

A short, thick orange horizontal bar is positioned to the left of the title.

JAMMING & SPOOFING DETECTION AND ALERT SYSTEMS FOR GNSS & PNT

IDEAS HOW SUCH A SYSTEM CAN BE EVOLVED FROM CURRENT BUILDING BLOCKS AND TECHNOLOGIES

STEPHAN ROEMER, BD MANAGER NAVIGATION, OH B GROUP

ISRMM 2026, BUCHAREST

01

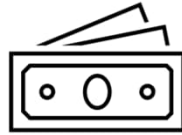
OHV & PNT/GNSS

OHB IN NUMBERS

TECHNOLOGICAL EXPERTISE IN EUROPE AND OVERSEAS
ONE OF THE THREE LARGE SPACE SYSTEM INTEGRATORS OF EUROPE



> 50
years
of experience



> 2 billion
EUR in OI
(plus backlog of 3 b€)

> 4.000
employees



> 30
nationalities



Germany | Italy | Sweden | Luxembourg | Czech Republic | Greece | Austria | UK | Belgium | French Guiana | Chile

We. Create. Space.

LATEST UPDATE - IRIS² - OHB SELECTED FOR MEO SEGMENT



OHB has been awarded a contract worth nearly €1 billion for the development and production of eighteen satellite platforms for the EU's IRIS² Secure Connectivity Programme

LARGEST FAMILY-OWNED EUROPEAN SPACE COMPANY



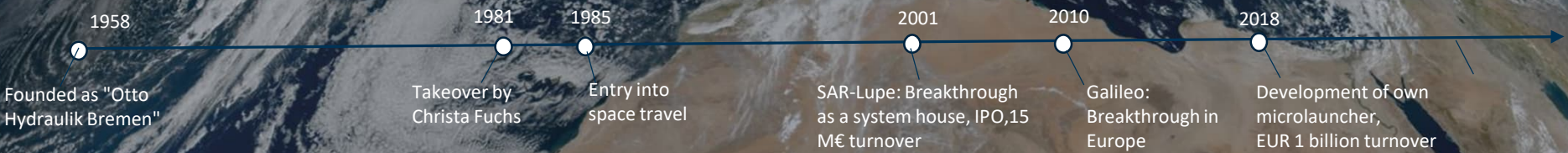
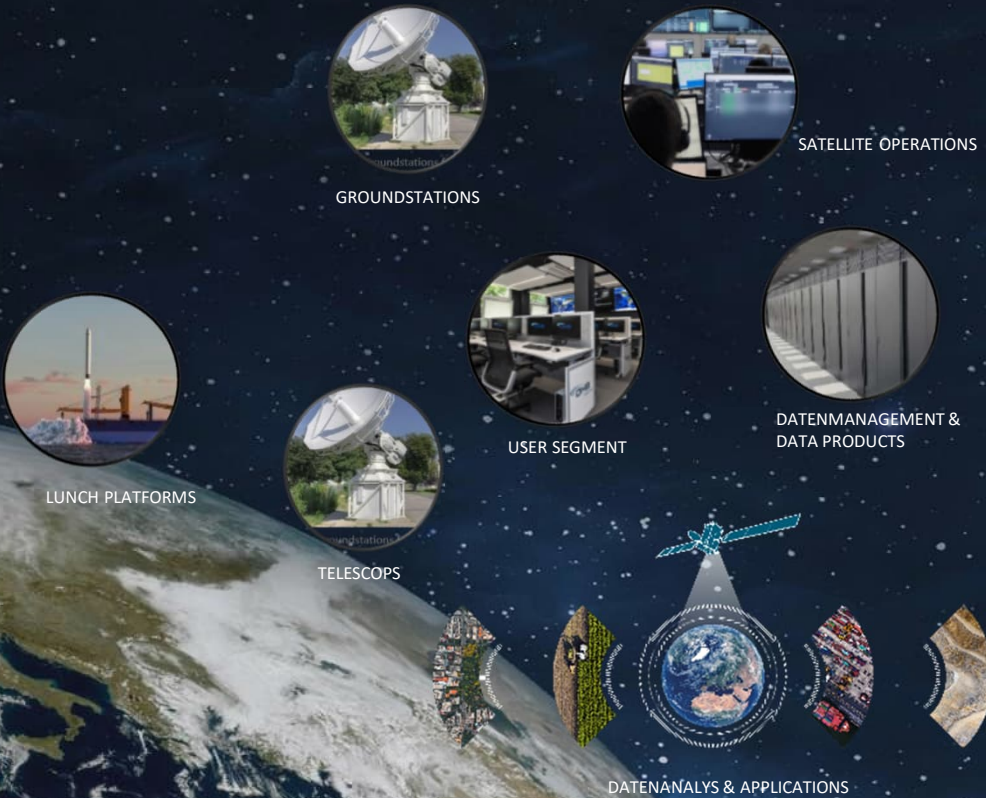
SPACE SYSTEMS



