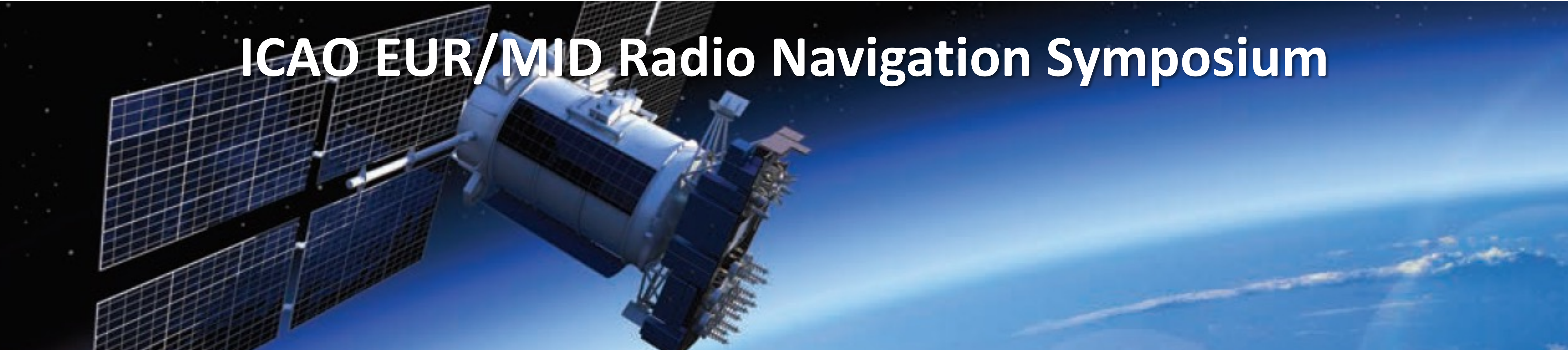


ICAO EUR/MID Radio Navigation Symposium

GNSS interference: A Pilot's Perspective

Niklas AHRENS

International Federation of Air Line Pilots' Associations (IFALPA)

Antalya, Turkiye
(6-8 February 2024)

01 **GNSS manipulations**

Jamming/Spoofing

02 **Loss of GNSS as a source**

Avionic system architecture

03 **Flawed position information**

Deteriorated position information

04 **False warnings**

ETAWS/EGPWS warnings

05 **Recommendations**

Procedures and System Design

06 **Outlook**

General robustness

GNSS-Jamming

- Broad blocking of frequencies

- Often used for privacy reasons (e.g. lorry drivers)

