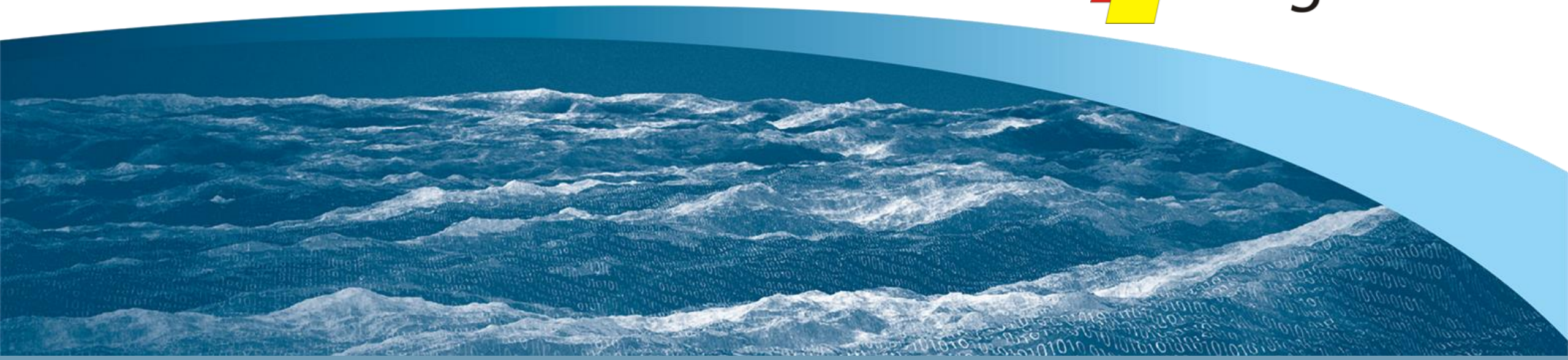
OHB Digital Solutions GmbH
Video Conference, 2020-09-04

M. Kadletz, P.B. Ober, K. Eschbacher



Final Presentation

Sp-ATM – Techniques for spoofing detection and mitigation in Aeronautical receivers

OHB Digital Solutions - Company profile

- OHB Digital Solutions GmbH (TeleConsult Austria GmbH), founded 1999, acts as prime partner for anyone looking for data solutions in the arena of Positioning, Navigation and Mobility.
- TeleConsult is since December 2018 a member of the OHB Group of Companies
- Strong cooperation with
  - Fraunhofer – IIS, Germany
  - BMLV, Bundeswehr
  - TU Graz University of Technology

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

OHB Digital Solutions - “The Navigation Experts”

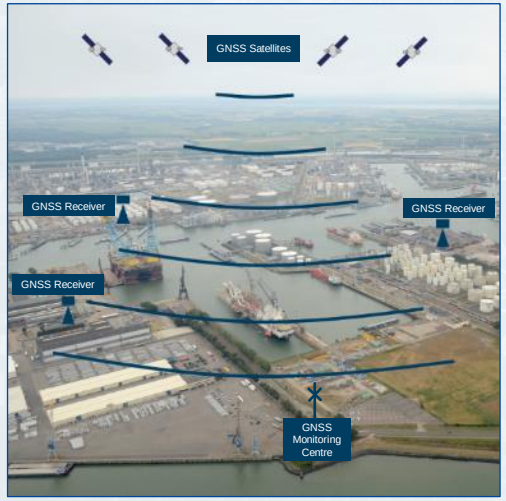
- Our field of work is
  - Precise positioning and reliable navigation
  - Development of navigation, telecommunication and information technologies
  - Services for applications in the context of transport and mobility.
- Our value streams
  - Telematics and technical consultancy in the field of GNSS
  - Location-based services
  - GNSS algorithm and software development, as well as simulation and testing
  - IoT devices and solutions
  - Defence – GNSS quality assurance

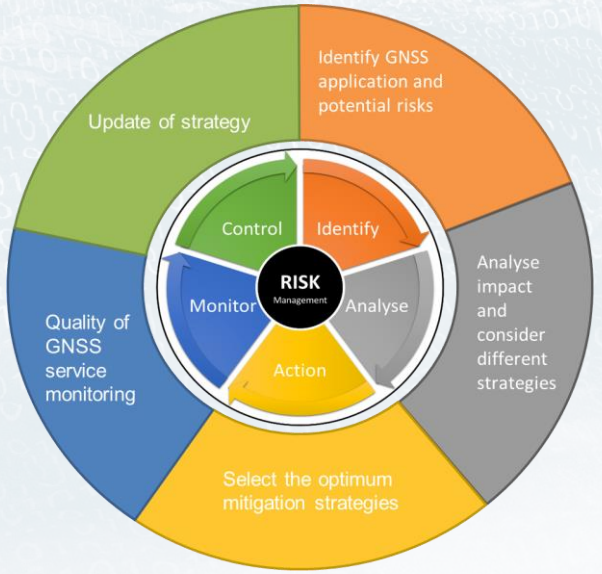
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

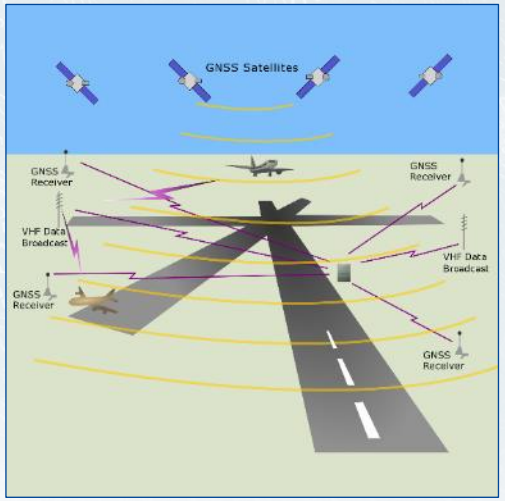
OHB Digital Solutions - GNSS Quality Assurance

- OHB Digital Solutions GmbH provides services for quality assurance for your GNSS data with the product GIDAS.
- If you have a need for an effective quality assurance system for GNSS-based multimodal positioning, navigation or timing services GNSS Quality Assurance is indispensable.