AEROSPACE

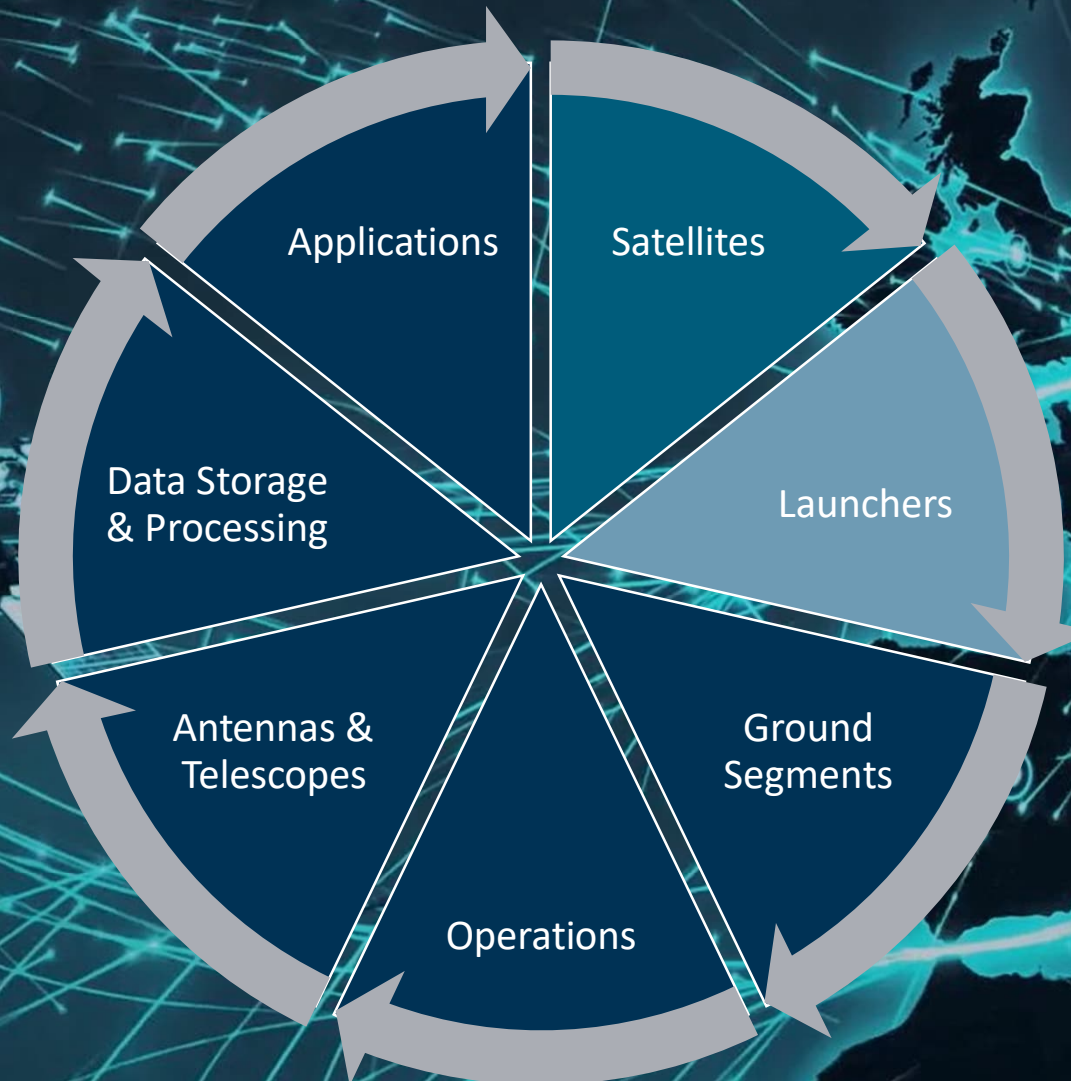


DIGITAL



END-TO-END SPACE SOLUTIONS

SPACE FROM A TO Z







GALILEO
EUROPE'S GLOBAL
NAVIGATION SATELLITE SYSTEM



G1G
(FOC Batch 3)



GSSOP 1 & 2



G2G
Testbeds, Studies
& Proposals



LEO-PNT
EUROPE'S NEXT GENERATION
PNT SERVICE



IOD
LEO-PNT In-Orbit Demonstration



IOPP
LEO-PNT Initial Operational
Pilot Programme



EU LEO-PNT FOC
Future Operational Constellation



OpSTAR
Optical Synchronised
Time And Ranging



Phase A/B1
(ongoing)



Phase B2/C/D(E/F)
(proposal phase)



PRECISION
TIMING



HIGH
ACCURACY



RESILIENT TO
JAMMING & SPOOFING



**RFI DETECTION
& RESILIENCE**
PROTECTING PNT SERVICES



NavGuard
RFI Monitoring &
Threat Detection



MOGSI / LISA
Interference Analysis &
Location



SAFIR-PNT
PNT Service Assurance
& Resilience



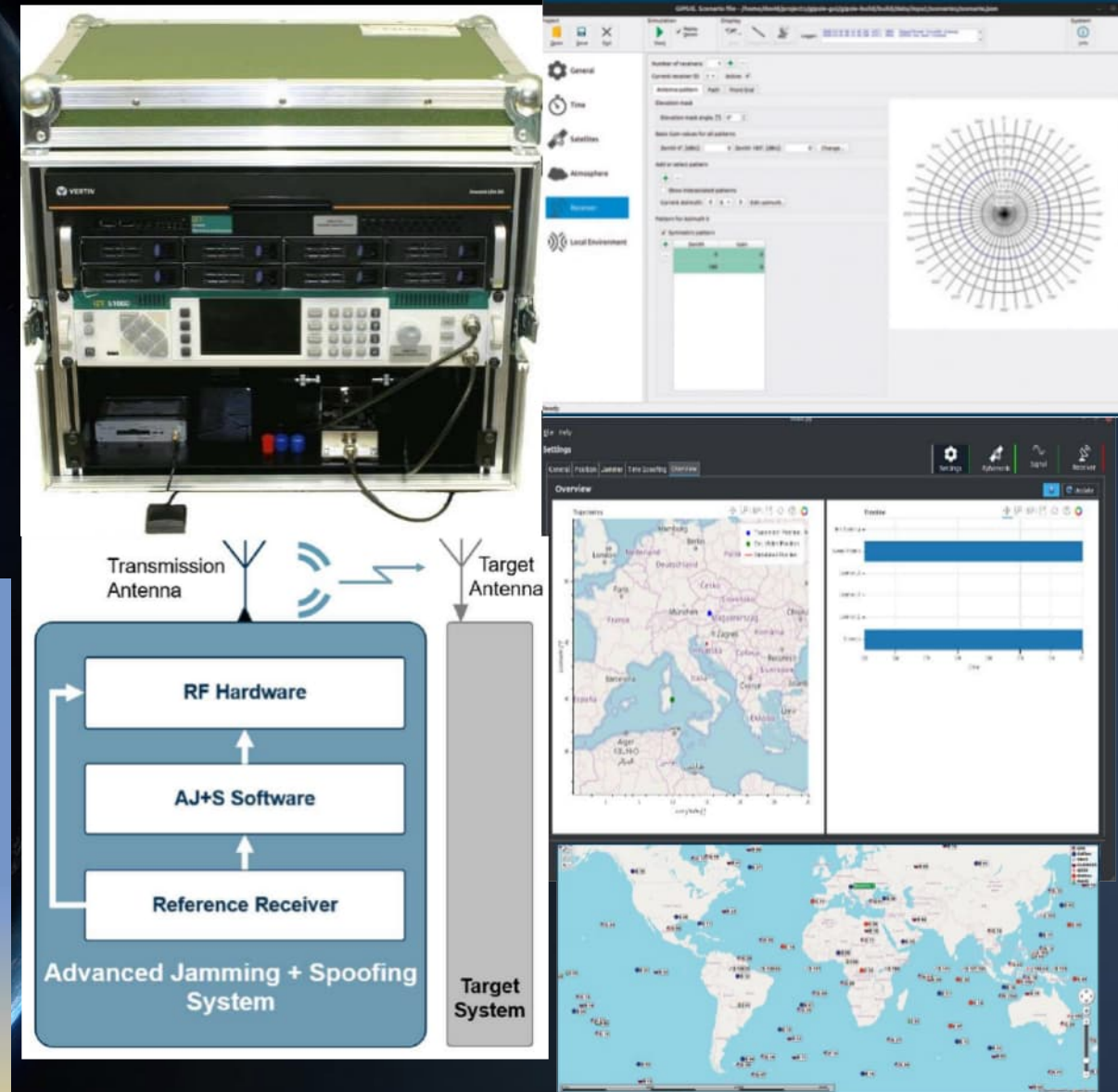
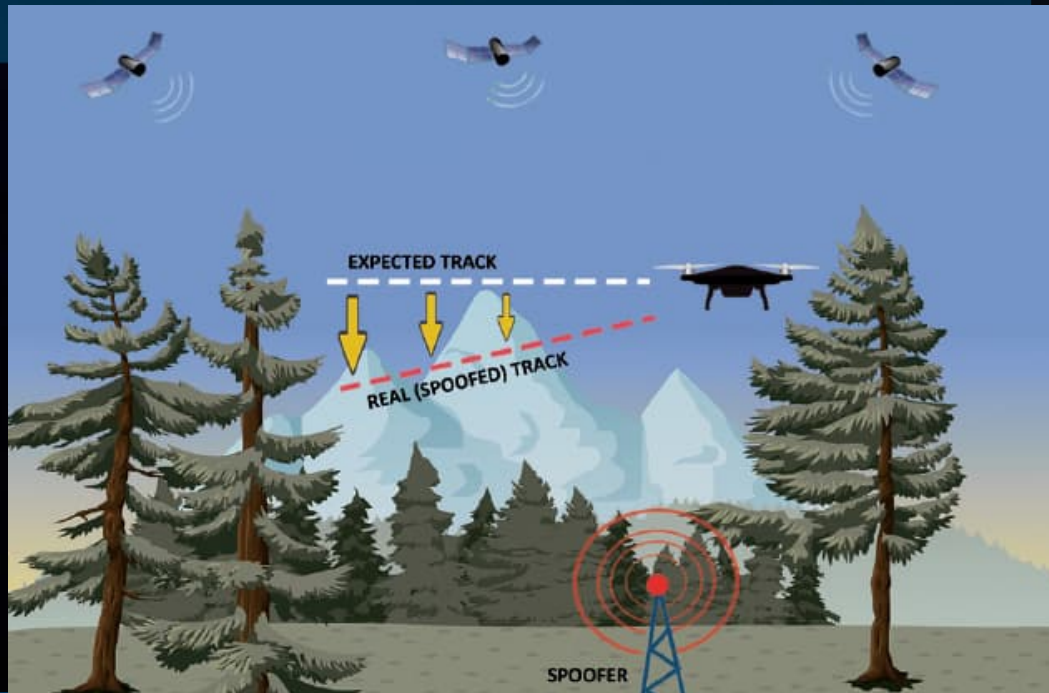
SIGNAL
INTERFERENCE