GNSS-Spoofing

- Targeted attack to alter position information

- Position of the targeted object known

Loss of GNSS as a source

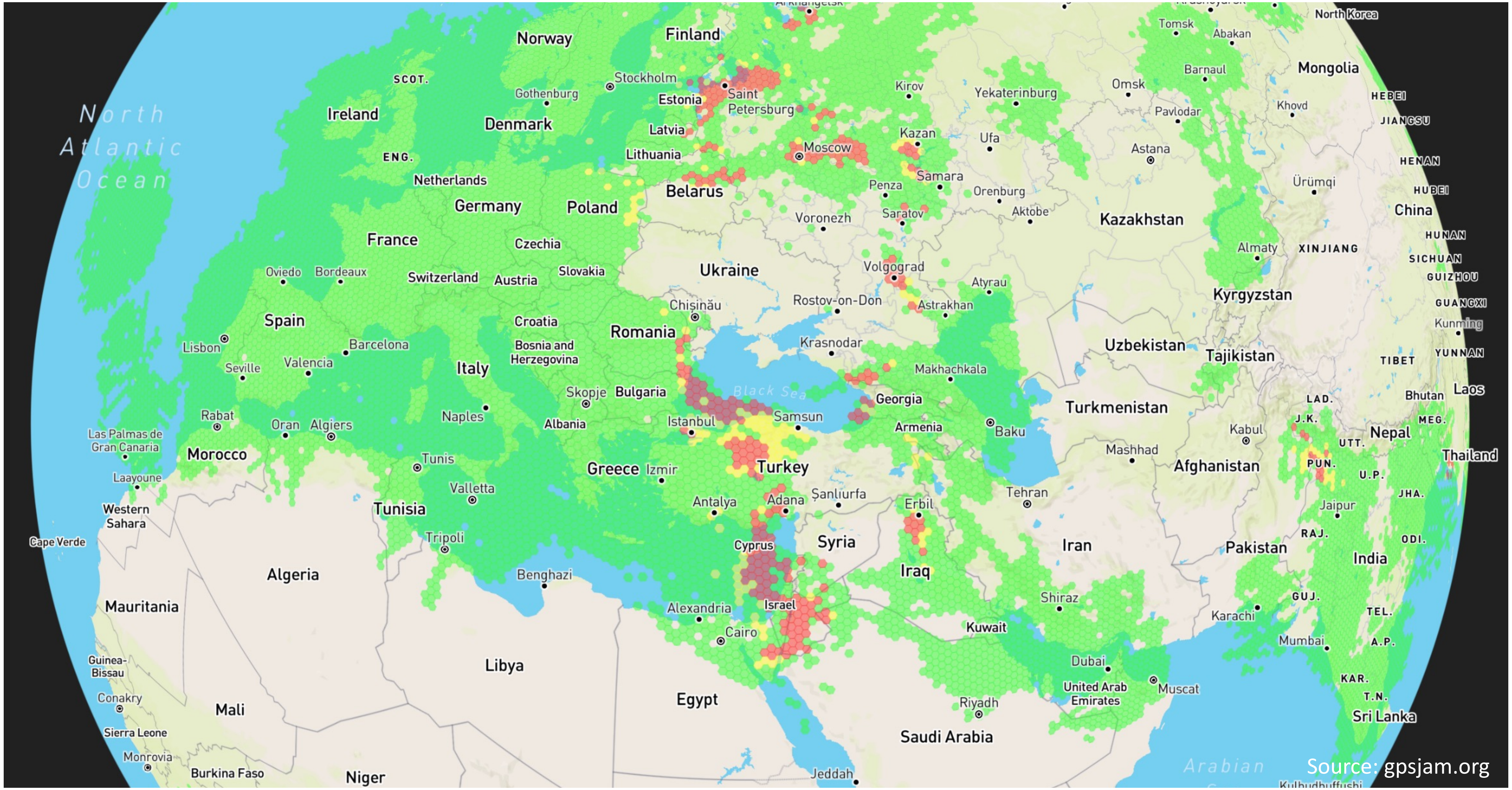
Different aircraft architectures

- In former designs often used as one source of navigation combined with Inertial Reference System (IRS) and Radio Position
- In case of loss of the GNSS position other sources are used
- IRS as a robust platform to counter short time position alterations at the cost of long-term drift
- More modern systems calculate a correction factor for IRS drift to correct during longer flights
- ADS-capability lost/clock errors

Problem: System architecture not always described extensively, internal discarding might not be noticed by pilots

