Network Manager
nominated by
the European Commission

EUROCONTROL

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

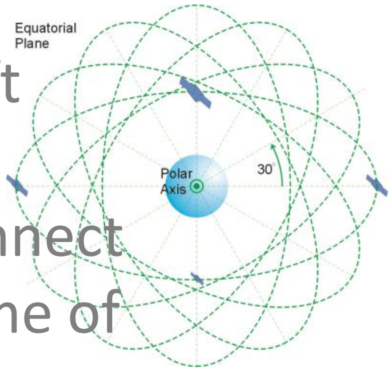
Prof. dr. Octavian Thor Pleter, MBA (MBS)

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

Main Points

- Aircraft are densly packed computer networks flying together everywhere, including some of the most remote / isolated regions of the world **(air segment)**

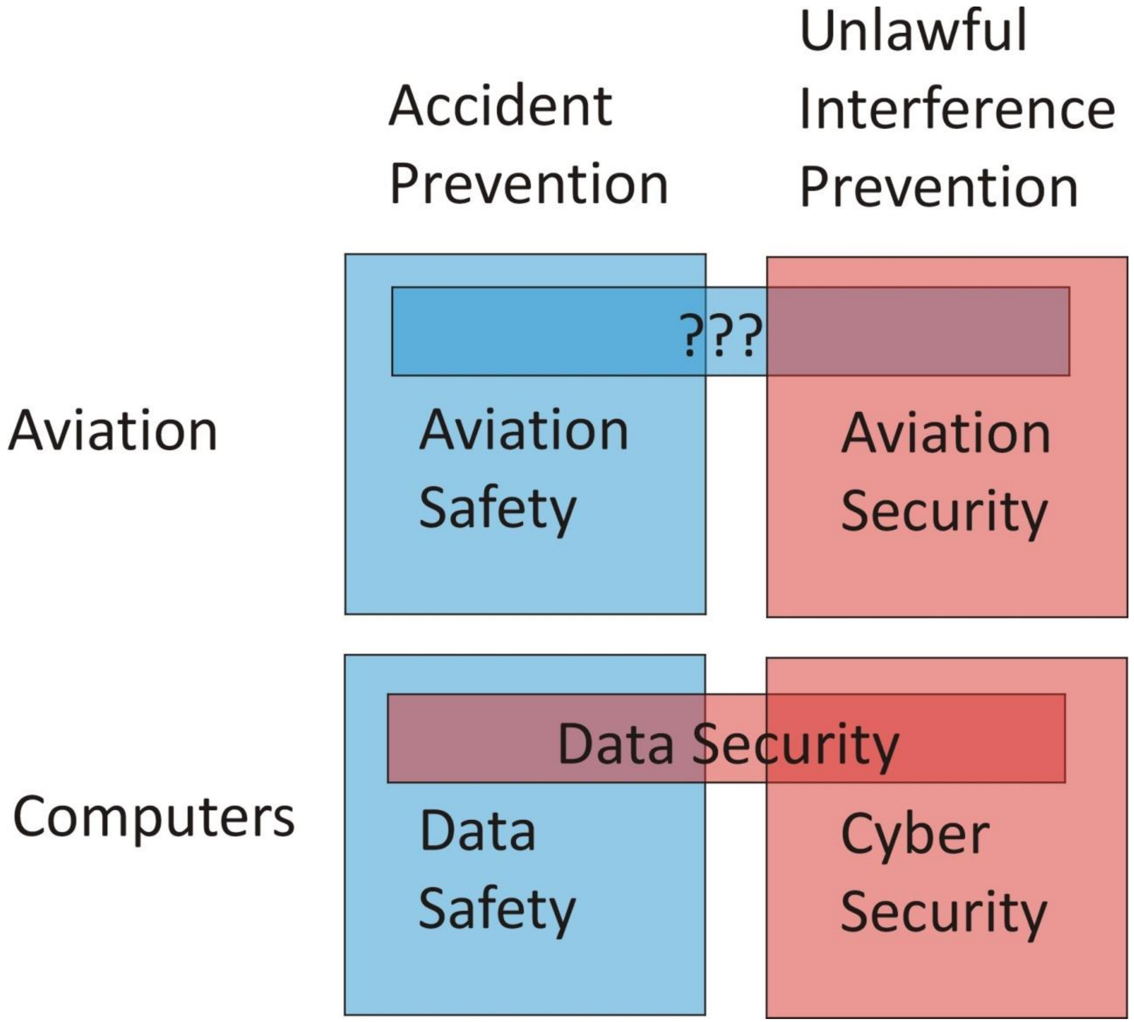
- ATM systems are part of a global ground based computer network **(ground segment)** + a global satellite network **(space segment)**, in need to communicate in real time with the above aircraft



- 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

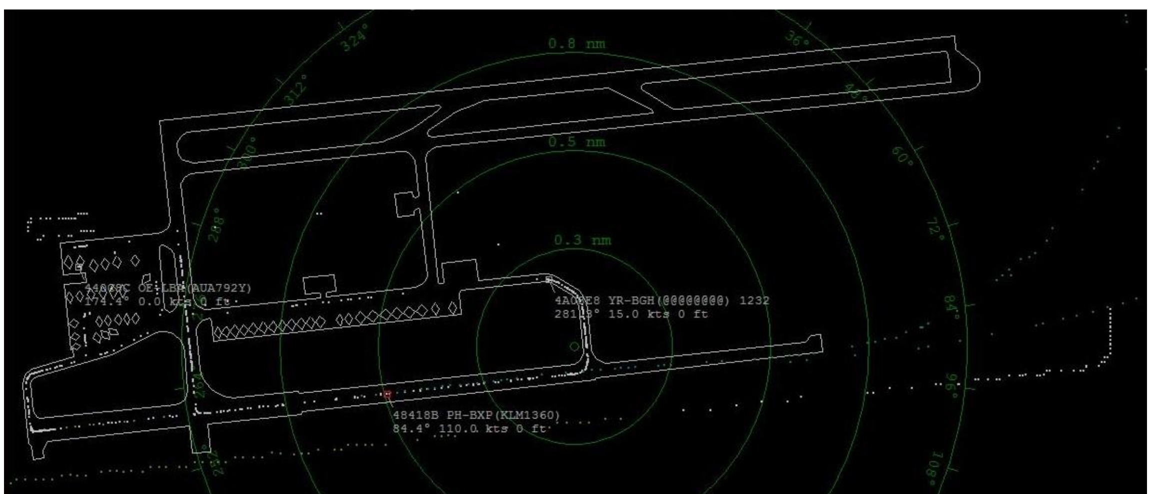
Main Questions

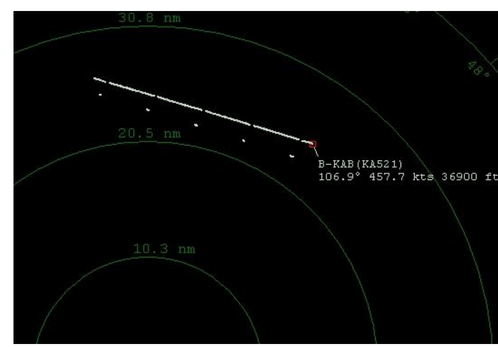
- How do ADS/B and ADS/C work?
- Do they improve on aviation safety and aviation security?
- Do they bring in new threats, such as data security problems or human factors problems (e.g. over-reliance on automation, mistrust in automation)?
- What could go wrong? What are the vulnerabilites?
- Who owns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


Accident
Prevention
Unlawful
Interference
Prevention
???
Aviation
Aviation
Safety
Aviation
Security
Data Security
Computers
Data
Safety
Cyber
Security

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	1. Compare ADS/B position to the SSR position 2. Compare ADS/B position to the runway/taxiway centerline





ADS-B & ADS-C Technology

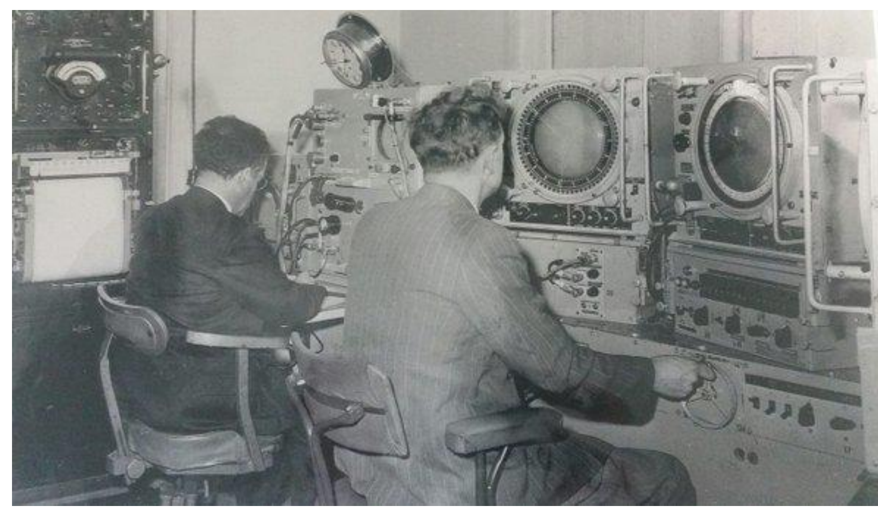
- **A**utomatic - Always ON and requires no operator intervention;
- **D**ependent - Depends on accurate GNSS signal for positioning;
- **S**urveillance - Provides "Radar-like" surveillance services;
- **B**roadcast - It continuously broadcasts aircraft position and other data to any aircraft, or ground station
- **C**ontract – 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)

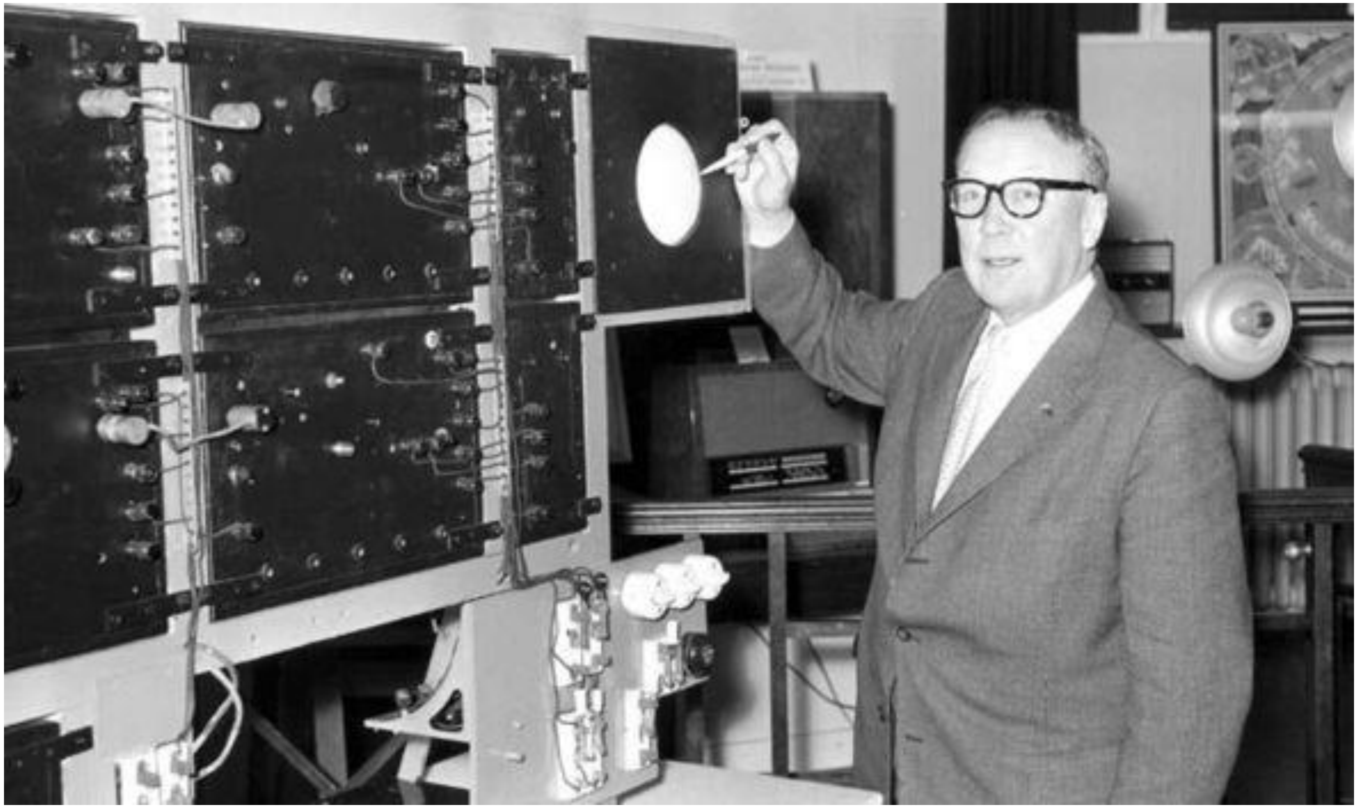
- False contractual CPDLC messages sent to aircraft **to descend, to climb, to turn**