OHb
NAVIGATION
PIONEERING SPACE.
EMPOWERING EUROPE.

WHITE HAT - JAMMING AND SPOOFING

- For testing your jamming/spoofing monitoring and protection services you need to know everything about jamming and spoofing
- Therefore, we had developed our own AJ&S system for testing and military use cases
- Simulating/executing sophisticated jamming and spoofing attacks
- Including high end Signal generator for all GNSS –L band signals (e.g. GPS L1, L2,L5, Glonass, Galileo, Beidou, SBAS..)
- Integrated reference receiver for performing synchronized spoofing attacks



02

THE PROBLEM

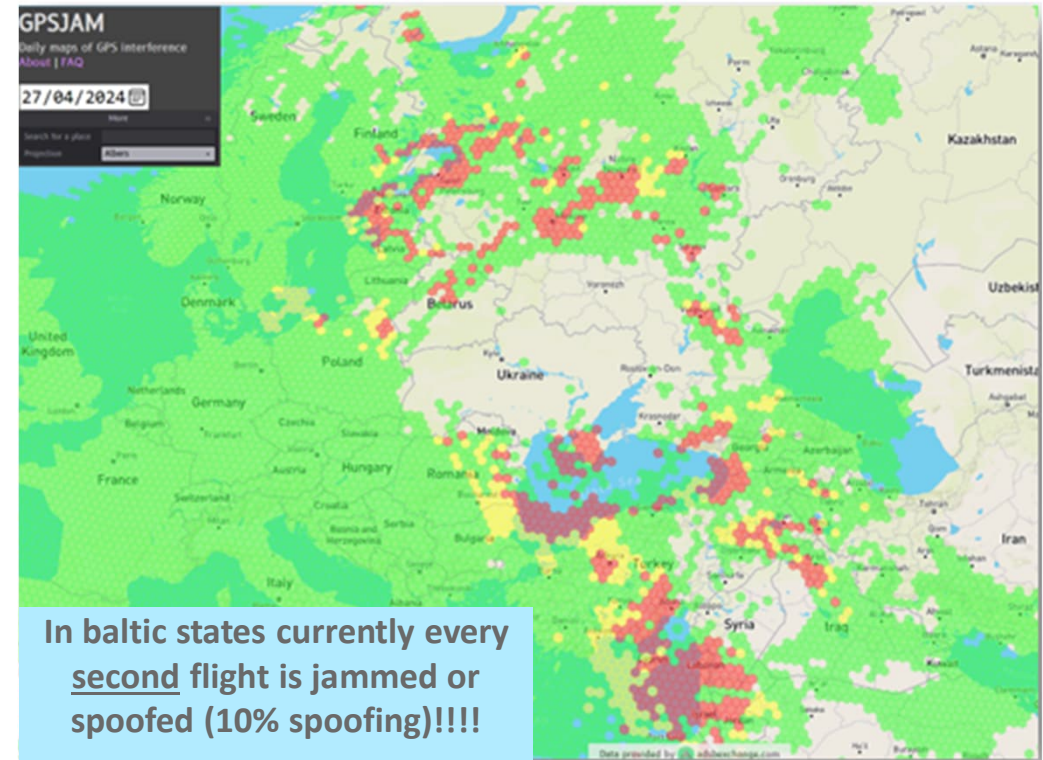
THE OBVIOUS THREAD TO GNSS

INTENTIONAL AND UN-INTENTIONAL DISTURBERS

Due to the increasing jamming and spoofing of governmental/military/black ops at different conflict zones in the world, it is obvious that these actors are using the jamming/spoofing not only for military actions, but also for hybrid warfare and sabotage.

Best known example here in Bucharest is of course the current situation at the EU eastern flank plus near east region.

Due to the conflict situation here, the political focus is (unfortunately) mainly on this thread source, but it is only half of the problem!!



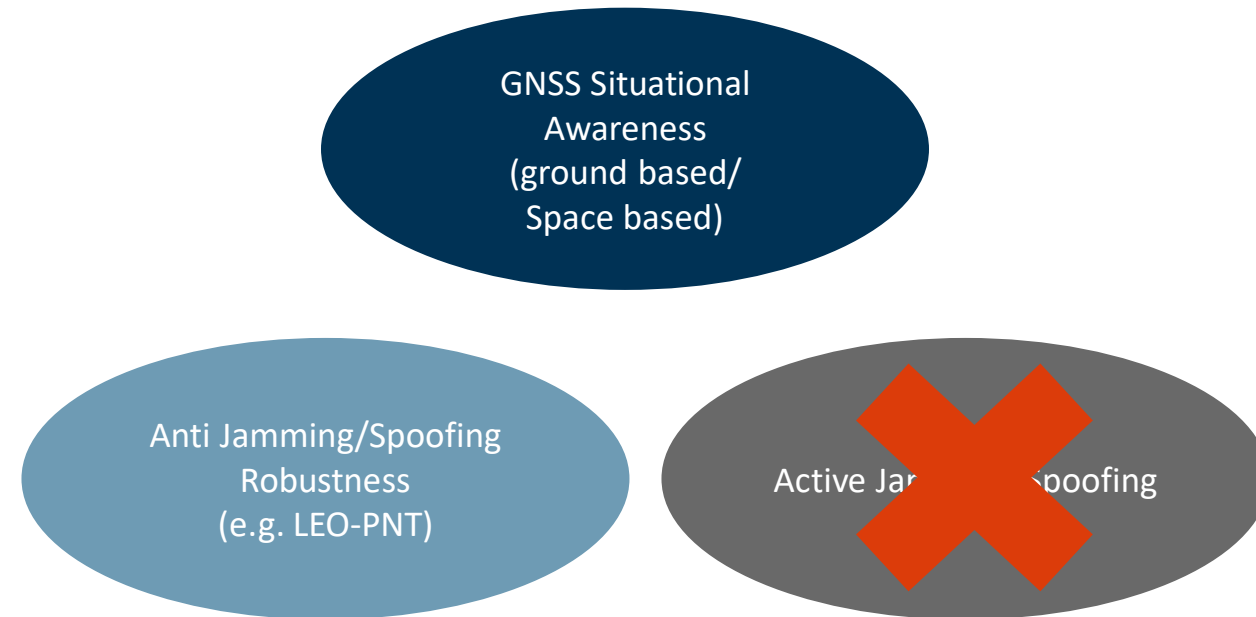
THE OFTEN FORGOTTEN PART OF THE PROBLEM

INTENTIONAL AND UN-INTENTIONAL DISTURBERS

- Beside governmental/military jamming and spoofing activities there is the massive increasing thread of individuals using jammers
- On main highways in northern Europe we detect such devices in interval of minutes, typically used by people who want to avoid toll, to be monitored by their employer or non-legal activities
- Loosing the navigation solutions is especially a thread to transport or logistics,
 - here two current examples
 - A truck with jammer was parked near the tower of a midsize airport and blocked GNSS landing approach for 30 min before removed
 - Container movers in European harbor lost GNSS due to a truck with jammer nearby. Massive capacity drop, because movers needed to be operated by teleoperator
- While such problems are locally limited, the problem of loosing the timing signal is MUCH more critical for important commercial and infrastructure sectors, as e.g. banking sector, energy grids, MNOs.....