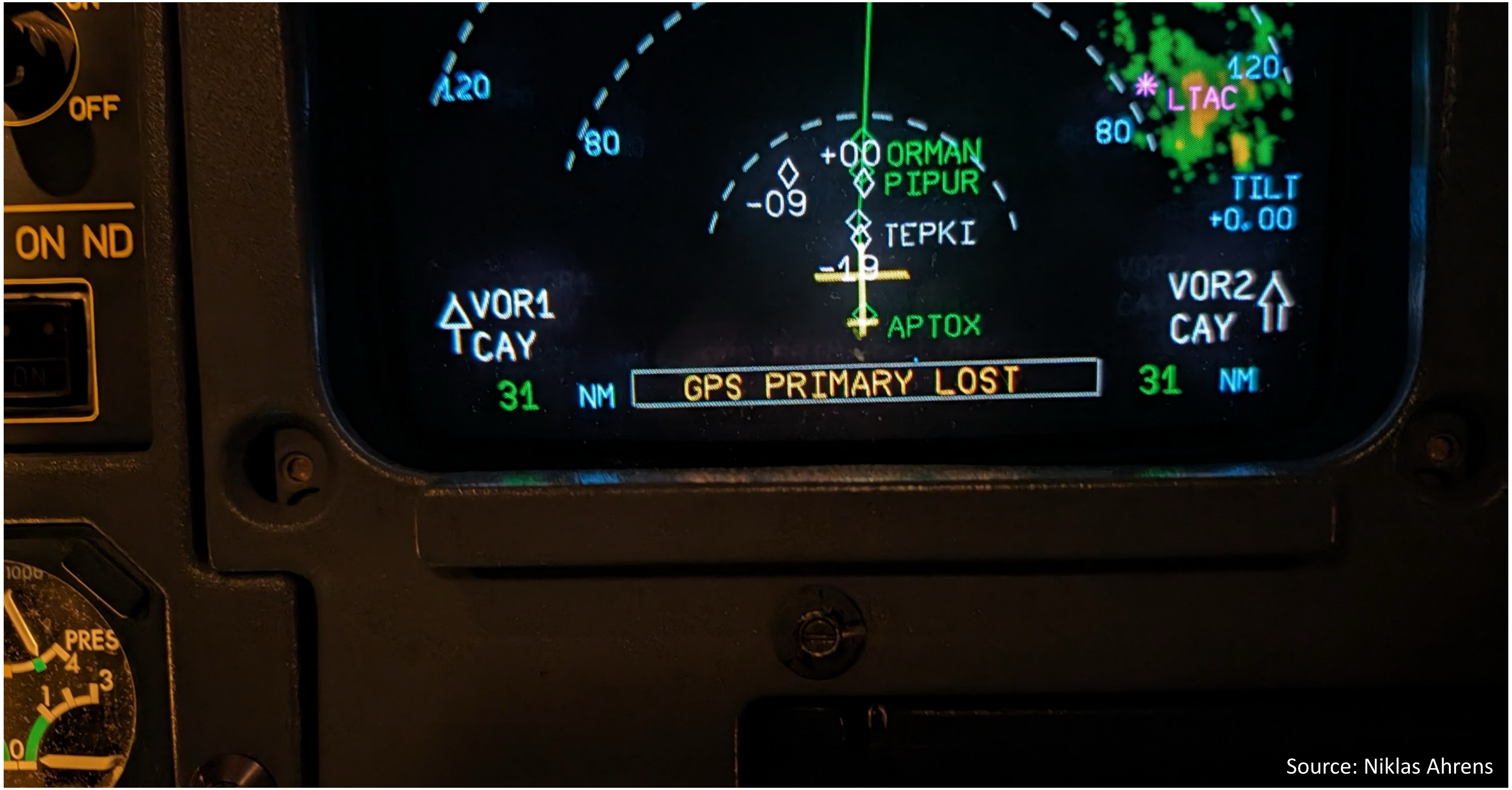
Source: Niklas Ahrens

GNSS-Jamming



Source: gpsjam.org

GNSS-Jamming



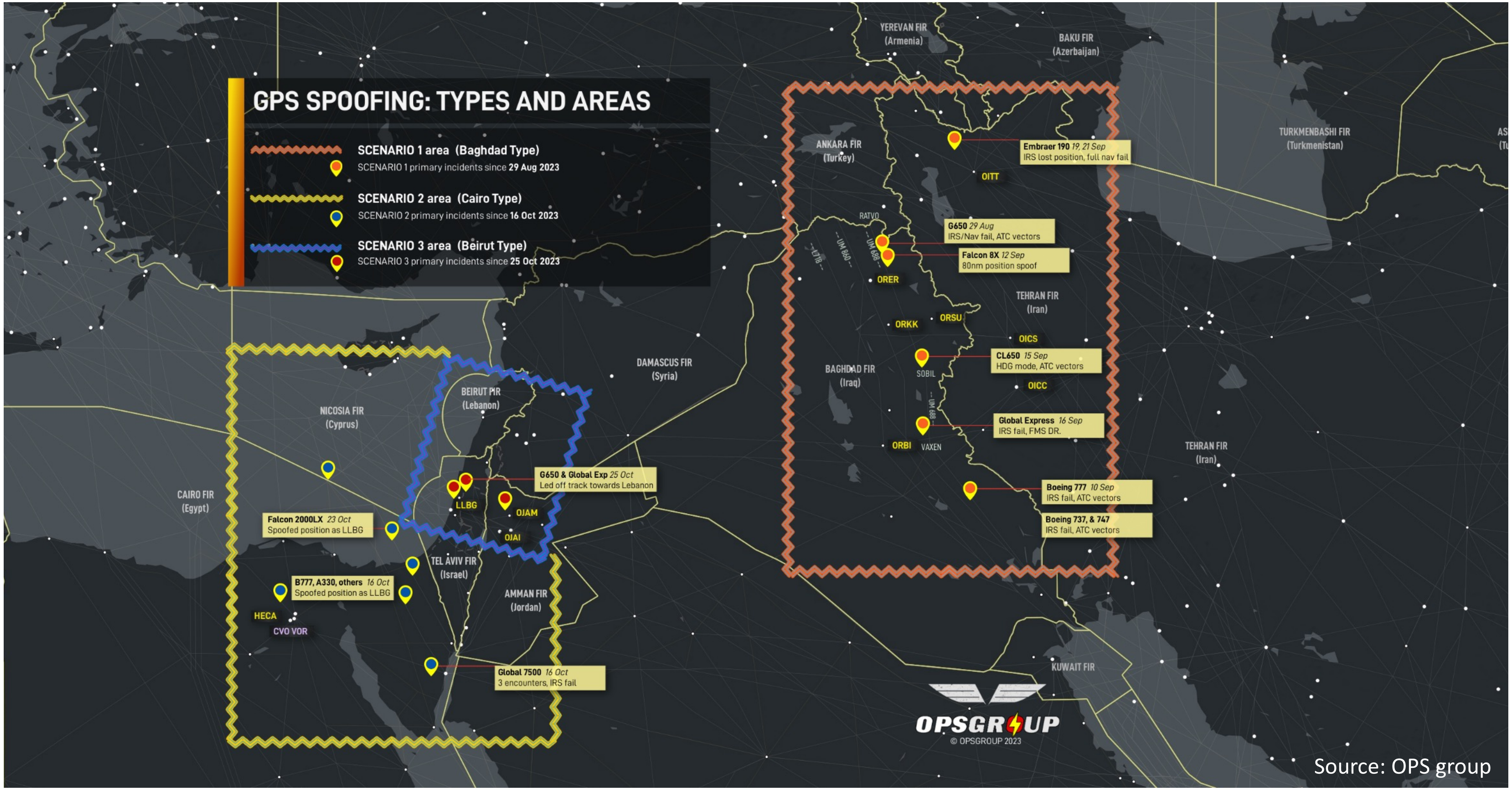
Source: Niklas Ahrens

> ”
>
> *Hybrid Function:*
>
> *The GPS Hybrid function utilizes existing hardware components in the IRU to receive GPS data from one or two GPS Receiver systems. Data received is one Hz nominal RS-422 time mark signal unique for each GPS receiver input and ARINC 429 GPS high-speed satellite measurement and autonomous data. The GPS Hybrid function blends received GPS autonomous Pseudo Range with Inertial and Air Data altitude data in a tightly coupled Kalman filter to achieve optimal position, velocity, and attitude performance. All satellites and sensors are individually calibrated in the Kalman filter. The resulting hybrid data is highly calibrated and provides exceptional navigation performance even if all satellites are lost.*
>
> “
>
> Source:
>
> Honeywell Product Description LASEREF VI (2016)

Flawed Positions

Adverse effects on navigational performance

- GNSS-Positions may be fed back to other navigational means
- In case of a spoofed GNSS-Position also other platforms will be affected
- Robust procedures would require a deactivation before entering the area of (suspected) spoofing or only a short time after entering to supress the adverse effects
- Procedures require an active deselection GNSS as a navigational source