- False TCAS targets causing unnecessary **TCAS descents / climbs**

- Loss of confidence in the systems – users **panic**

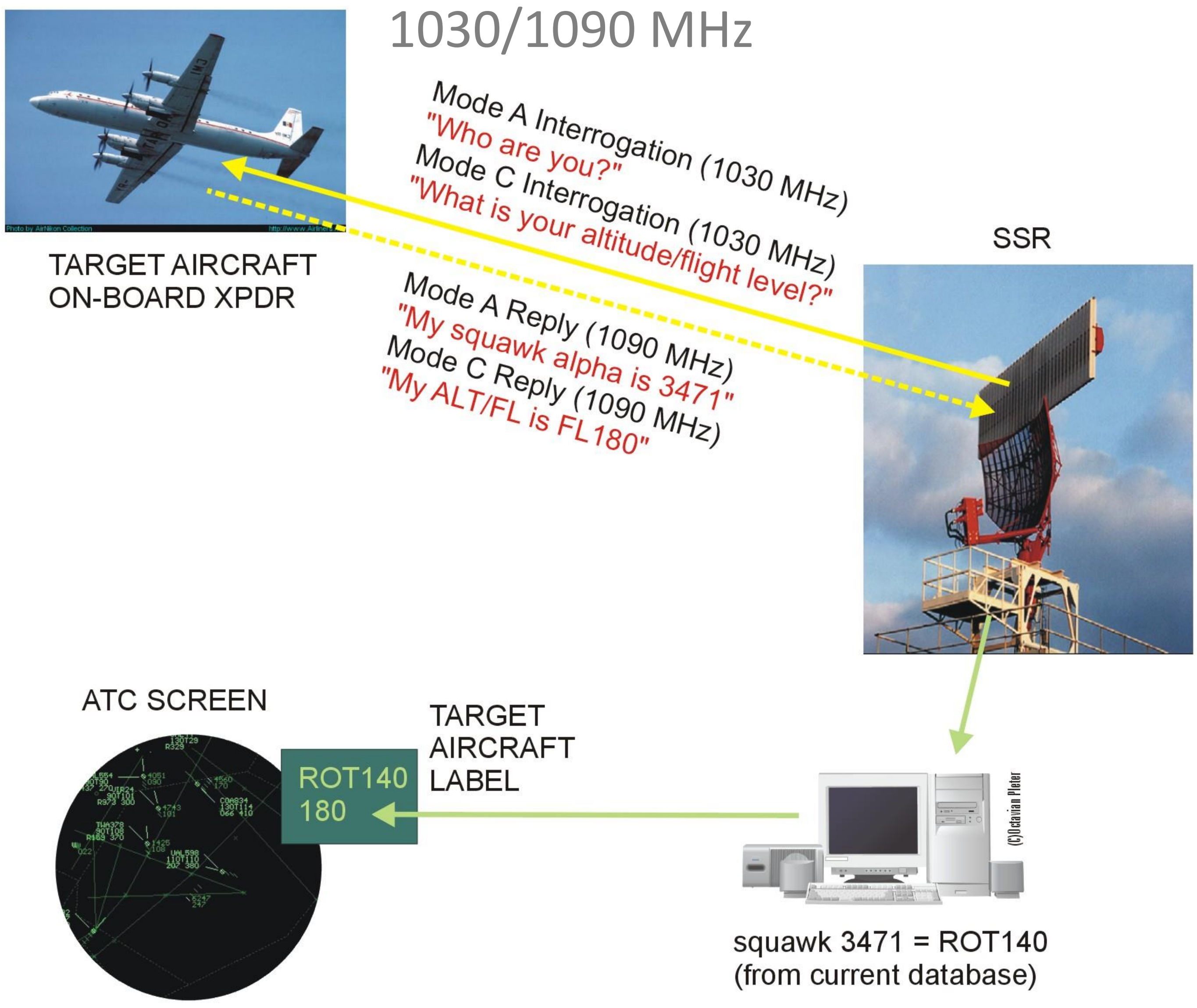
Sir Robert Watson-Watt

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



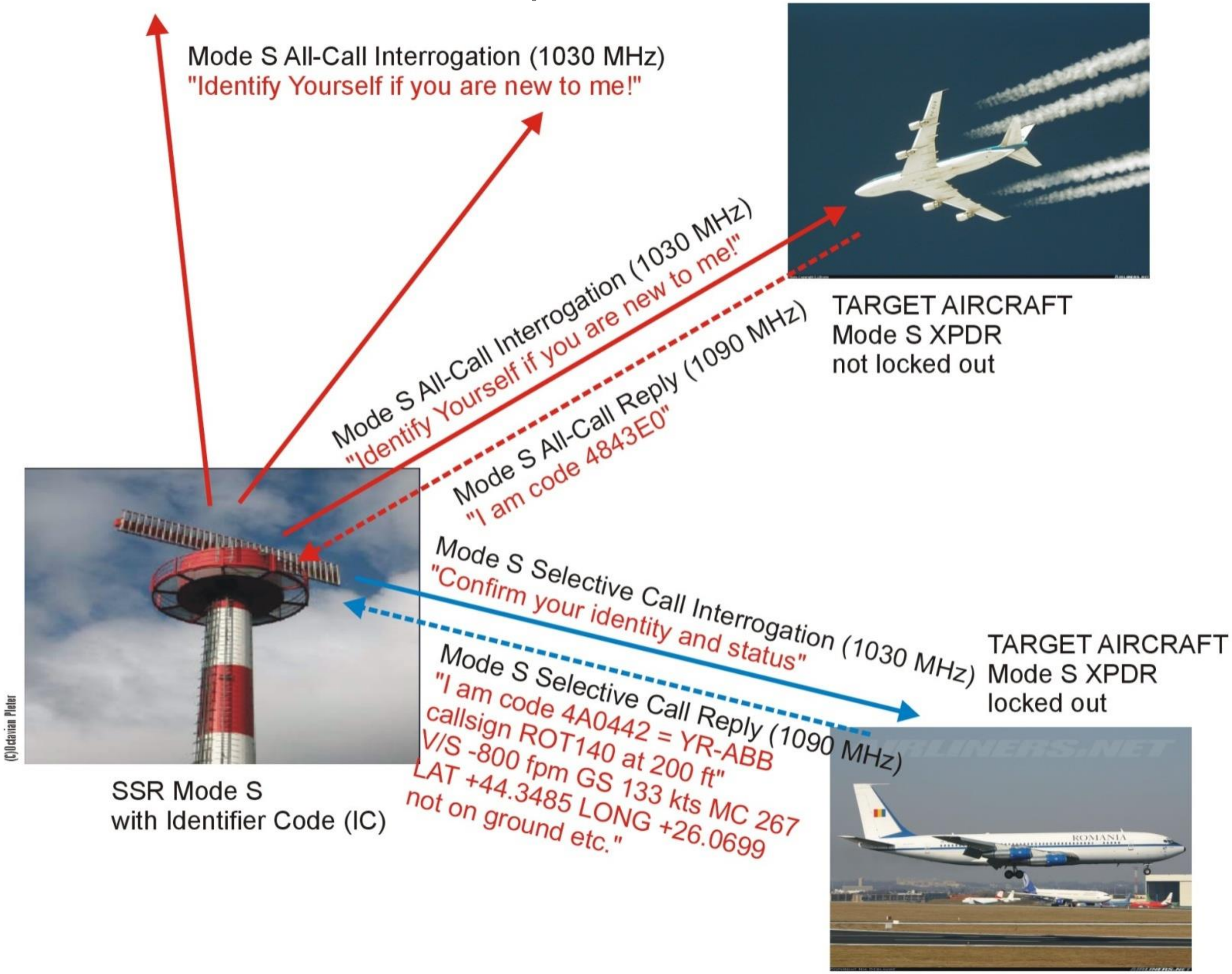
Picture: Daily Express

Mode A/C Classic SSR Transponder (1950)



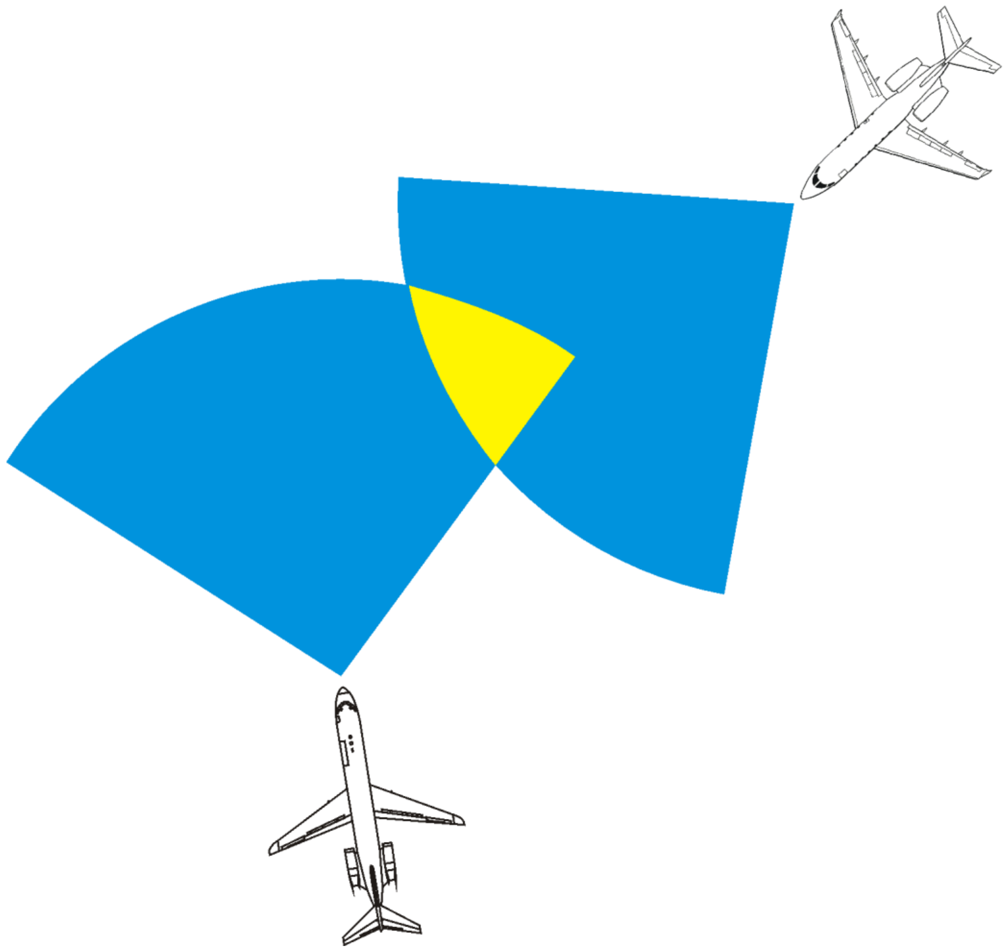
SSR Mode S Information Link (1980)

