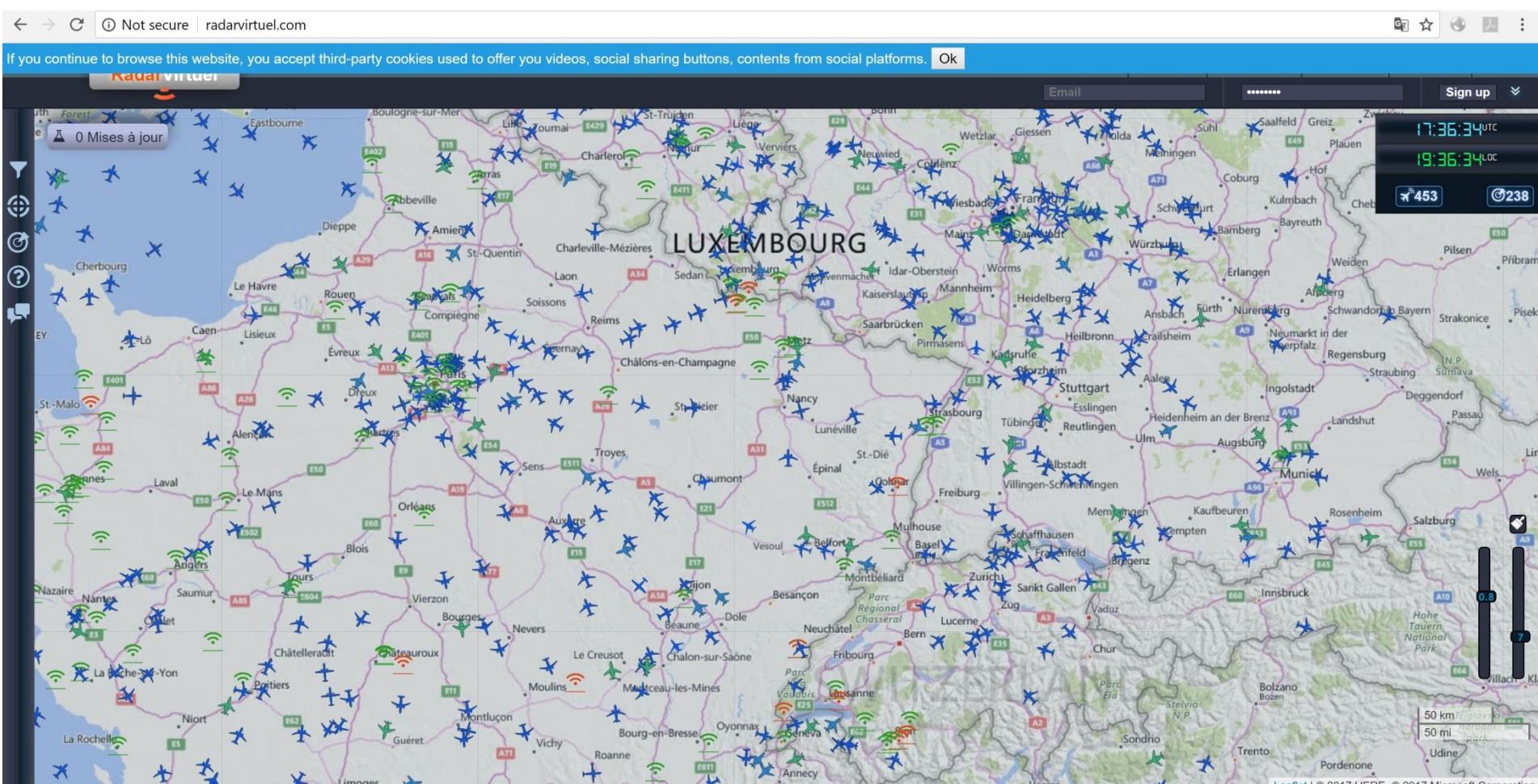


[view all photos](#)

[Report inaccuracies on this page](#)

RadarVirtual

<http://radarvirtuel.com/>



Jamming

- Is a brute force “denial of service attack”.
- Also affect all SSR modes and can partially affect non-military PSR.
- Must be done near receiver or with very high power
- Is immediately detected and the jamming device can be located with precision
- There are usually many distributed ADS-B receivers for ATC purposes, so it takes considerable effort to completely blackout a given area
- A targeted attack would create major denial-of-service problems at any airport.
- Jamming moving aircraft is also possible, however considered more difficult.

Message injection

- 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.
- One can conduct an attack with limited knowledge and very cheap and simple technological means which have been easily and widely available for some time.



30dBm SDR transceiver

- As a 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.