GPS SPOOFING: TYPES AND AREAS

SCENARIO 1 area (Baghdad Type)
SCENARIO 1 primary incidents since 29 Aug 2023

SCENARIO 2 area (Cairo Type)
SCENARIO 2 primary incidents since 16 Oct 2023

SCENARIO 3 area (Beirut Type)
SCENARIO 3 primary incidents since 25 Oct 2023

Embraer 190 19, 21 Sep
IRS lost position, full nav fail

G650 29 Aug
IRS/Nav fail, ATC vectors

Falcon 8X 12 Sep
80nm position spoof

CL650 15 Sep
HDG mode, ATC vectors

Global Express 16 Sep
IRS fail, FMS DR.

Boeing 777 10 Sep
IRS fail, ATC vectors

Boeing 737, & 747
IRS fail, ATC vectors

G650 & Global Exp 25 Oct
Led off track towards Lebanon

Falcon 2000LX 23 Oct
Spoofed position as LLBG

B777, A330, others 16 Oct
Spoofed position as LLBG

Global 7500 16 Oct
3 encounters, IRS fail

Source: OPS group

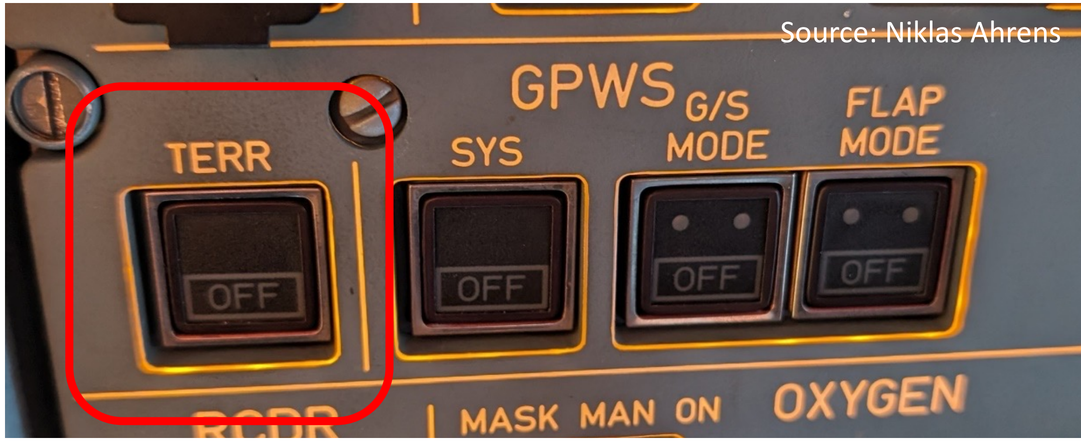
False Warnings

GNSS deselection is not possible for all systems

- The number of CFIT has decreased dramatically due to the development of Terrain Avoidance and Warning Systems (TAWS)
- System is using direct GNSS-signal input
- Deselection of GNSS is not possible for TAWS
- Very high level in warning hierarchy over ACAS/TCAS and Windshear
- Aural Warnings cannot be muted
- Procedures require strict adherence to avoidance manoeuvres after warnings

Problem:

Procedures would require either ignoring during long periods of false warnings or adherence in (dense) airspaces