1030/1090 MHz



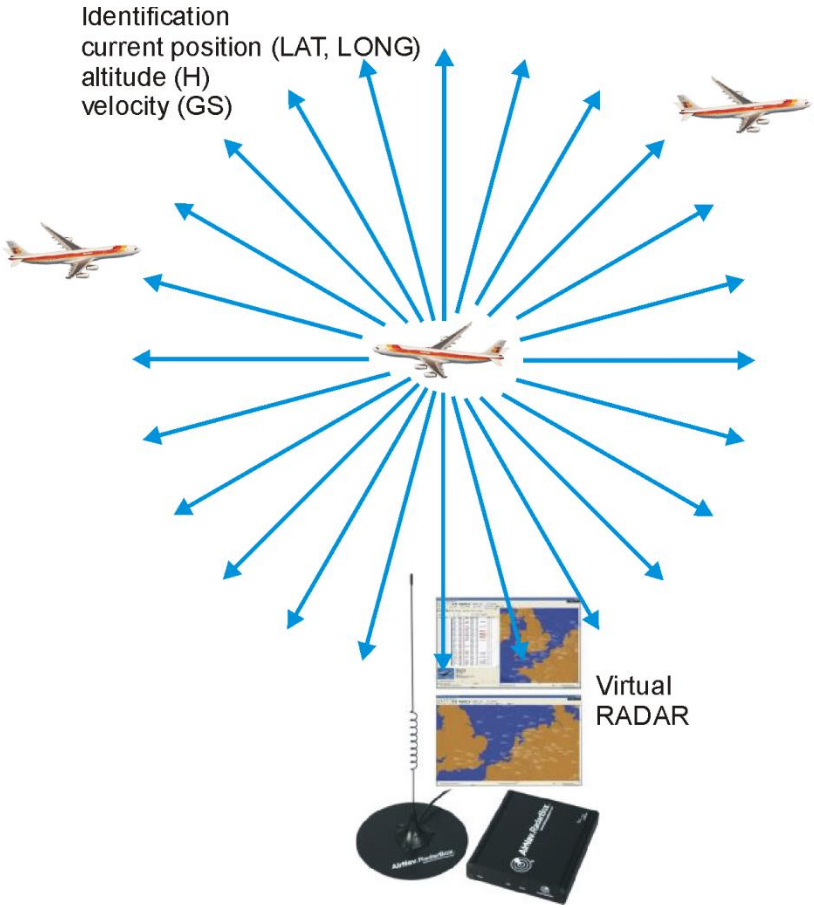
TCAS - Mode S interrogation (1992)

1030/1090 MHz



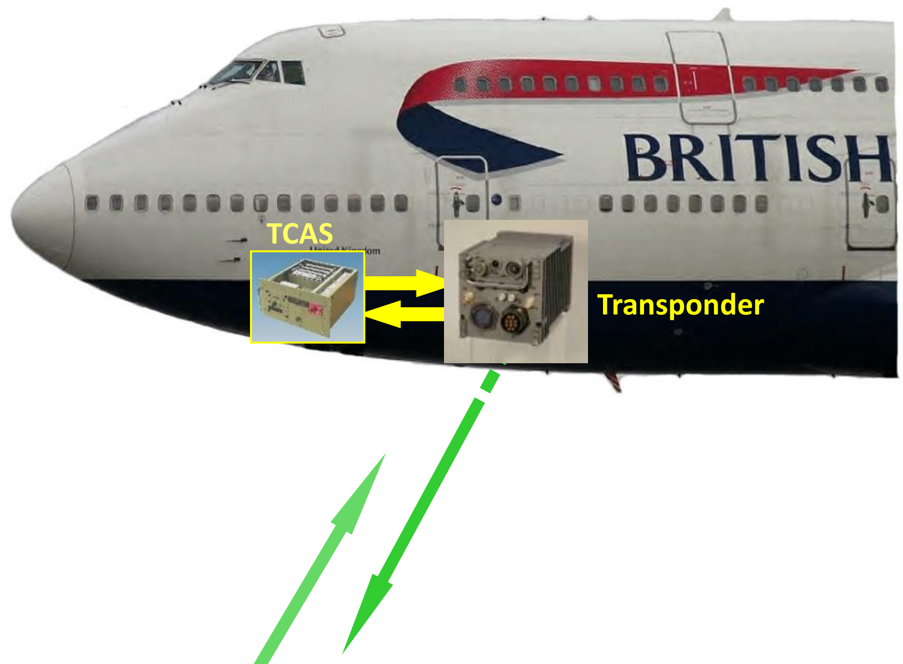
Automatic Dependent Surveillance / Broadcast (ADS/B - 2003)

1030/1090 MHz



1090 MHz
Extended Squitter

Mode S Transponder

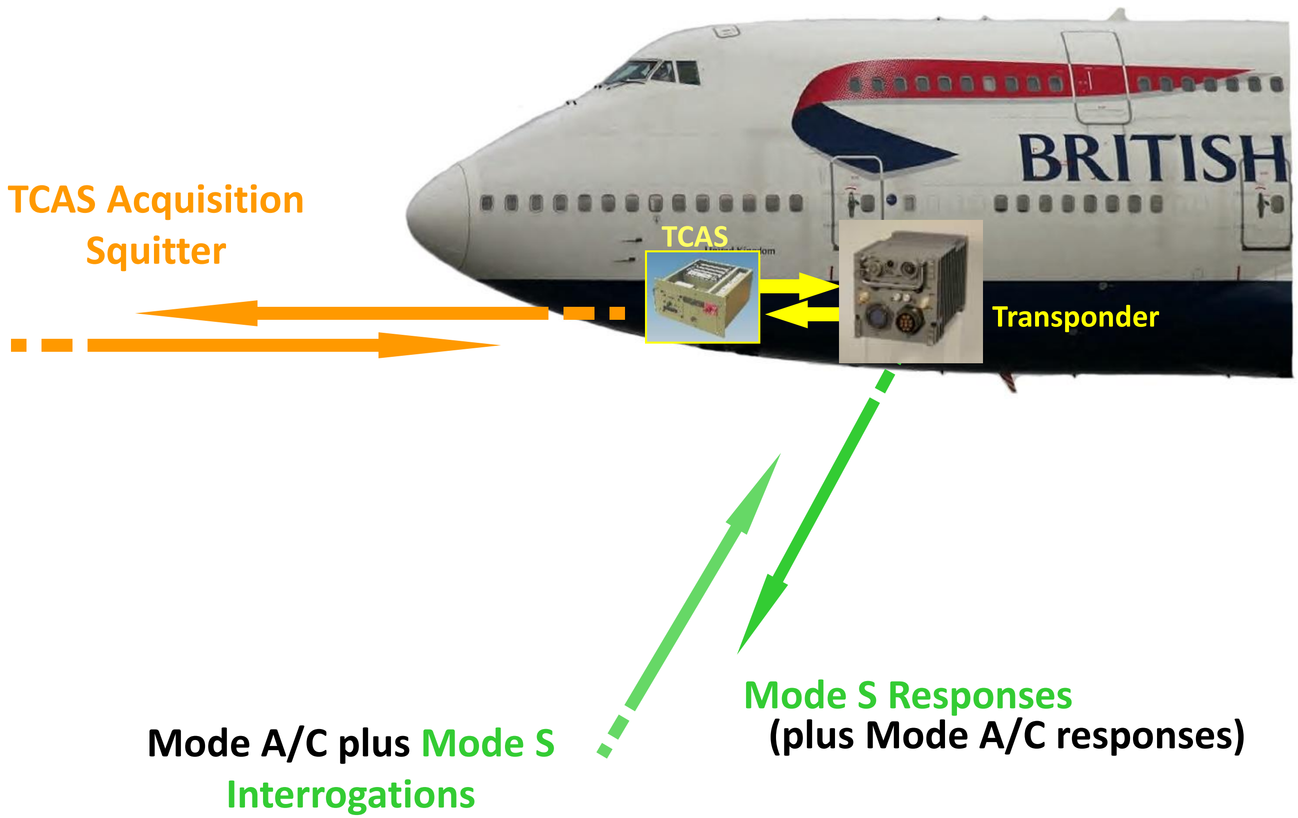


Mode A/C plus Mode S Interrogations

Mode S Responses (plus Mode A/C responses)

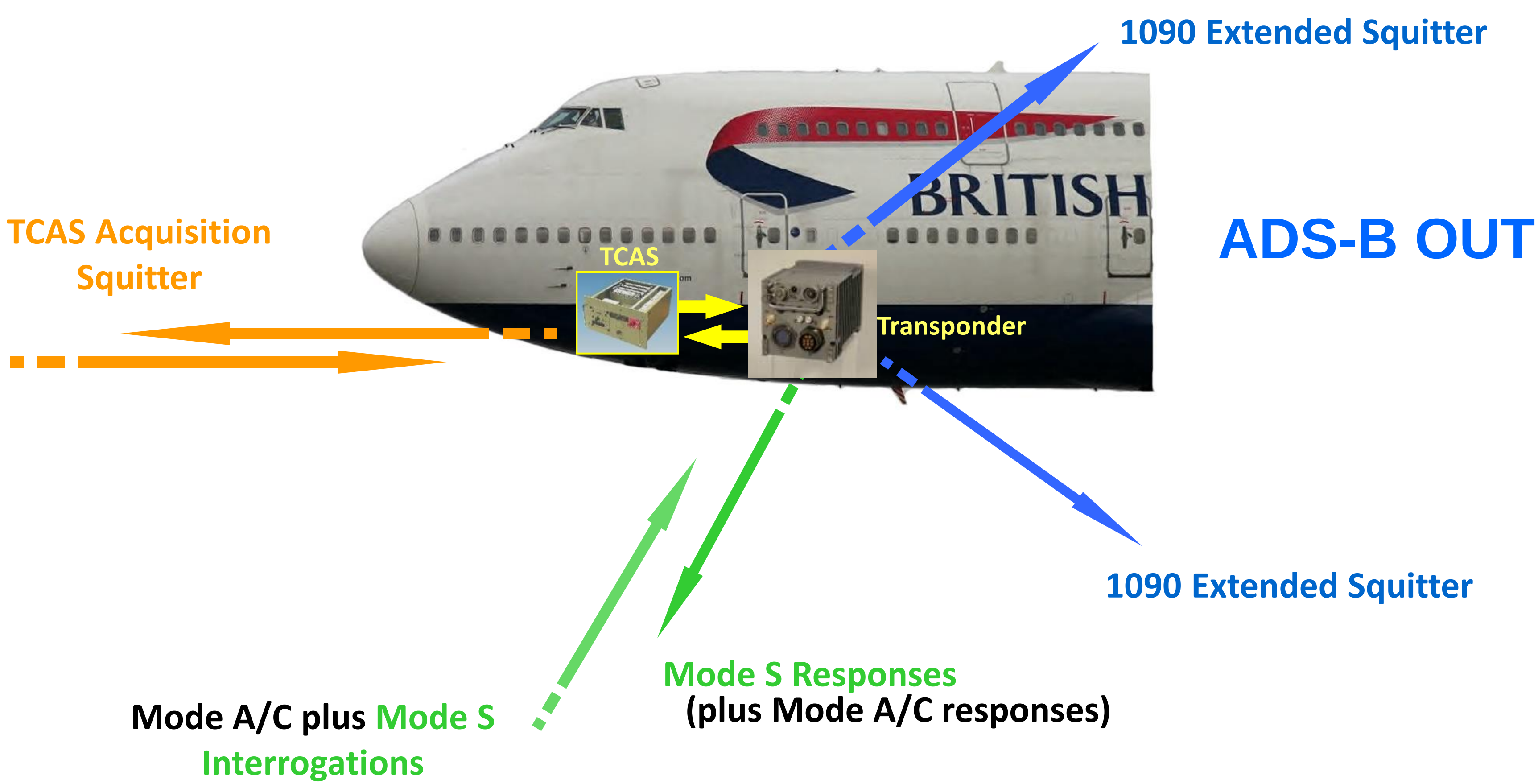
Source: Raytheon

Mode S Transponder (Level 2)