Message deletion

- ADS-B messages contain aircraft address at the beginning. A receiver can target a given address by listening and very short burst-jamming.
- If done quick enough, constructive interference will cause 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.
- It is more subtle than complete jamming of the 1090MHz frequency and may not be immediately detected.
- Besides aircraft “disappearance”, message deletion in conjunction with message injection is key to ATC manipulation.



Software suite for SDR

- While the original message is effectively destroyed by interference, depending on the implementation and the circumstances the receiver might at least be able to verify that a message has been sent.

ADS-B - How to manipulate the ATC console?

- Use a SDR transceiver (and matching software)
- Position such as:
 - ADS-B signal coming from aircraft are of comparable power or less then own signal at receiver position.
 - The time-of-arrivals delay between aircraft signals and own signals is less then the remaining duration of the ADS-B message after ICAO address.
- Listen for ADS-B messages originating from target aircraft. Delete them.
- Inject new message with target aircraft address and fake position, taking care not to “jump”.
- If properly implemented in software one can fake a large number of planes simultaneously with a single device!

Satisfying the requirements

- Mode S transponder transmitting impulse power is typically 125-500W (51-57dBm) as imposed by ICAO Annex 10 Vol IV AL77.
- HackRF maximum transmitting power is 1W (30dBm)
- Using free space path loss formula:

$$FSPL(dB) = 10 \cdot \log_{10} \left(\left(\frac{4\pi \cdot d \cdot f}{c} \right)^2 \right) = 20 \cdot \log_{10}(d) + 20 \cdot \log_{10}(f) - 147.55$$

- Imposing equal power at the receiver (D_a is the distance between aircraft and receiver and D_f is the distance from attacker (fake) to the receiver):

$$20 \cdot \log_{10} \left(\frac{D_a}{D_f} \right) = 51 - 30$$

- To be able to erase an airplane the attacker must be at least 11 times closer to the receiving antenna (i.e. to erase an airplane 100km away one needs to be at no more than 9km from the antenna)

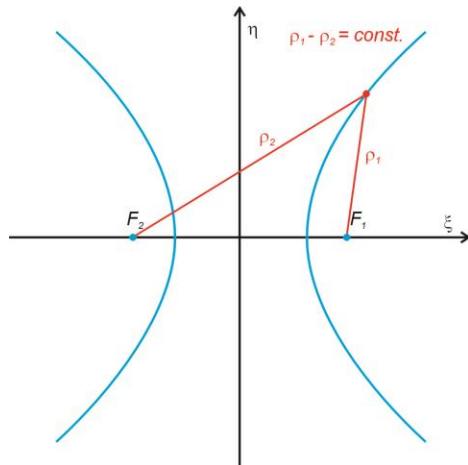
Satisfying the requirements

- The second condition impose that the difference in time of arrival between direct and fake signal must be less than 70us.
- That translate to a difference in distance of 21Km
- If the first condition is fulfill then the maximum difference is 18km, and so all aircraft far enough are erasable
- If the attacker can increase the transmitter power (and move further away) then only aircraft inside a hyperbola can be erased

To be effective an attacker has to be as close as possible form the receiving antenna (within 1-2km). Power is not an issue as distances more than 10.5km will not allow full console manipulation.

Immediate Countermeasure: ADS-B Multiple Receiving Antennas (Distributed Reception)

1. Multiple receiving antennas discourage / makes difficult a jamming attack
2. Multilateration may be performed to provide an independent positioning of the target



$$\frac{\xi^2}{a^2} - \frac{\eta^2}{b^2} = 1$$

$$a = \frac{t_1 \cdot c_0}{2}$$

$$b = \sqrt{\frac{(x_1 - x_2)^2 + (y_1 - y_2)^2}{4} - a^2}$$

TDOA =
Time
Difference
of Arrival

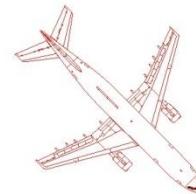
Immediate Countermeasure: ADS-B Kalman Filtering for position continuity

A legitimate target cannot jump from a position to another, it needs to follow a flight dynamics model (e.g. BADA).

A Kalman filter in the ADS-B surveillance position processing software could detect and discard fake targets.