Source: Niklas Ahrens

Recommendations

Procedures and System Design

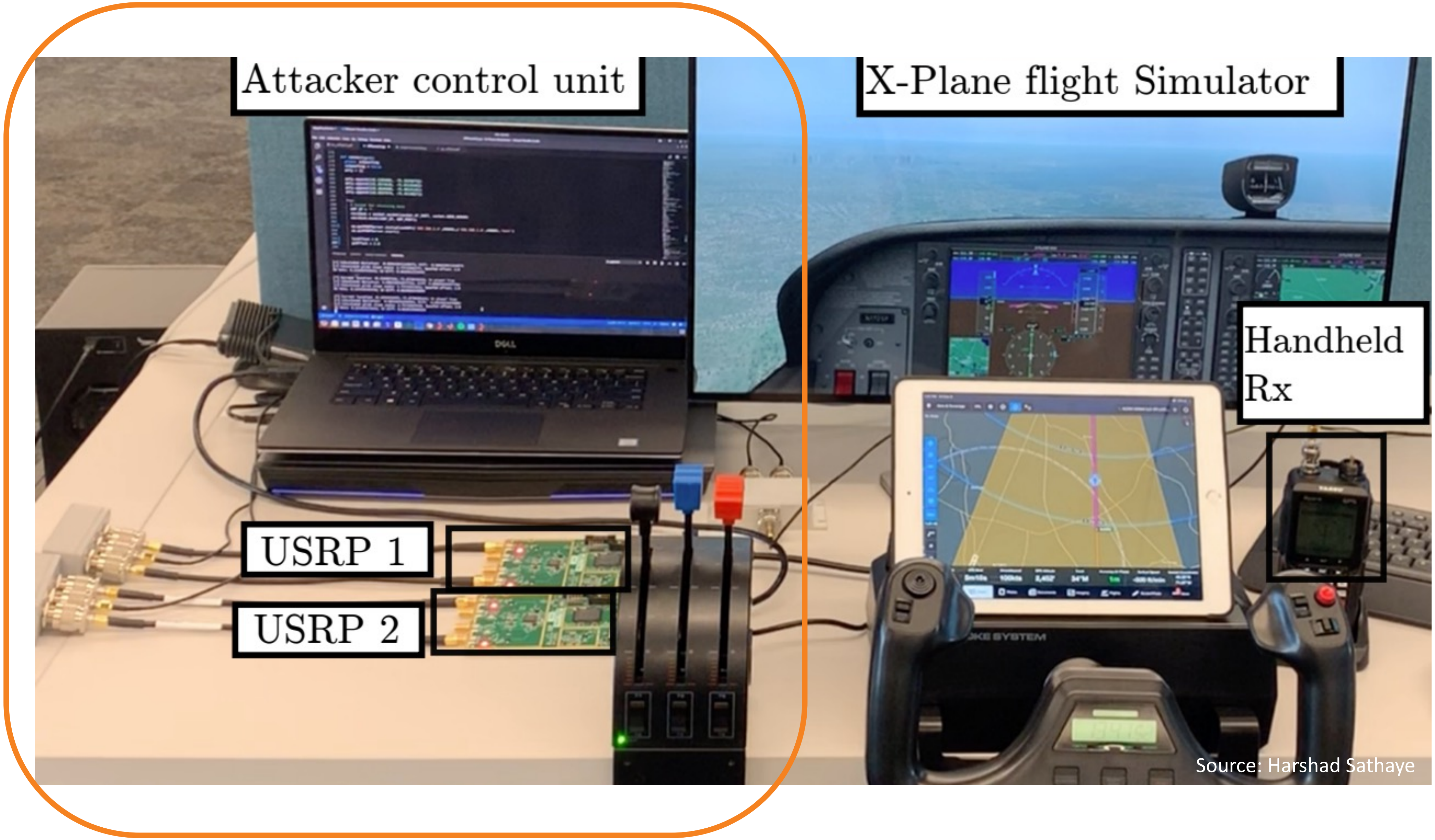
Source: Niklas Ahrens

☑ Have clear and unambiguous procedures based on a thorough risk evaluation (TAWS)

☑ Have clear procedures based on average pilot ability to detect different scenarios (GPS deselection)

☑ Have a thorough documentation of the system design

☑ Have a robust system design with independent IRS



Source: Harshad Sathaye

Source: Niklas Ahrens

Outlook

General Robustness

Standards based on common cybersecurity principles (ISO/IEC 27002):

Confidentiality

Integrity

Availability

MONTREAL
HQ
PARIS
Office
BEIJING
Sub-office
CAIRO
Office
MEXICO CITY
Office
DAKAR
Office
BANGKOK
Office
NAIROBI
Office
LIMA
Office

Thank You!

Niklas Ahrens, IFALPA, niklas.ahrens@vcockpit.de