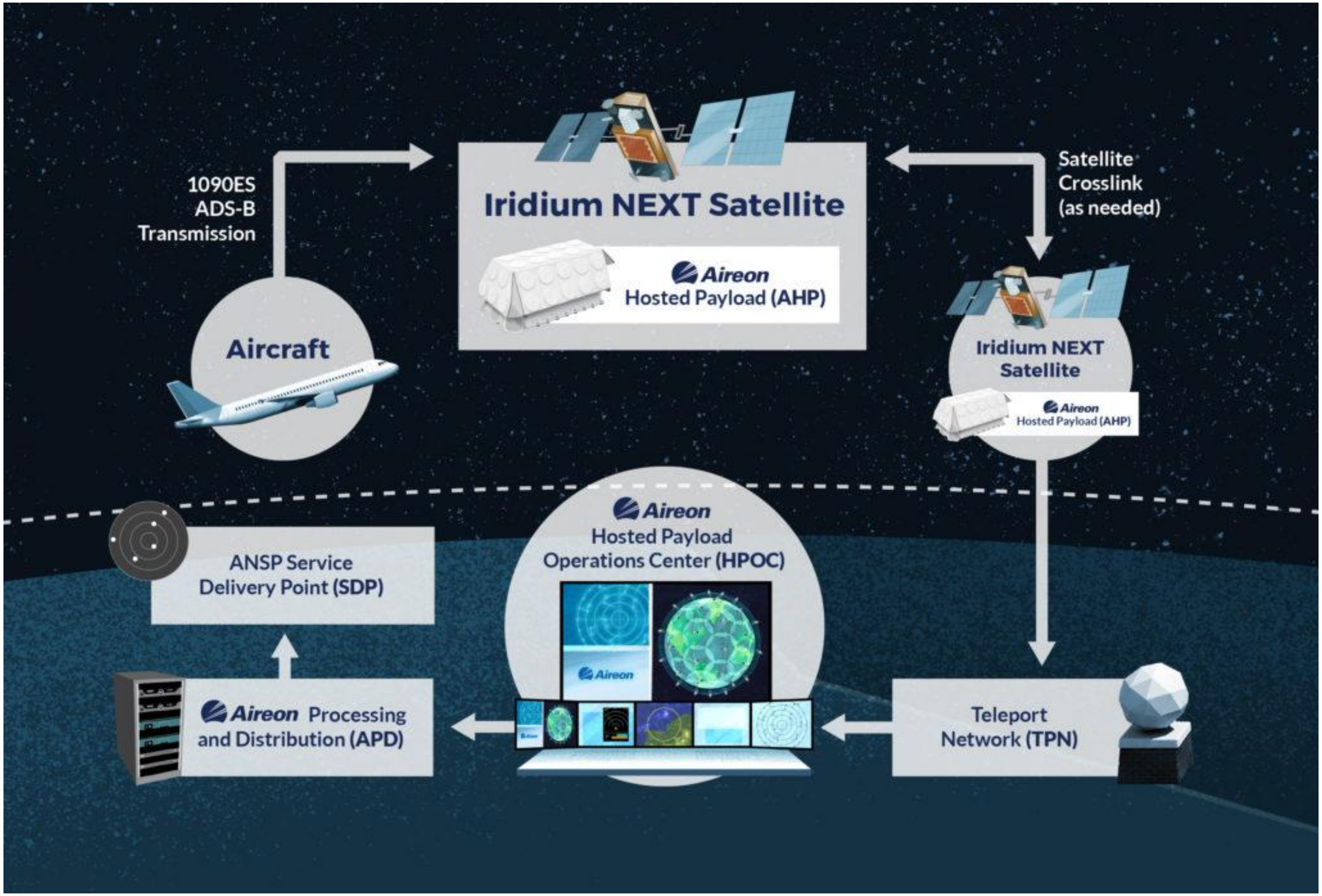
Source: Raytheon

Mode S Transponder (Level 2e)