- GNSS Situational Awareness
 - Detection, Geolocalisation and characterisation of Jamming/Spoofing (RFI)
- Anti Jamming/Spoofing-Robustness
 - Increase of Robustness of GNSS Systems
 - Hardware-based, e.g. CRPA Antennas
 - Software-based, e.g. Interference detection algorithm
 - Signal flexibility, e.g. Galileo/GPS, ARAIM, OSNMA, PRS
 - Signal diversity, e.g. LEO-PNT
- ONLY FOR MILITARY - > Offensive Jamming/Spoofing
 - Jamming/Spoofing Capabilities



03

MAKING SPACE BASED SIGNALS MORE ROBUST

MOVING TOWARDS A CONSTELLATION IN STEPS



LEO PNT Full Operational Capability:

LEO-PNT FOC is a resilient, robust and multi frequency Navigation and Timing System service of EU for governmental, defence and civil use. It will bring EU GNSS into next generation and will create a technical independent LEO layer towards Galileo. It will operate in parallel to G2G.

ESA

IOPP:

Industrialize Production for FOC Satellites
To be launched 2028/29 (tbc)

ESA

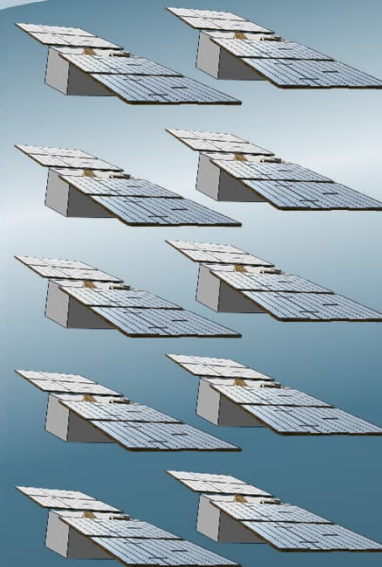
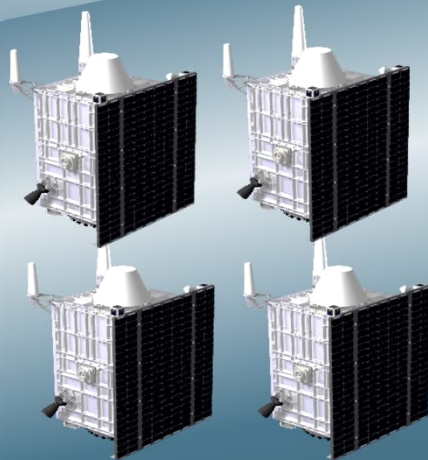
IOD Pathfinder B:

Industrialize Production for
FOC Satellites
To be launched 2027

ESA

IOD Pathfinder A:

Demonstrate Core Principle
and Technologies
Launched 2026

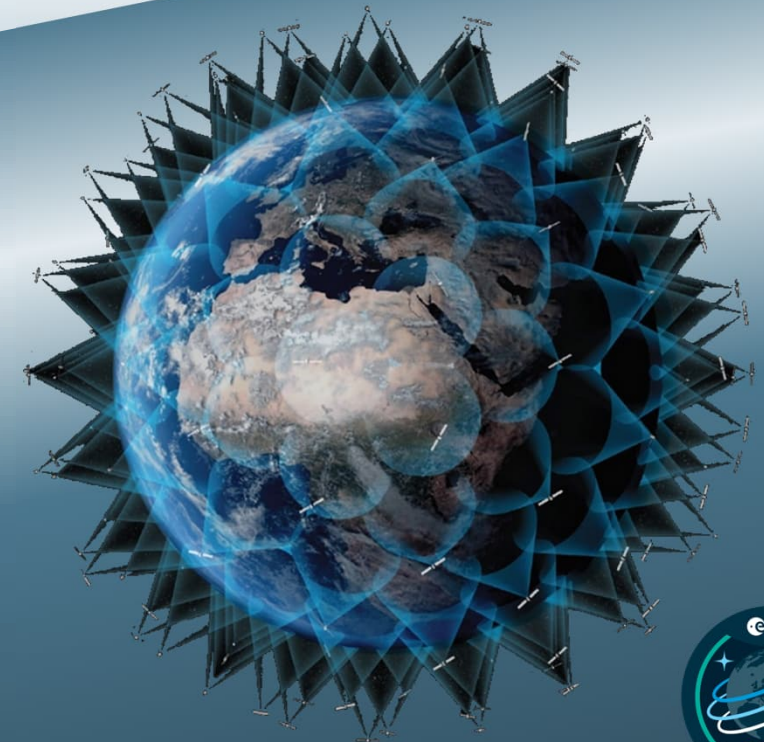


Replenishment, updates,
future generations

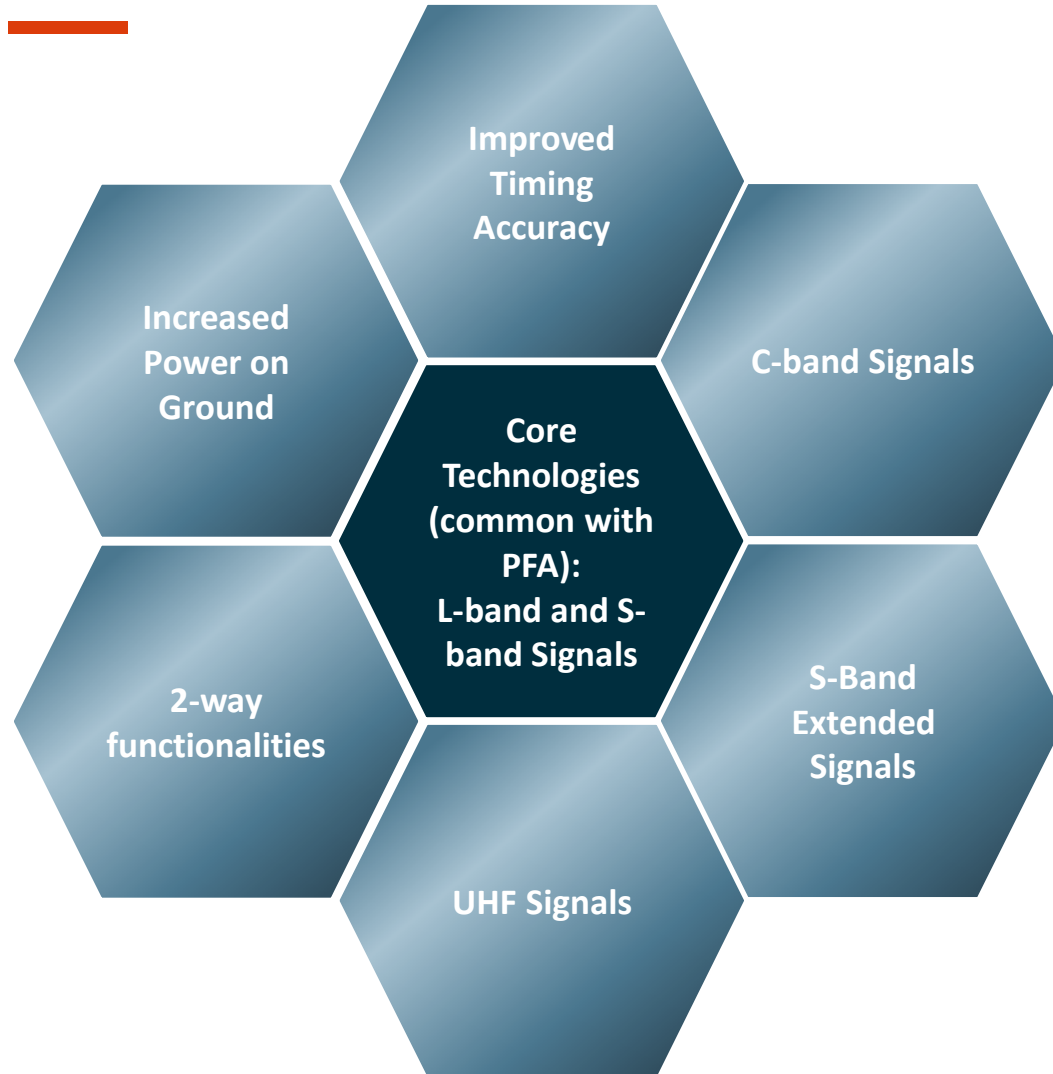
EU/EUSPA

Full Operational Constellation (FOC)