● ADS-B Receiver Antenna

Fake Target

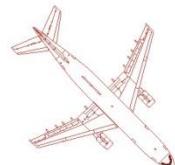


Real Target

● ADS-B Receiver Antenna

● ADS-B Receiver Antenna

Fake Target Position by ADS-B



● ADS-B Receiver Antenna



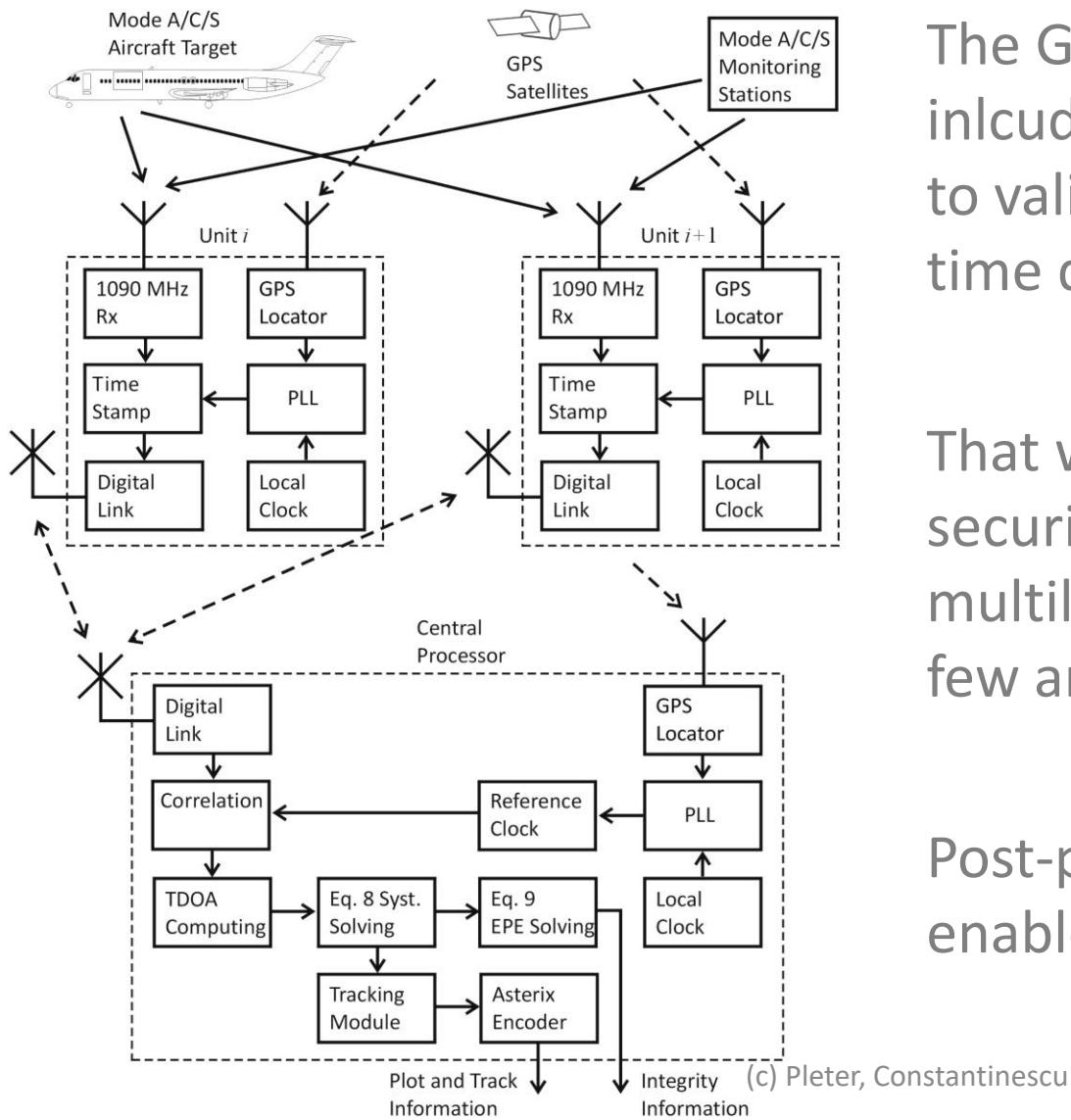
Real Target Position by MLAT+ADS-B
Moves with the Expected Speed
of an Aircraft

● ADS-B Receiver Antenna

● ADS-B Receiver Antenna

● Attack Position by MLAT
Does not move as expected

Medium Term Countermeasure: ADS-B/C Time Stamp included in the message



The GNSS accuracy time stamp included in the message will allow to validate the message by the time difference of arrival.

That would provide a minimal security even in areas where multilateration is not possible (too few antennas).

Post-processing multilateration is enabled.

ADS-B Receiver Antenna

Distance
validated
by Time stamp

Fake Target



Distance
invalidated
by Time stamp

Real Target

Provides instantly the position of
the attack device antenna

Attack
Position

Long Term Countermeasure: ~~Encrypted~~ Authenticated ADS-B/C Messages

A new authenticated standard by ICAO with:

- Private key encoding
- Public key decoding

Each registered aircraft will receive an encryption chip with its ICAO-24 address

Each legitimate Air Traffic Control Service Provider / AFTN Address Owner will receive an encryption chip with its address