Source: Raytheon

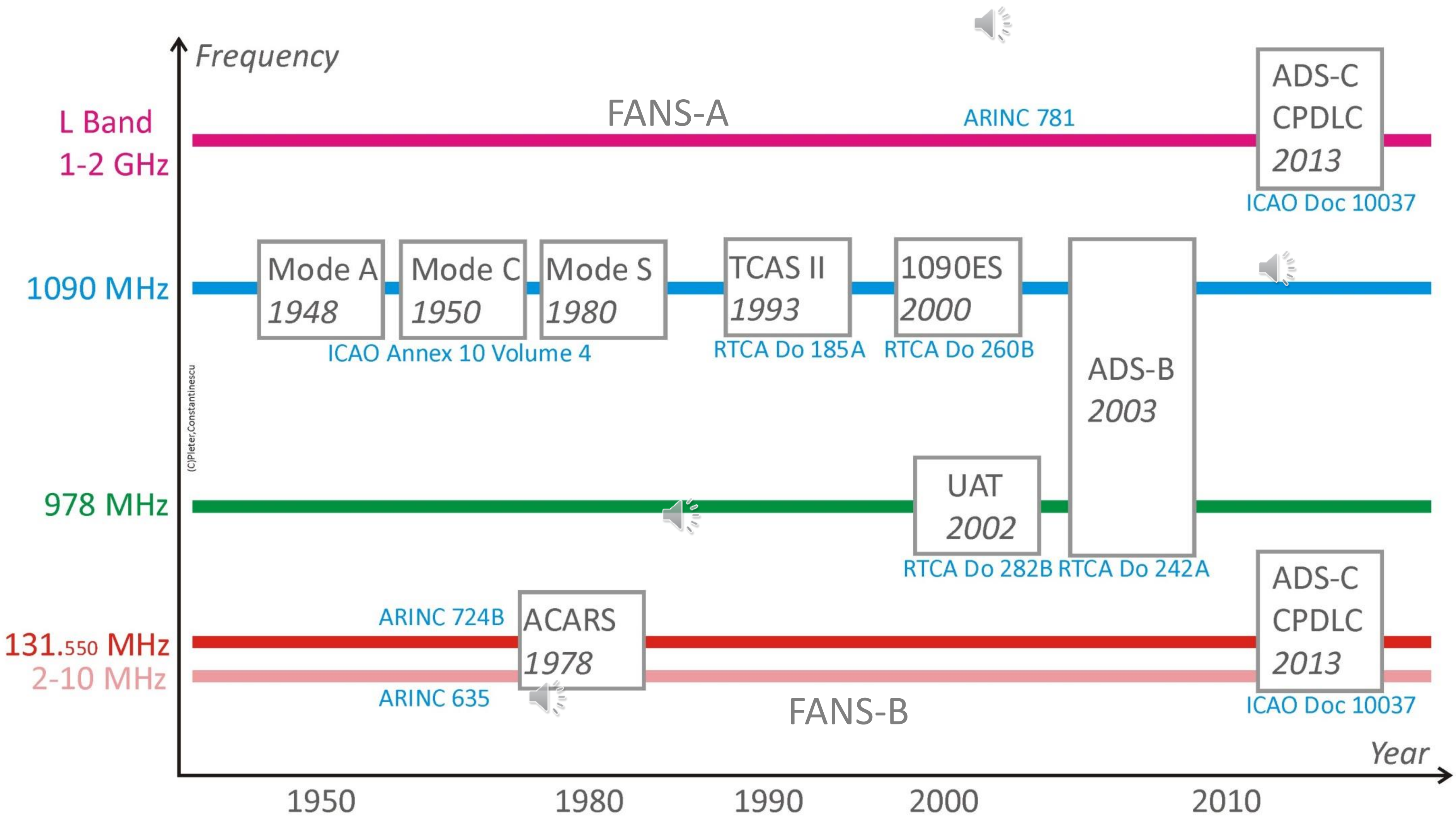
Global ADS/B Tracking by Aireon

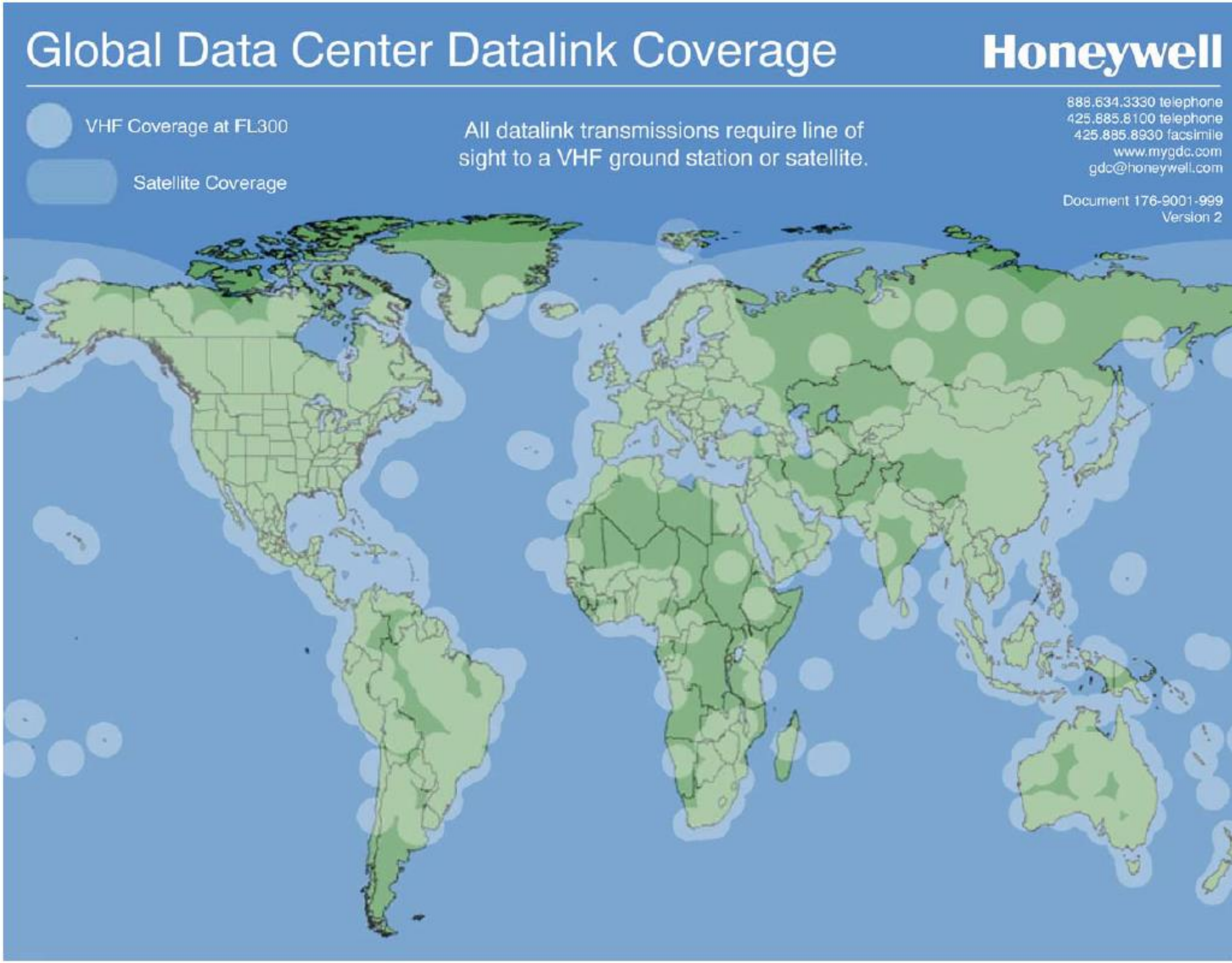


Source: Aireon

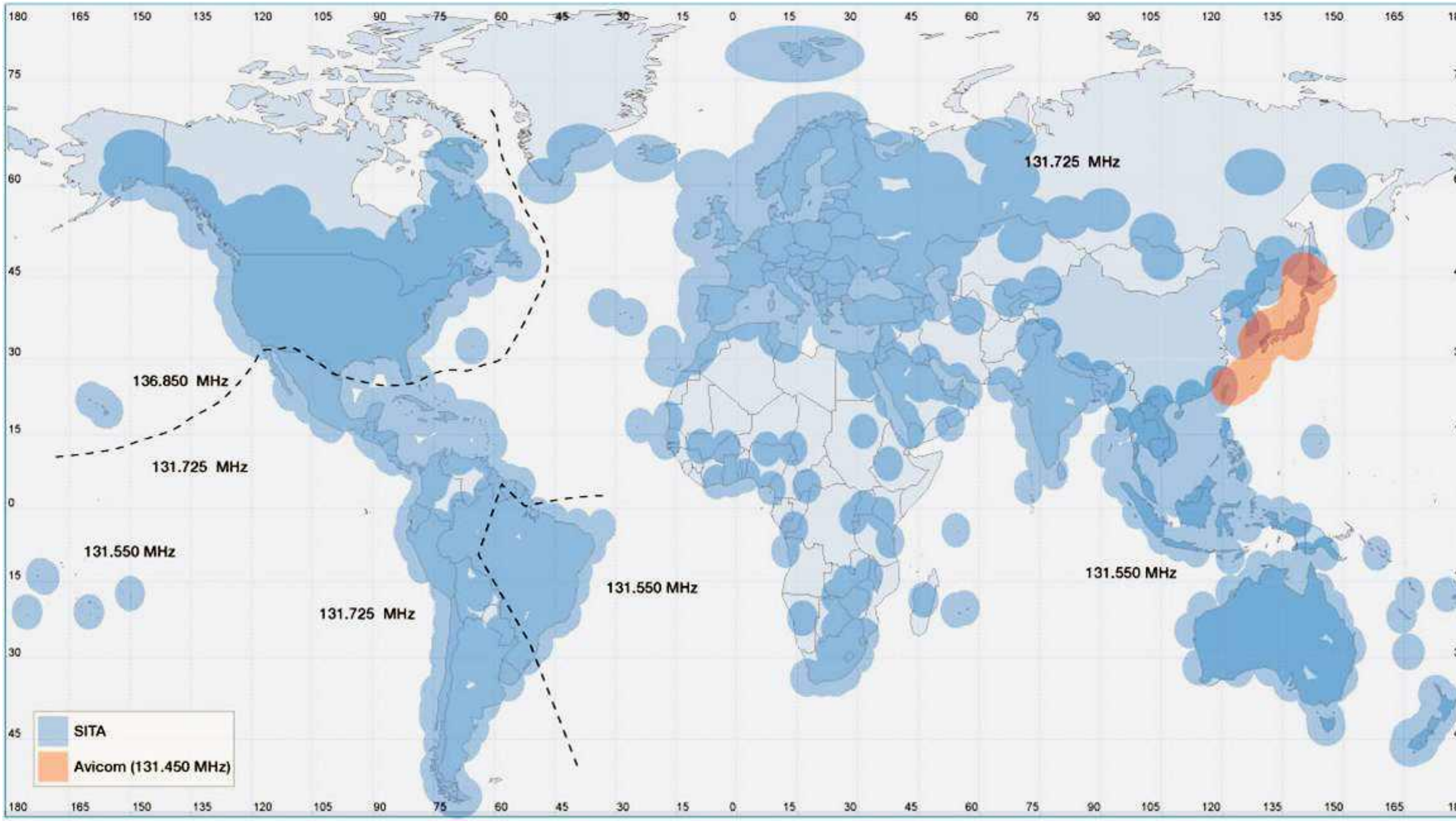
ADS-B and ADS-C

FANS Future Air Navigation Systems
Data Link

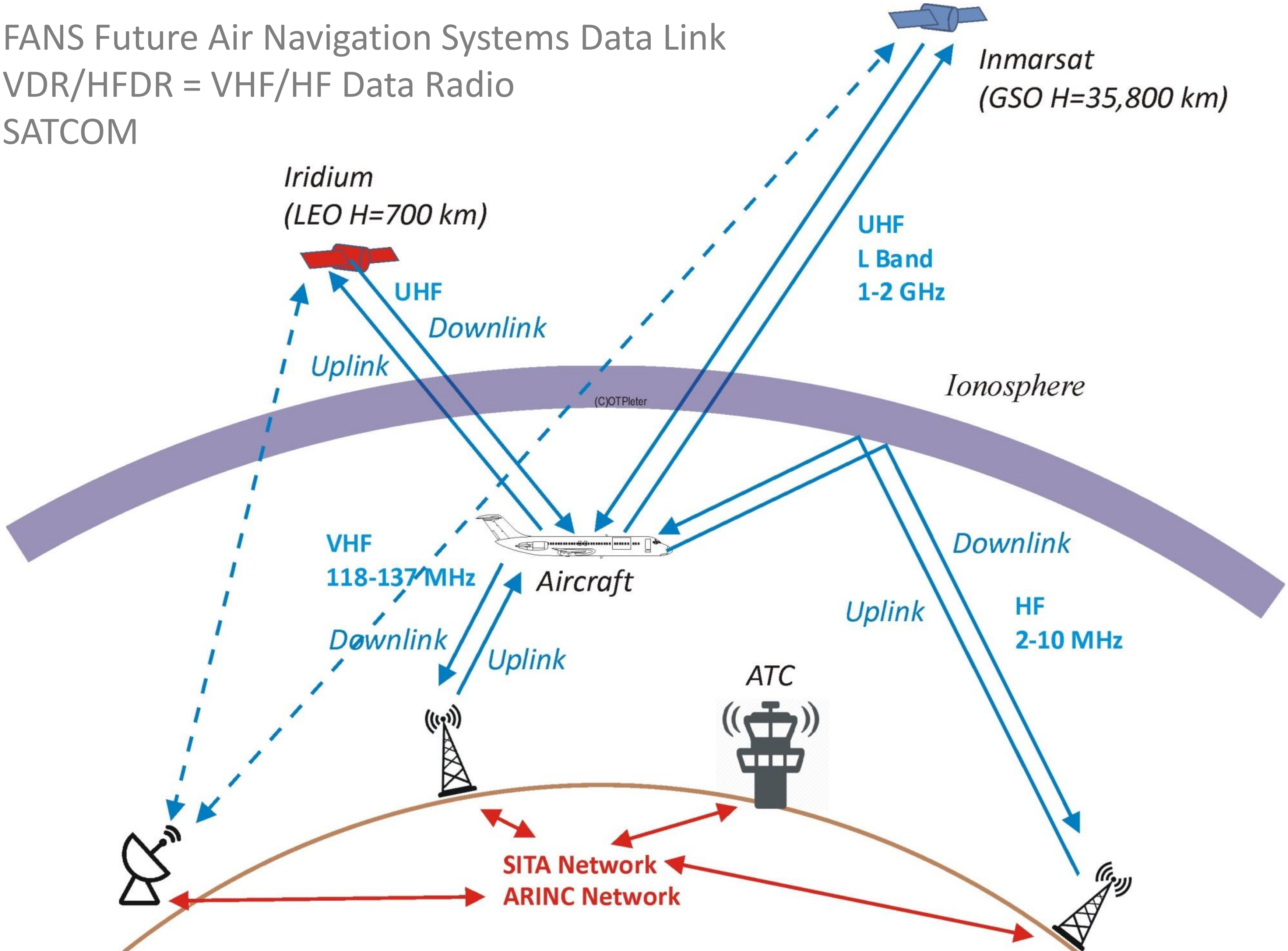



Global Data Center Datalink Coverage
Honeywell
VHF Coverage at FL300
Satellite Coverage
All datalink transmissions require line of sight to a VHF ground station or satellite.
888.634.3330 telephone
425.885.8100 telephone
425.885.8930 facsimile
www.mygdc.com
gdc@honeywell.com
Document 176-9001-999
Version 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

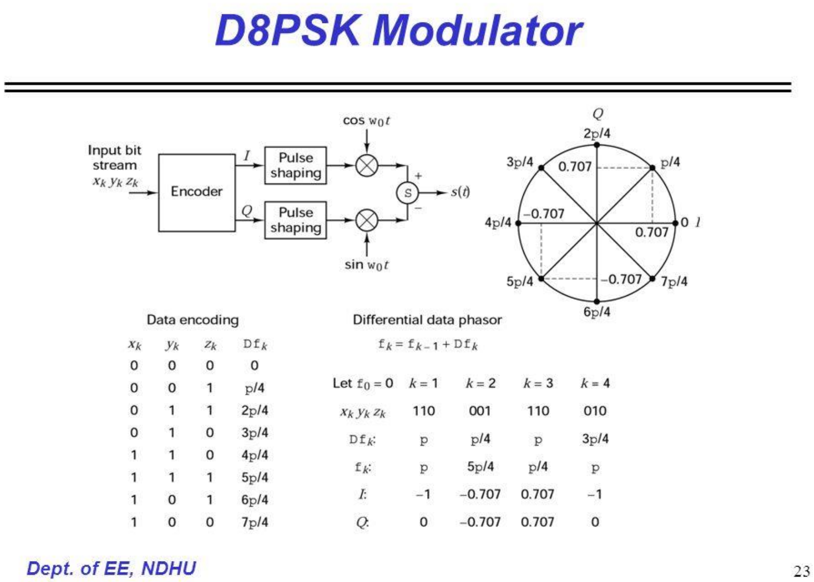
VDL-M2 or VDL2 is a means of sending information between aircraft and ground stations

- 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



*) 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

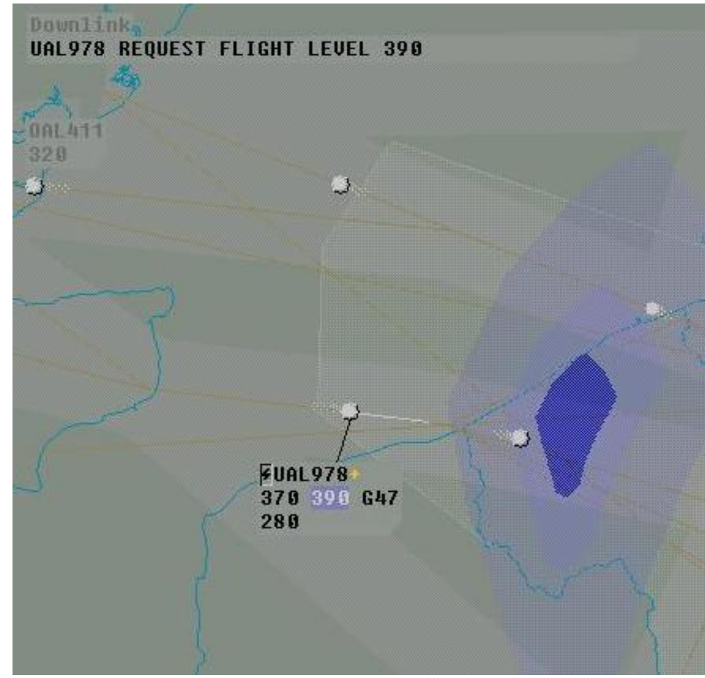
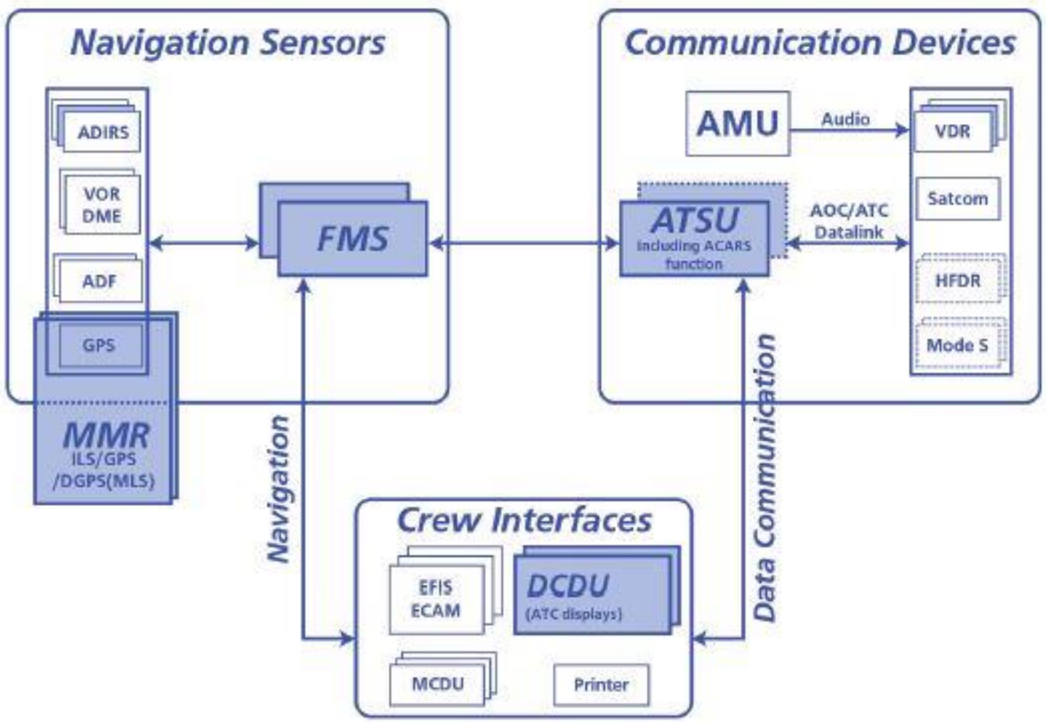