Initial Services 2032

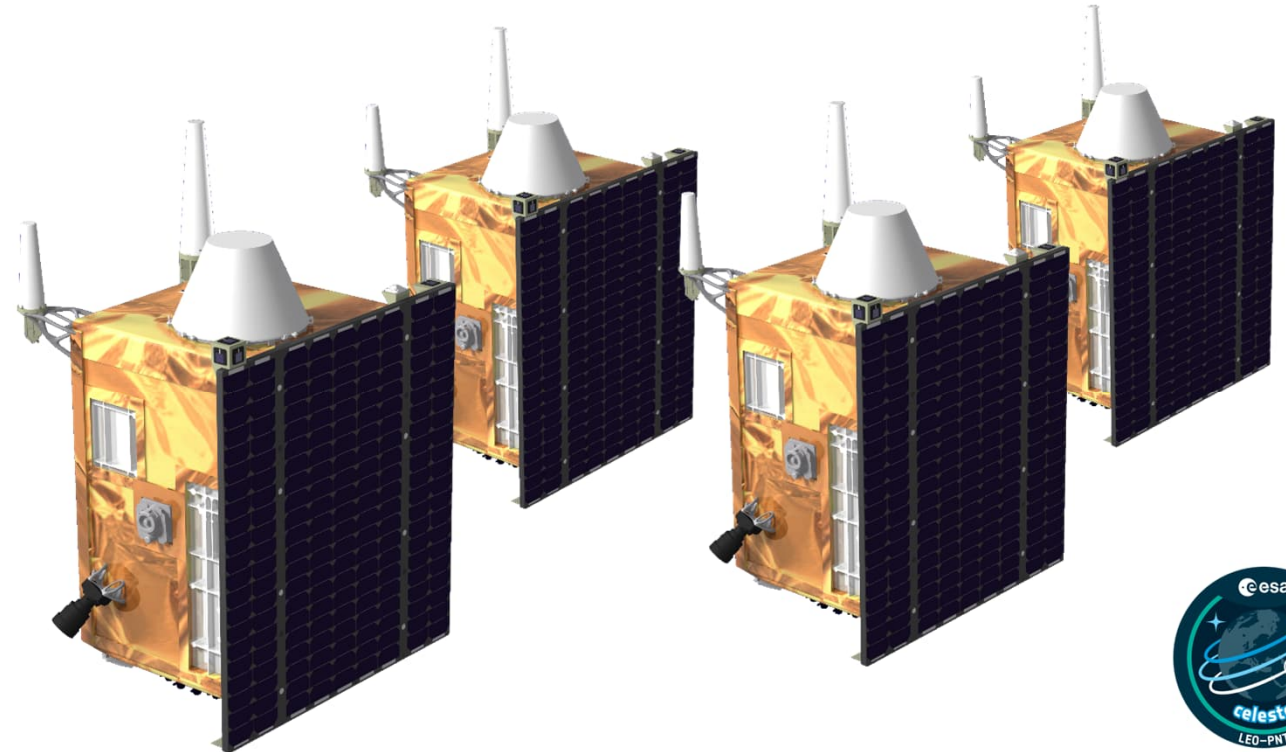


NEXT STEP: END TO END TESTS WITH FOUR PFB SATELLITES

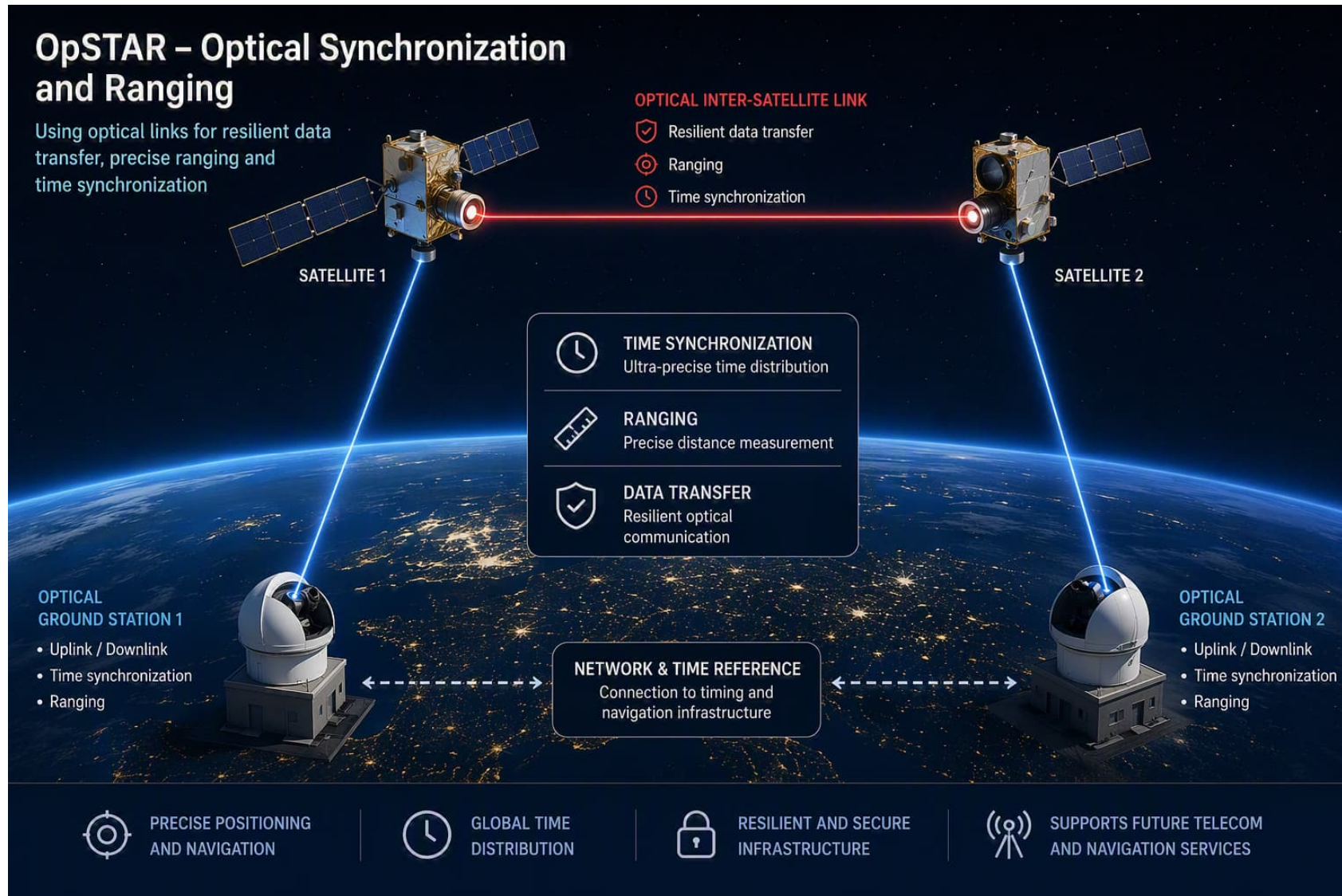


Services to be tested with Pathfinders B in 2027:

- L-band with increased power
- S-band with increased power and additional elements
- UHF-band navigation (enabling indoor navigation)
- C-band high-resilience and accuracy services



OPSTAR – OPTICAL SYNCHRONIZED TIME AND RANGING



04

PROTECTING PNT/GNSS SERVICES

- The impact of jamming/spoofing to our security and also the economic effect is increasing rapidly, and will do so also in the near future
- An adequate action plan here is urgently required, as e.g. seen in the EU documents and plans MFF28 for an EU RFI Alert System
- And there is not a single solution to fix that problem, but with some major building blocks a big percentage of the effect can be avoided

1. Protecting of critical infrastructure by stationary sensors

GNSS SITUATIONAL AWARENESS

STAGE 1 – GROUND BASED STATIONARY

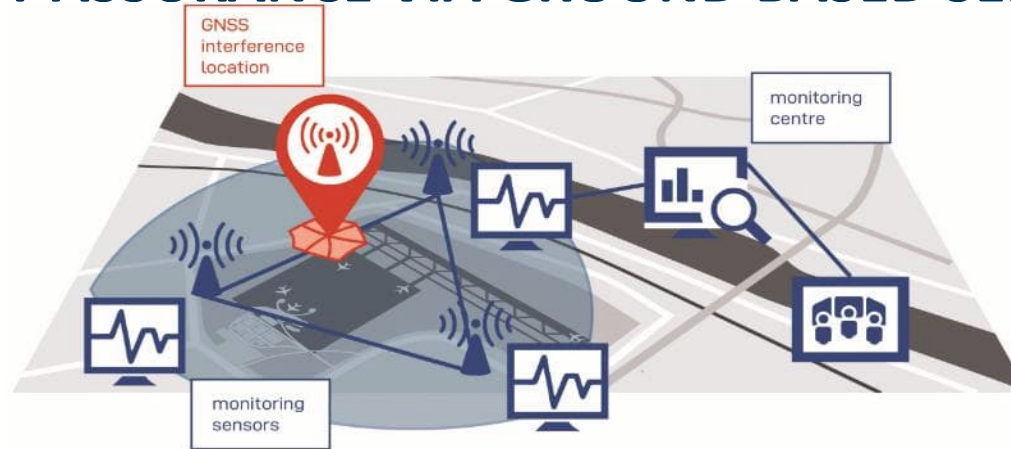
GNSS Situational
Awareness
(ground and space based)



GIDAS – GNSS QUALITY ASSURANCE VIA GROUND BASED SENSORS

GIDAS STATIONARY

- Ports
- Airports
- Toll Collection
- Power Grids etc.



ROMATSA: Integration of GNSS quality control systems at the 17 Romanian Airports in 2024/25