Photo: Telenet.be / CPDLC

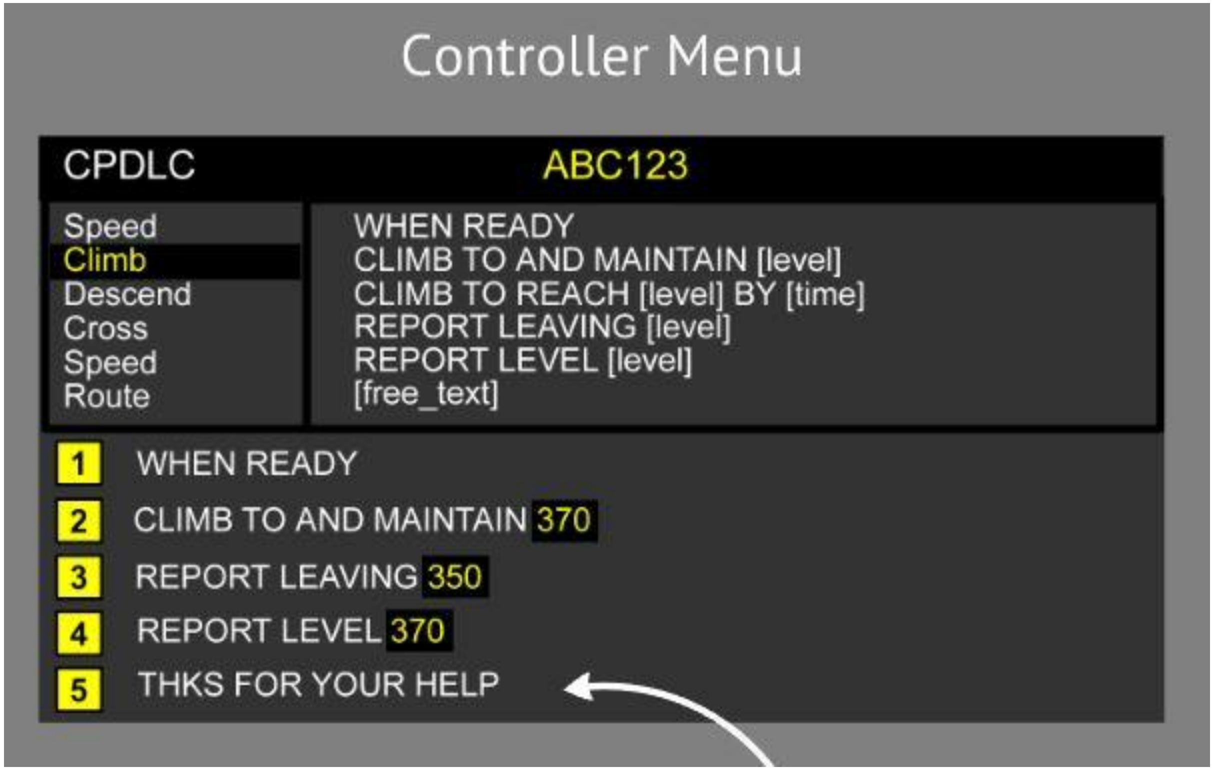
CPDLC Architecture



MMR = Multi Mode Receiver
AMU = Audio Management Unit
ATSU = Air Traffic Service Unit

Source: Oxford Aviation ATPL Instrumenation

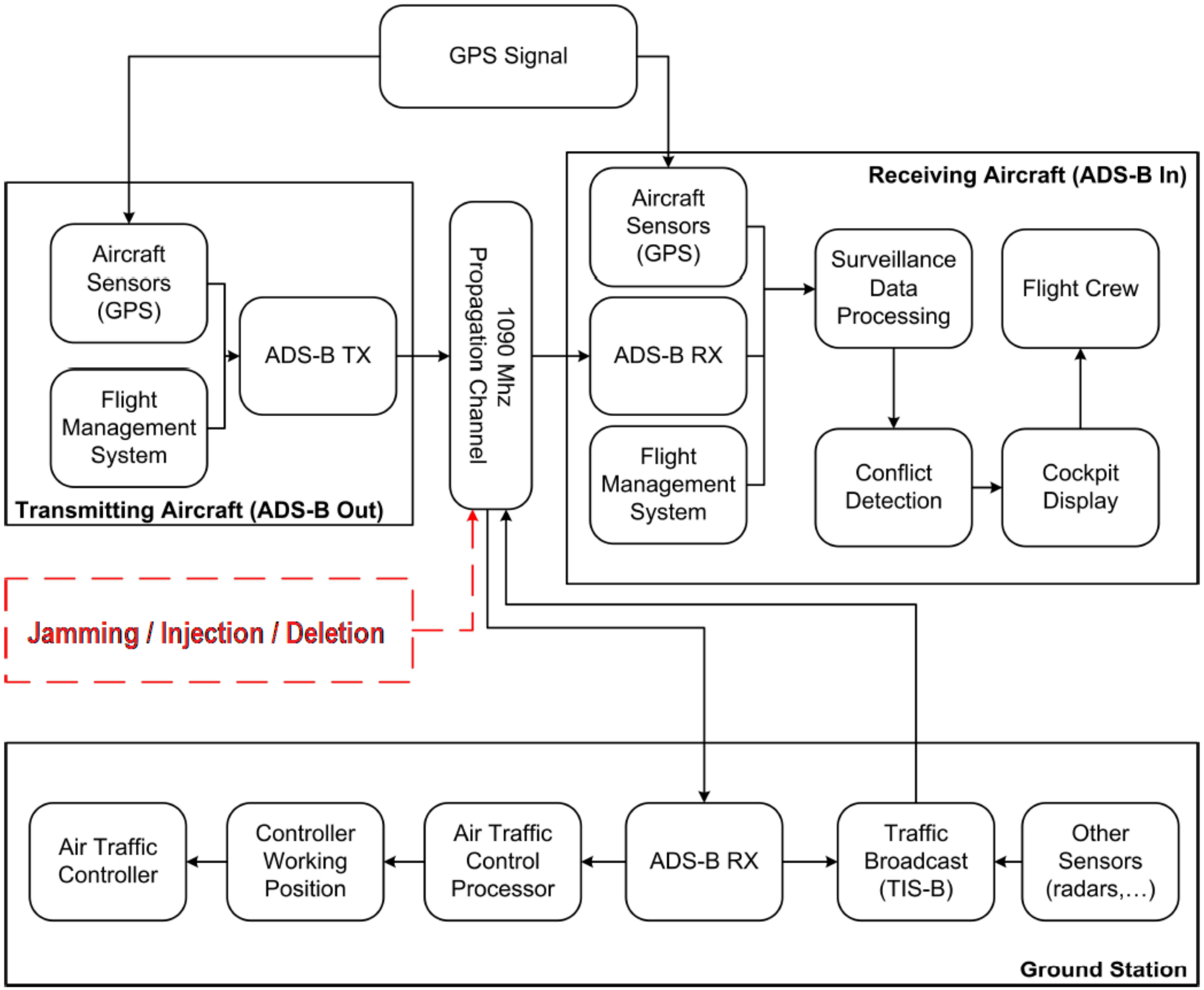
CPDLC – Controller Interface



CPDLC – Pilot Interface

Photo: Oxford Aviation ATPL Instrumenation

ADS-B and ADS-C Vulnerabilities



Source: ICAO

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;

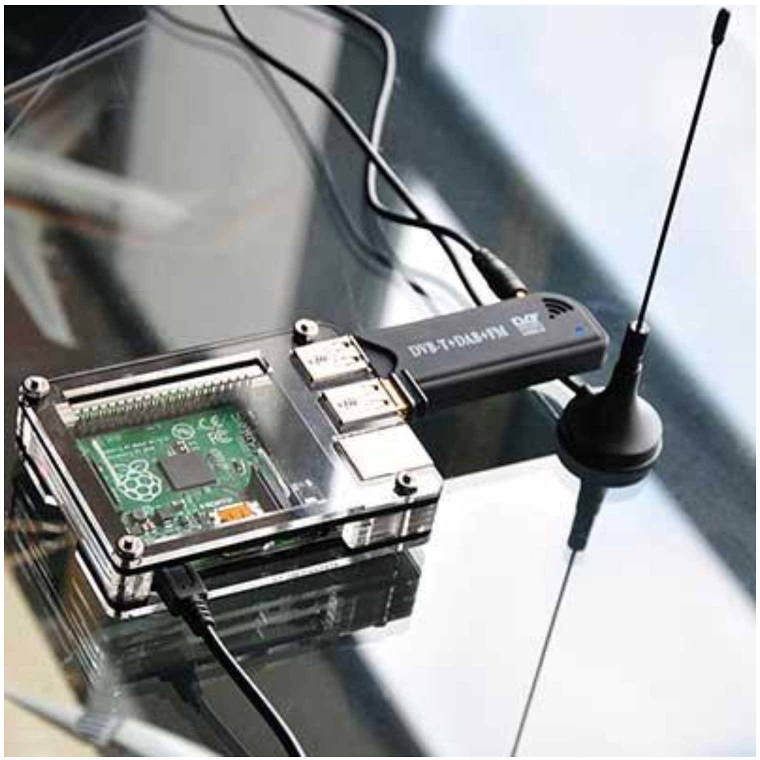
- **Jamming**, i.e., the intentional transmission of high power harmful signals in the RF channel in order to disable the air–ground communication: for a single receiver or in a particular geographical area, this type of attack may create denial-of-service problems at any ATC;

- **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

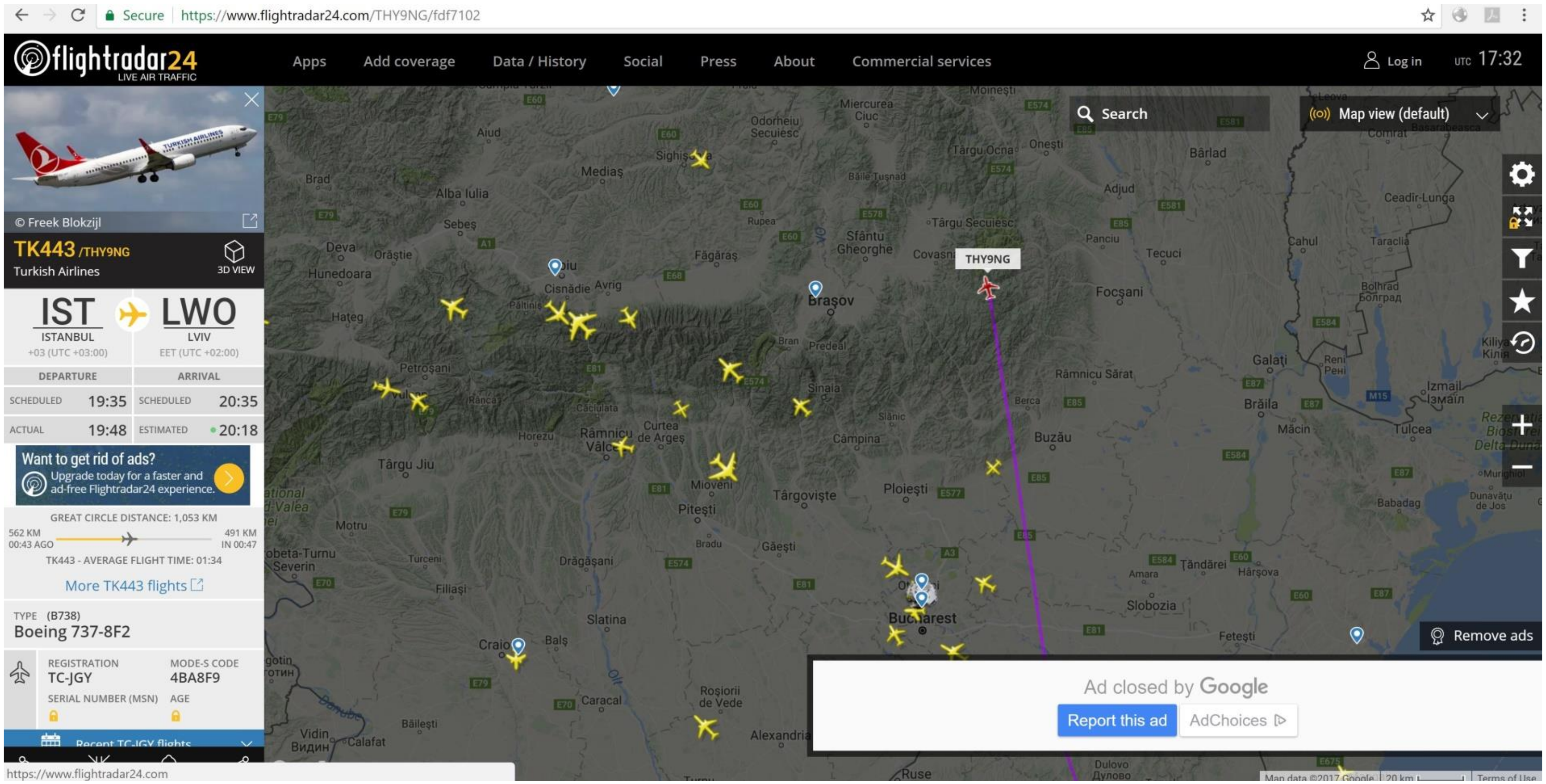
2: made **public** by means of radio or television

3: of or relating to radio or television broadcasting

(Myriam-Webster Dictionary)

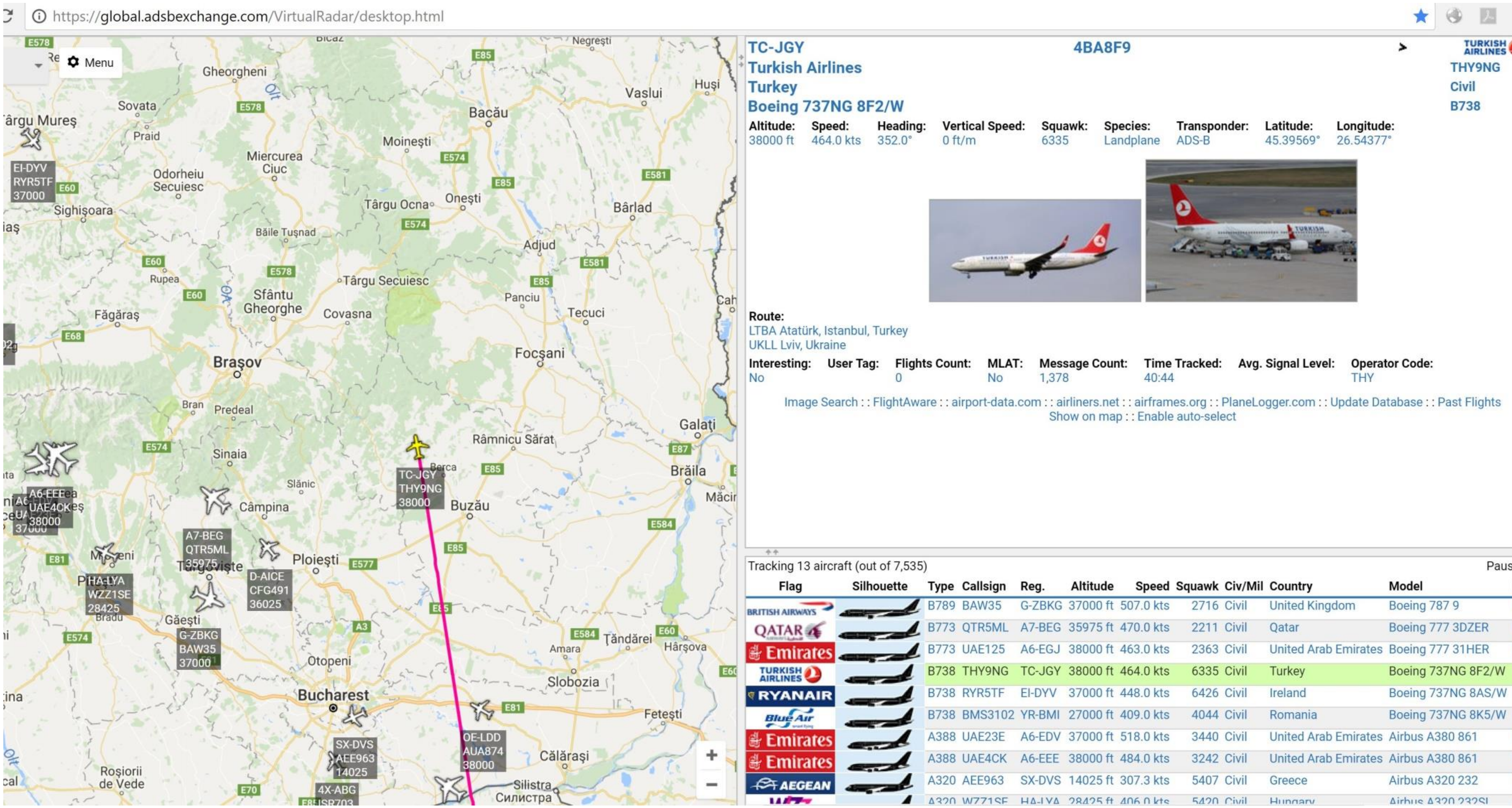
FlightRadar24

https://www.flightradar24.com



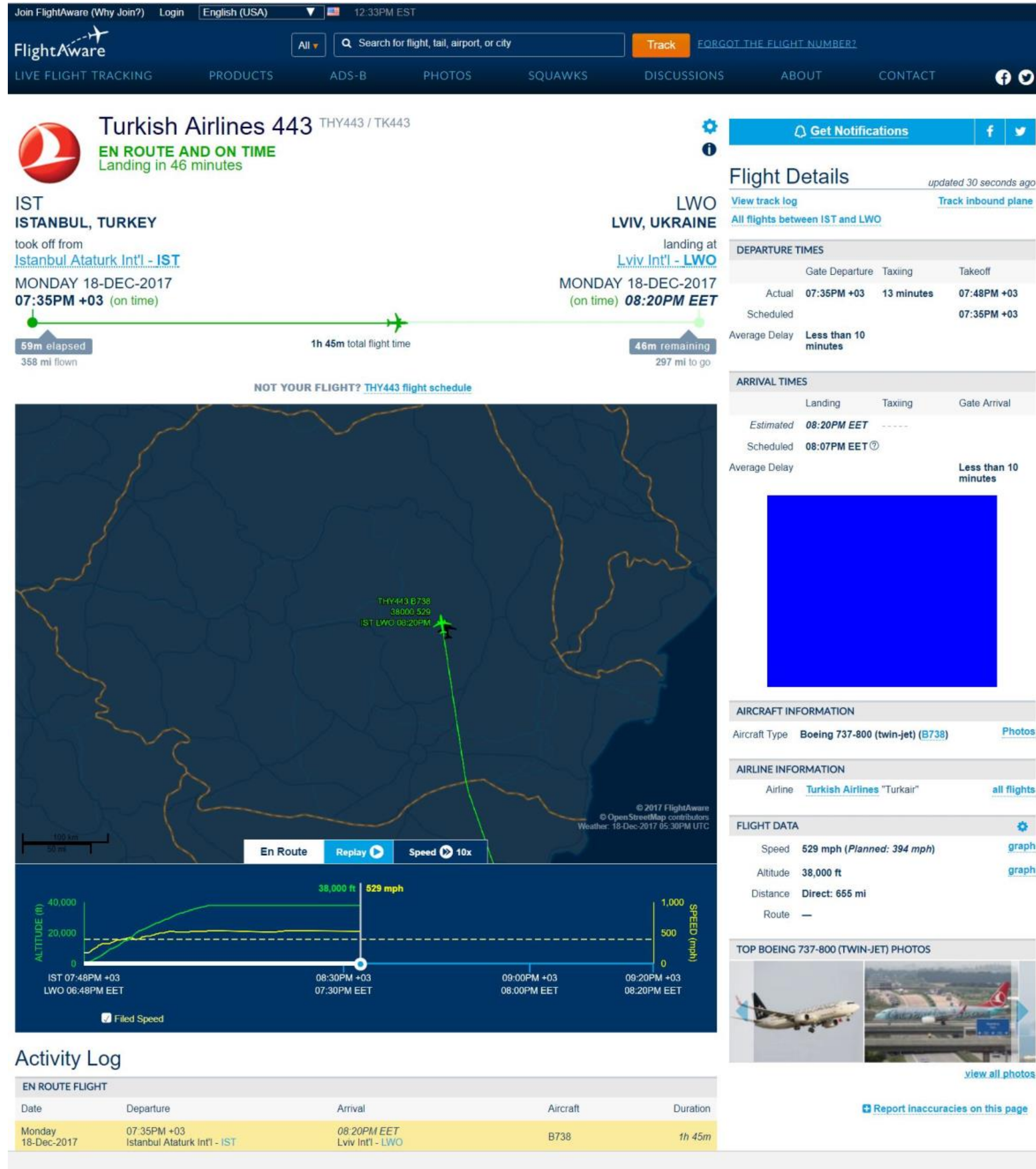
Global ADS-B Exchange

https://www.adsbexchange.com/



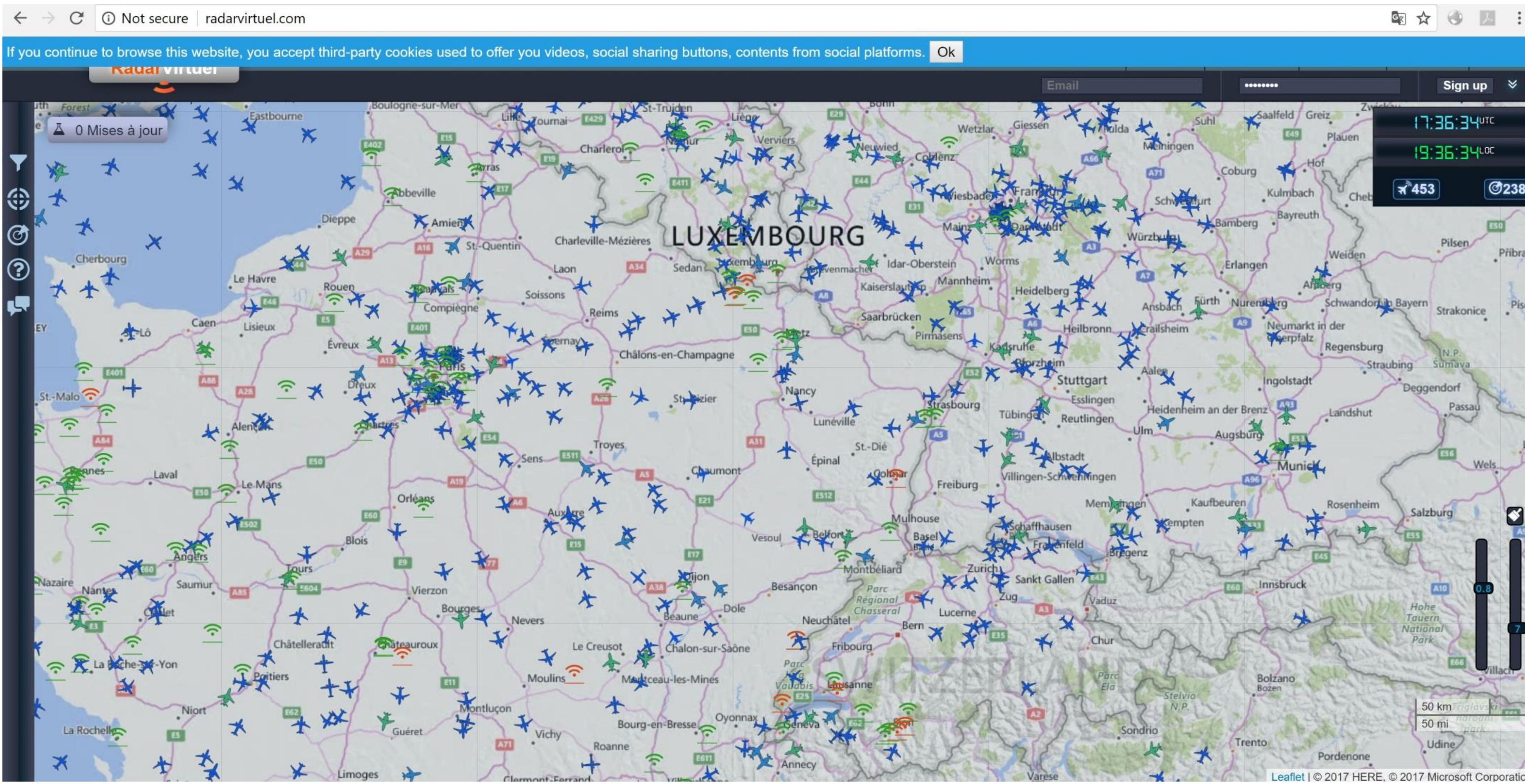
Flight Aware

https://flightaware.com/



RadarVirtuel

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.