GRAZ AIRPORT



PORT OF TALLINN



BRNO AIRPORT



FRANKFURT AIRPORT



TOLL COLLECTION

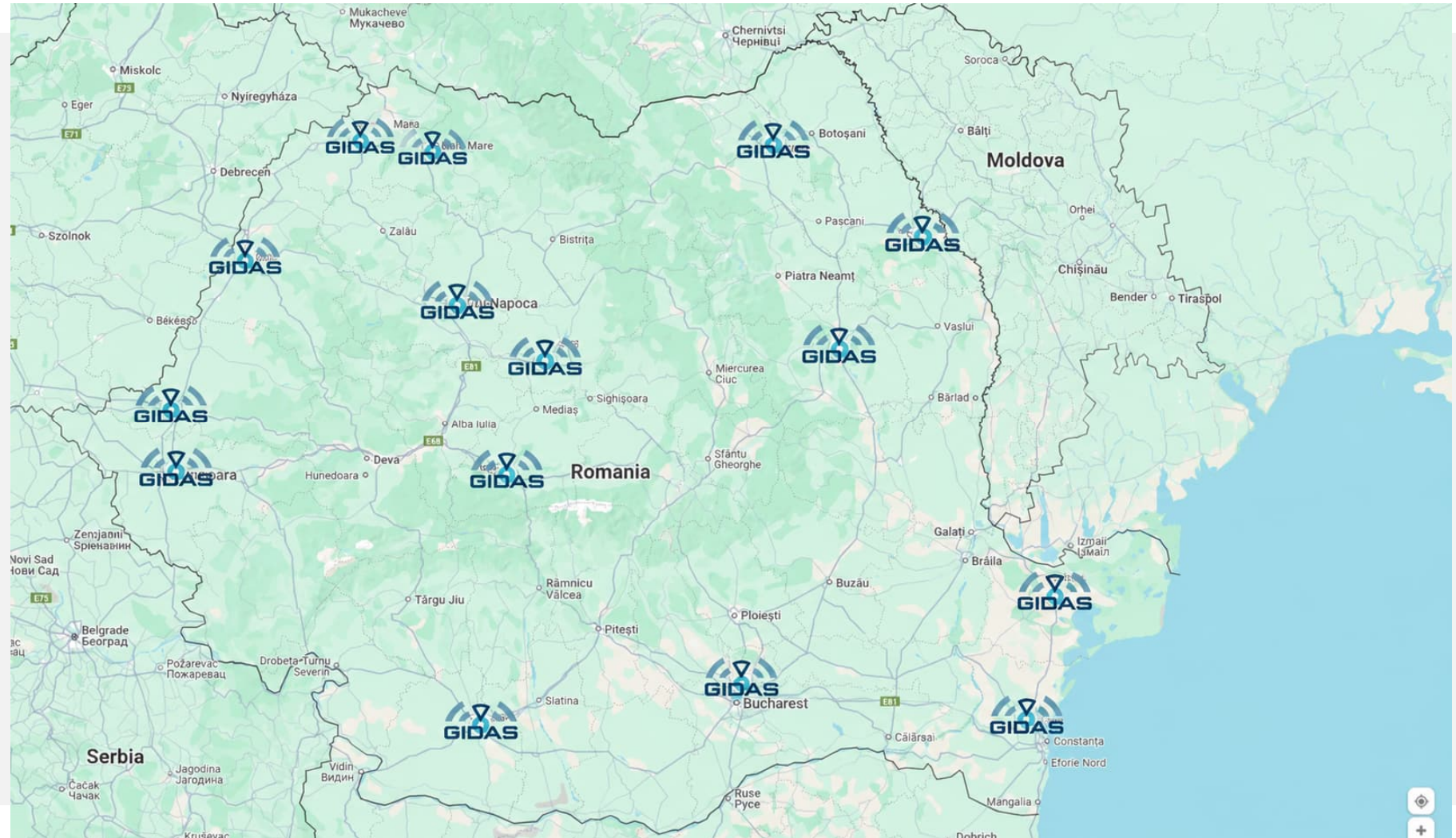
GIDAS IN ROMANIA

16 AIRPORTS – ONE NATIONAL MONITORING NETWORK

GNSS Situational
Awareness
(ground and space
based)



- OHB Austria currently **equips** the **entire country** of Romania **with GIDAS Stationary** (16 airports)
- **Nation-wide monitoring center** to collect data from all airports
- **24/7 real time** GNSS signal quality **monitoring**, jamming and spoofing **detection**



GIDAS IN ROMANIA

GIDAS STATIONARY – THE 24/7 GNSS MONITORING SOLUTION

GNSS Situational
Awareness
(ground and space
based)



Network of on-premise GIDAS monitoring sensors

- Spatially distributed, on-premise GNSS sensors cover the area of interest
- 24/7 monitoring of the local GNSS service quality and interference situation
- Bearing estimation of local interference sources and localization of the threat by Angle of Arrival (AoA)

Central GIDAS monitoring center

- Local data processing without costly cloud infrastructure
- On-premise data hosting – full control of the recorded data
- Central data archive for post processing and analysis of interference events
- Web-based user interface for seamless operational integration
- Custom alert interface – depending on the operational context

**PRECISION.
PROTECTION.
PERFORMANCE.**

Reliable GNSS monitoring
for a secure and resilient
infrastructure.



**DETECT
THREATS**
in real time



**ENSURE
CONTINUITY**
of critical services



**BUILD
RESILIENCE**
for the future

OHB Austria equips Romania with GIDAS for GNSS Interference Detection.



We are proud to contribute to safer aviation across **Romania.**



Implementation Roadmap

- December 2023:
Project awarded through competitive tender process
- H1 2024:
Detailed design and solution development
- October 2024:
Factory Acceptance Test (FAT) successfully completed
- H1 2025:
Pilot installation and field testing at three reference airports
- H2 2025 - ongoing
Full-roll-out and phased implementation

- The impact of jamming/spoofing to our security and also the economic effect is increasing rapidly, and will do so also in the near future
 - An adequate action plan here is urgently required, as e.g. seen in the EU documents and plans MFF28 for an EU RFI Alert System
 - And there is not a single solution to fix that problem, but with some major building blocks a big percentage of the effect can be avoided
-
1. Protecting of critical infrastructure by stationary sensors
 2. **Sophisticated Mobile Sensors AND Software embedded in receivers**

GNSS SITUATIONAL AWARENESS

STAGE 2 – PORTABLE AND MILITARY SYSTEMS

GIDAS Portable

- The portable, standalone GIDAS designed to be deployed at any place at any time
 - Law Enforcement
 - Frequency regulation authorities
 - Toll Collection
 - Airports
 - Etc.
 - MilGIDAS in final Development



GIDAS Embedded

- Directly integrated into receivers for
 - Time Servers,
 - Bank Houses, Stock Exchange
 - Drones
 - Navigation systems
 - Auto-pilots
 - Etc.



The availability of constant connectivity via 5G/6G and D2D in the near future, combined with future PNT/GNSS, would allow to use major user groups (as logistic companies, Energy grid operators, MNOs,..) to be the source of data from mobile sensor network, by embedding software that not only detects that a jamming/spoofing is happen, but also delivers information about the characteristics. And that delivers this information in real time into an Quality of Signal & Alert Service.

By „Alliance of the Willing“ or do we need here a governmental action plan?

- The impact of jamming/spoofing to our security and also the economic effect is increasing rapidly, and will do so also in the near future
 - An adequate action plan here is urgently required, as e.g. seen in the EU documents and plans MFF28 for an EU RFI Alert System
 - And there is not a single solution to fix that problem, but with some major building blocks a big percentage of the effect can be avoided
-
1. Protecting of critical infrastructure by stationary sensors
 2. Sophisticated Mobile Sensors and Software embedded in receivers
 3. **A space based Jamming/Spoofing detection constellation (or hosted payloads) to cover open waters, rural or hostile ground**