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

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 impose 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 a least 11 time closer to the receiving antenna (i.e. to erase an airplane 100km away one need to be at no more than 9km from the antenna)

Satisfying the requirements

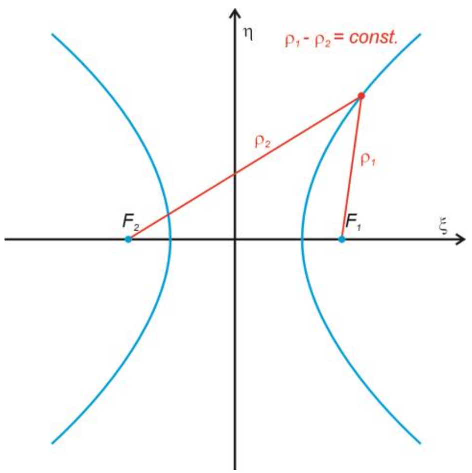
- The second condition impose that the difference in time of arrival between direct and fake signal must be less then 70us.
- That translate to a difference in distance of 21Km
- If the first condition is fulfill then the maximum difference is 18km, and so all aircraft far enough are erasable
- If the 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



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

TDOA = Time Difference of Arrival

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

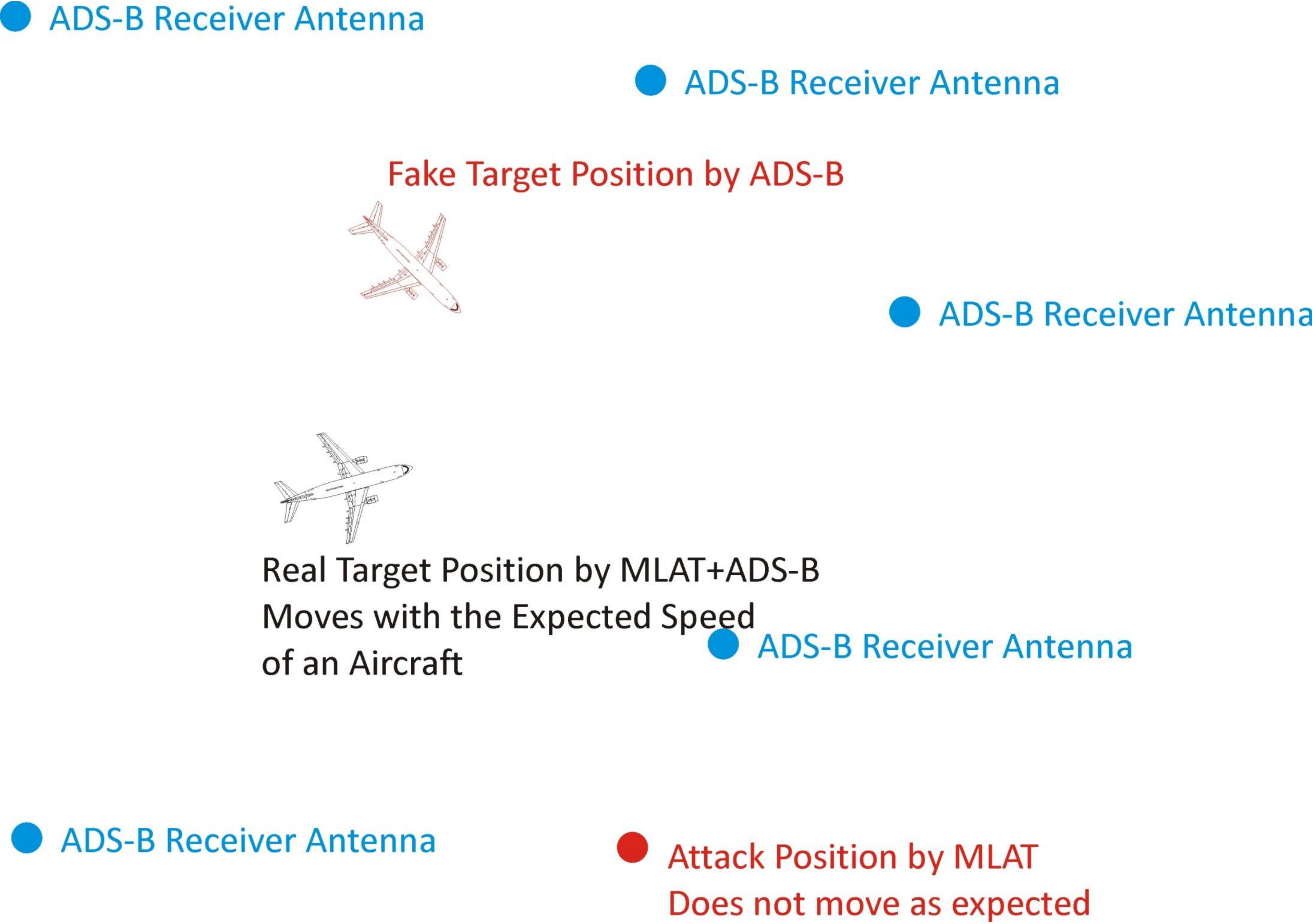
$$b = \sqrt{\frac{(x_1 - x_2)^2 + (y_1 - y_2)^2}{4} - a^2}$$

Immediate Countermeasure: ADS-B Kalman Filtering for position continuity

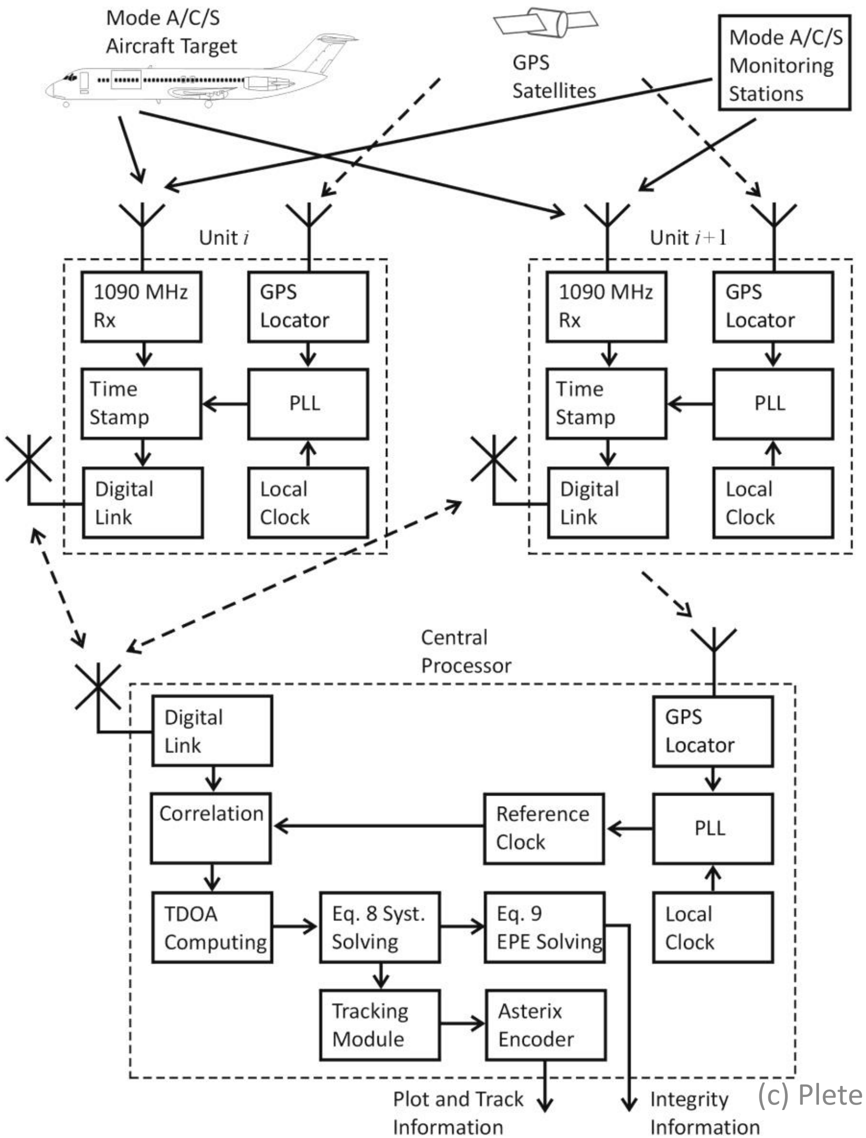
A legitimate target cannot jump from a position to another, it needs to follow a flight dynamics model (e.g. BADA).

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

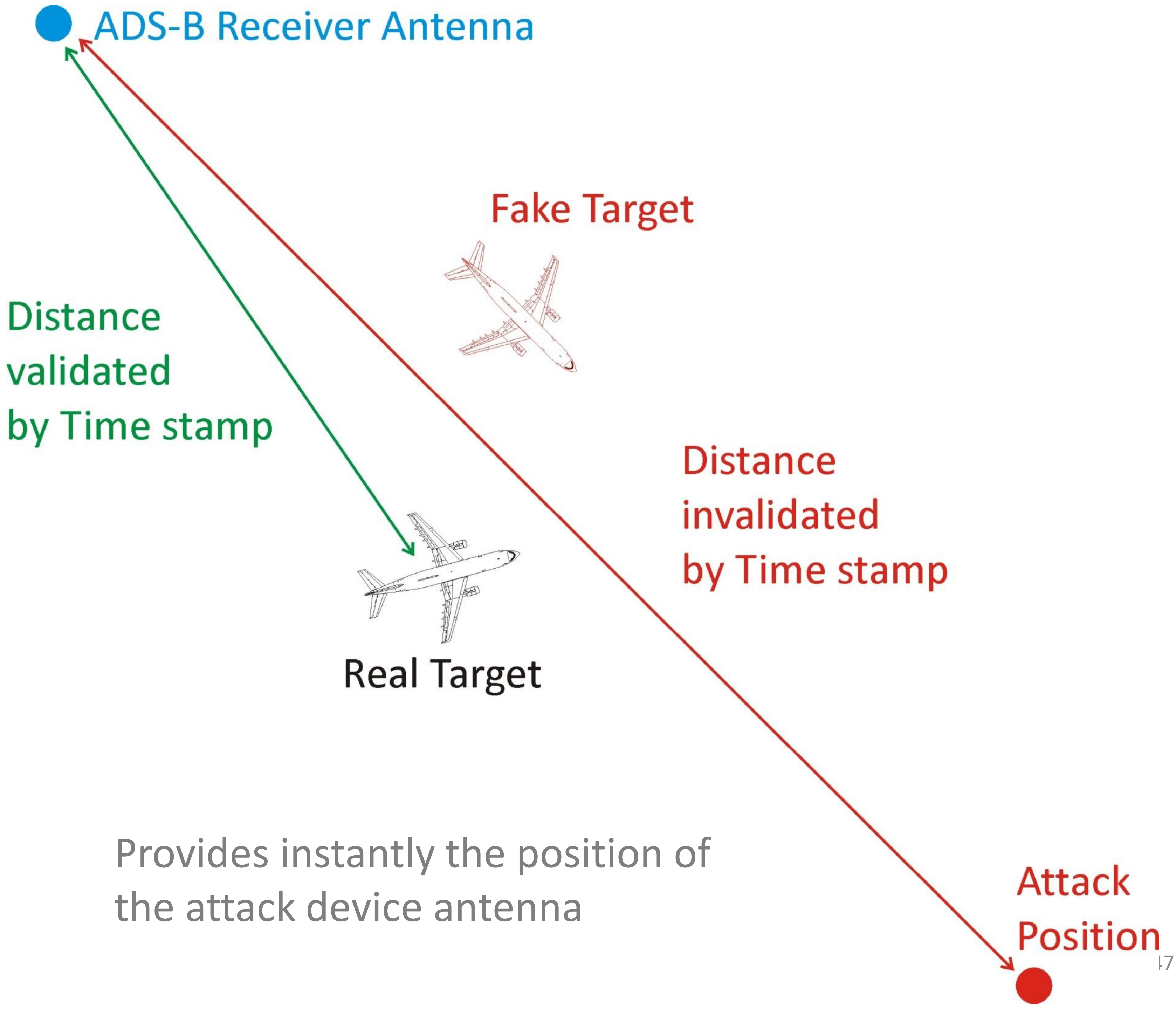
Medium Term Countermeasure: ADS-B/C Time Stamp inlcuded in the message



The GNSS accuracy time stamp inlcuded 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.



Provides instantly the position of the attack device antenna

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