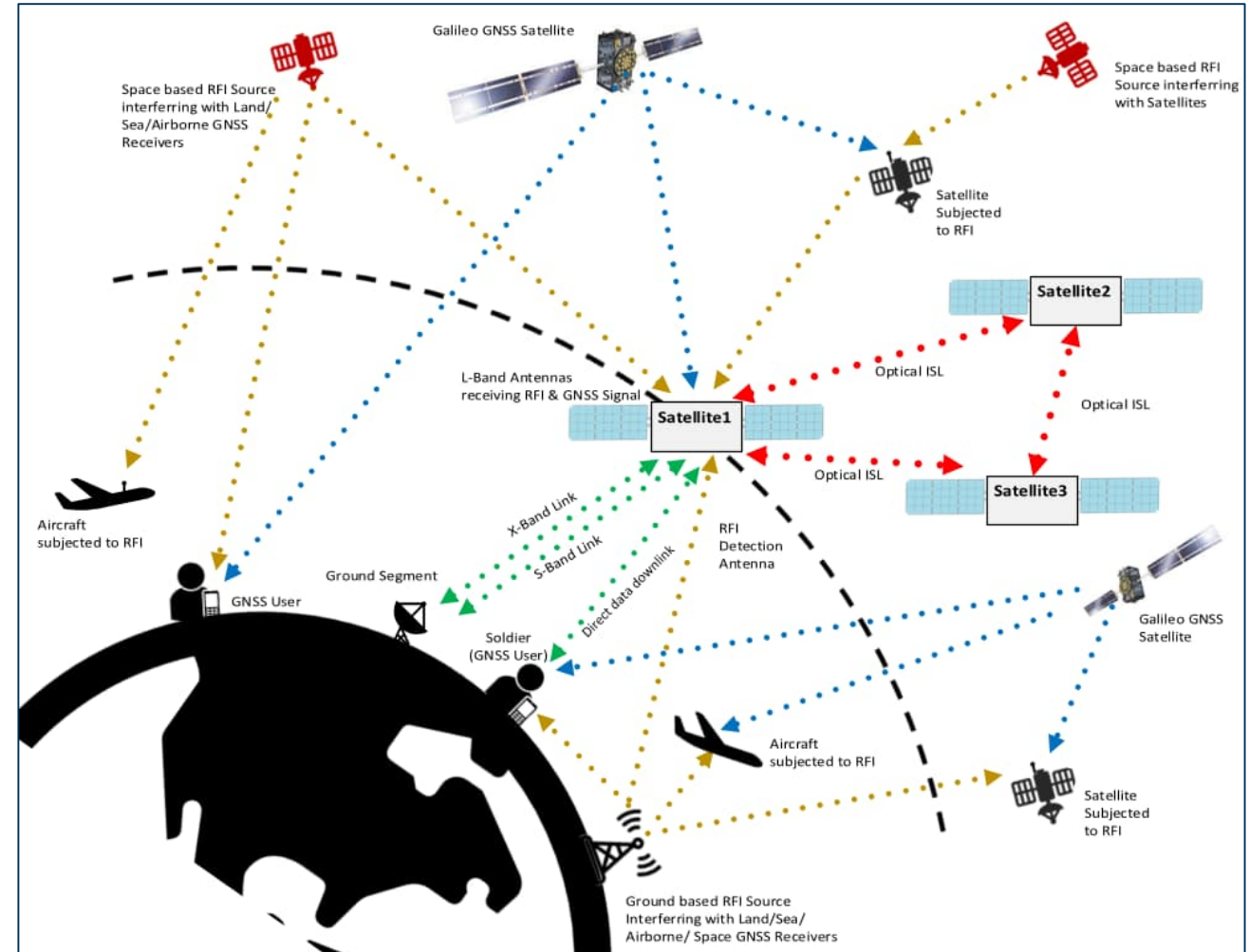
GNSS SITUATIONAL AWARENESS FROM SPACE

SPACE BASED JAMMING/SPOOFING DETECTION (E.G. EUSPA)

GNSS Situational
Awareness
(ground and space based)



- System for high performance military and civil Jamming Spoofing detection (incl. high precision geolocation, classification, fingerprinting)
 - High performance needed to empower blue force to act against identified RFI source and to record „court proof“!!
- Triplets of Satellites in Formation Flying
- Orbit 500 to 600 km
- Inclination SSO or (for constellation) 65°
- Microsat ~100 kg
- OISL for data exchange, time synch and position/distance measurement
- Payload currently developed in National Program as well as in EDF program lines, as MOGSI/LISÁ

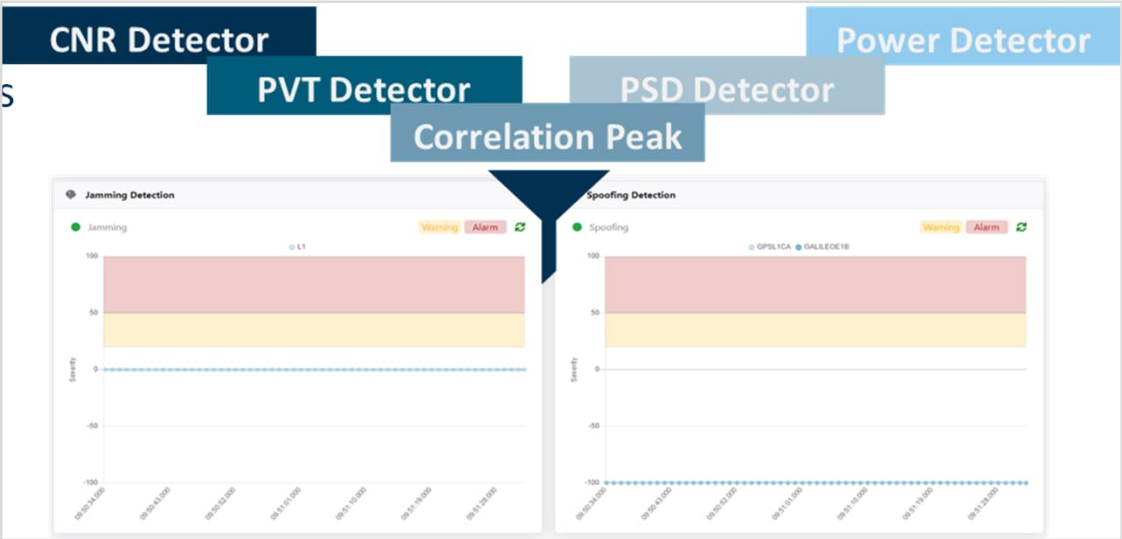


- The impact of jamming/spoofing to our security and also the economic effect is increasing rapidly, and will do so also in the near future
 - An adequate action plan here is urgently required, as e.g. seen in the EU documents and plans MFF28 for an EU RFI Alert System
 - And there is not a single solution to fix that problem, but with some major building blocks a big percentage of the effect can be avoided
-
1. Protecting of critical infrastructure by stationary sensors
 2. Sophisticated Mobile Sensors and Software embedded in receivers
 3. A space based Jamming/Spoofing detection constellation (or hosted payloads) to cover open waters, rural or hostile ground
 4. **Data fusion into and combined Quality of Signal Service and Alert Service**



RFI ALERT AND ACTION SYSTEM

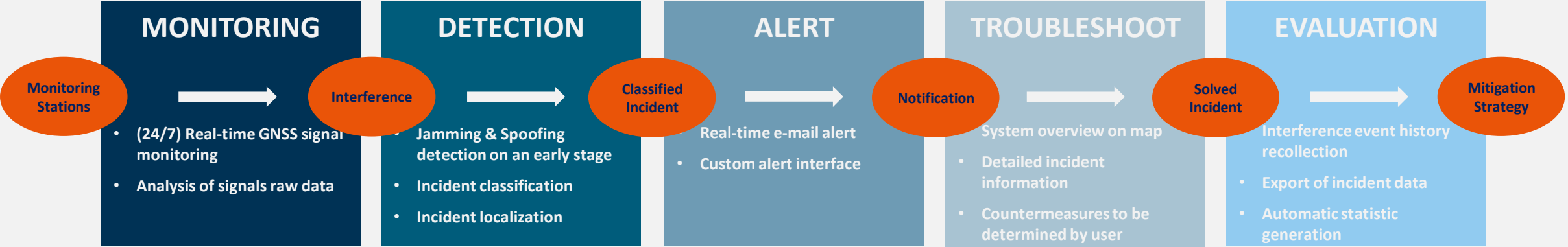
1. Combining Multiple detection techniques and sensor sources
2. Quasi Real Time
3. Weighted combination of multiple techniques to improve robustness
4. Simple to read and interpret decision metrics for jamming and spoofing



Problem: Data Governance!!

Can be done by commercial operator BUT must be hosted/controlled by governmental entity! Because it need to be REALTIME Information

Can it be EUSPA (MFF28)?



- The impact of jamming/spoofing to our security and also the economic effect is increasing rapidly, and will do so also in the near future
 - An adequate action plan here is urgently required, as e.g. seen in the EU documents and plans MFF28 for an EU RFI Alert System
 - And there is not a single solution to fix that problem, but with some major building blocks a big percentage of the effect can be avoided
1. Protecting of critical infrastructure by stationary sensors
 2. Sophisticated Mobile Sensors and Software embedded in receivers
 3. A space-based Jamming/Spoofing detection constellation (or hosted payloads) to cover open waters, rural or hostile ground
 4. Data fusion and transfer into a combined Quality of Signal Service and Alert Service
 5. **Empowerment of Police or other blue forces to act immediately in case of detection of threads to the PNT/GNSS signals**



QUESTIONS ?

Stephan Roemer

OHb SE

Manfred Fuchs Platz 2-4

28359 Bremen

Germany

Phone: +49 421 2020 8

Fax: +49 421 2020 700

Email: stephan.roemer@ohb.de

Web: www.ohb.de