GIDAS
GNSS Interference Detection & Analysis System







OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Integricom – Company Profile

- Founded in 1998
- Technical consultancy in the field of navigation systems.
- Specializes in performance-related issues
- Has a proven track record with Eurocontrol, national aviation authorities, industry and navigation service providers
- Actively participates in the Eurocae Working Group 62 on Galileo.
- Member of Eurocontrol's ESTB/EGNOS data collection network in cooperation with the Technical University of Budapest

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Integricom – Expertise (excerpt)

- Participation to Eurocae Working Group 62 on Galileo, developing a multi-system GNSS receiver standard
- Design and validation of software-defined receiver algorithms for dedicated GNSS signal monitoring solutions [GASHIMOV]. In cooperation with Astron (NL), NLR (NL) and Science & Technology (NL). Project commissioned by the Netherlands Space Office.
- Integration of GNSS interference and spoofing sensors into Integricom's and DWI's GPMS GNSS monitoring system [GMCA]. In cooperation with DW international (UK), Spirent (UK), Qascom (IT) and Chronos Ltd. (UK). Project commissioned by the European GNSS Agency (GSA) under a Horizon 2020 grant

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Integricom – Expertise (excerpt)

- Algorithm and data processing design, validation and verification for a GNSS data processing system to characterize ARAIM performance [MCLTGA]. In cooperation with Iguassu Software Systems (CZ). Project commissioned by ESA.
- Design, development and operation of GNSS system monitoring facilities (currently operational at Korean, Chinese, Bulgarian and Saudi airports) [GPMS]. In cooperation with DW international (UK) (now NAVBLUE). This is a commercial system.
- Study on the use of combined GPS and Galileo (with a focus on RAIM). Study commissioned by Eurocontrol.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Paris Lodron University Salzburg – Company Profile

- Office Location
  - Jakob-Haringer-Straße 2, A-5020 Salzburg, Austria (Aerospace Research)
  - Jakob-Haringer-Straße 3, A-5020 Salzburg, Austria (Aviation Competence Center)
- Project related experience

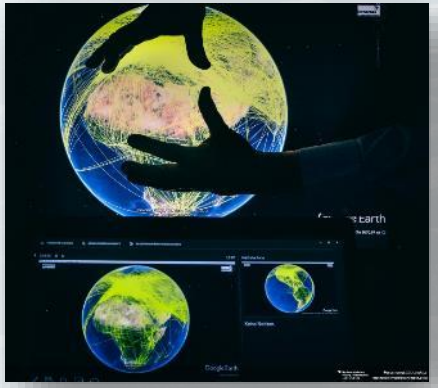
  Aerospace Research Salzburg has been involved in numerous European and national projects
  - 5th, 6th, and 7th European Framework Programme
  - Horizon 2020 Programme
  - ESA, Eurocontrol, SESAR, Inmarsat
  - Programme of the Austrian Research Promotion Agency (FFG)
  - Etc.

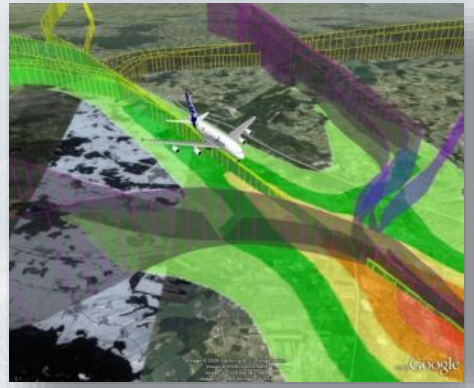
Paris Lodron University Salzburg – Company Profile

- Our field of work is
  - Digital Aeronautical Communications (Airp.,Terrestr., Satellite)
  - Optimization of airport operations & decision support tools
  - ATC/Remote Tower Control Training (automatic speech recognition)
  - Weather impact on ATM/ATC, Volcanic Ash, Space Debris
  - Innovative Arrival & Departure Procedures (GBAS, EGNOS)
  - Advanced cockpit simulation (ASR) & Flight deck perspective
  - Remotely piloted aircraft systems (RPAS/UAV)
  - Impact of Cyber-Attacks on Air Traffic Control mission
  - And others

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Paris Lodron University Salzburg – Company Profile





Communication

- Development of new wireless technologies
- Integration of networks
- Communication security

Air Traffic Management / Control

- Automated support
- Human in the loop evaluation
- Mission planning

Environment

- Air traffic forecast simulation
- Weather impact
- Noise abatement
- CO_2 reduction

Sp-ATM –
Techniques for spoofing detection and mitigation in Aeronautical receivers

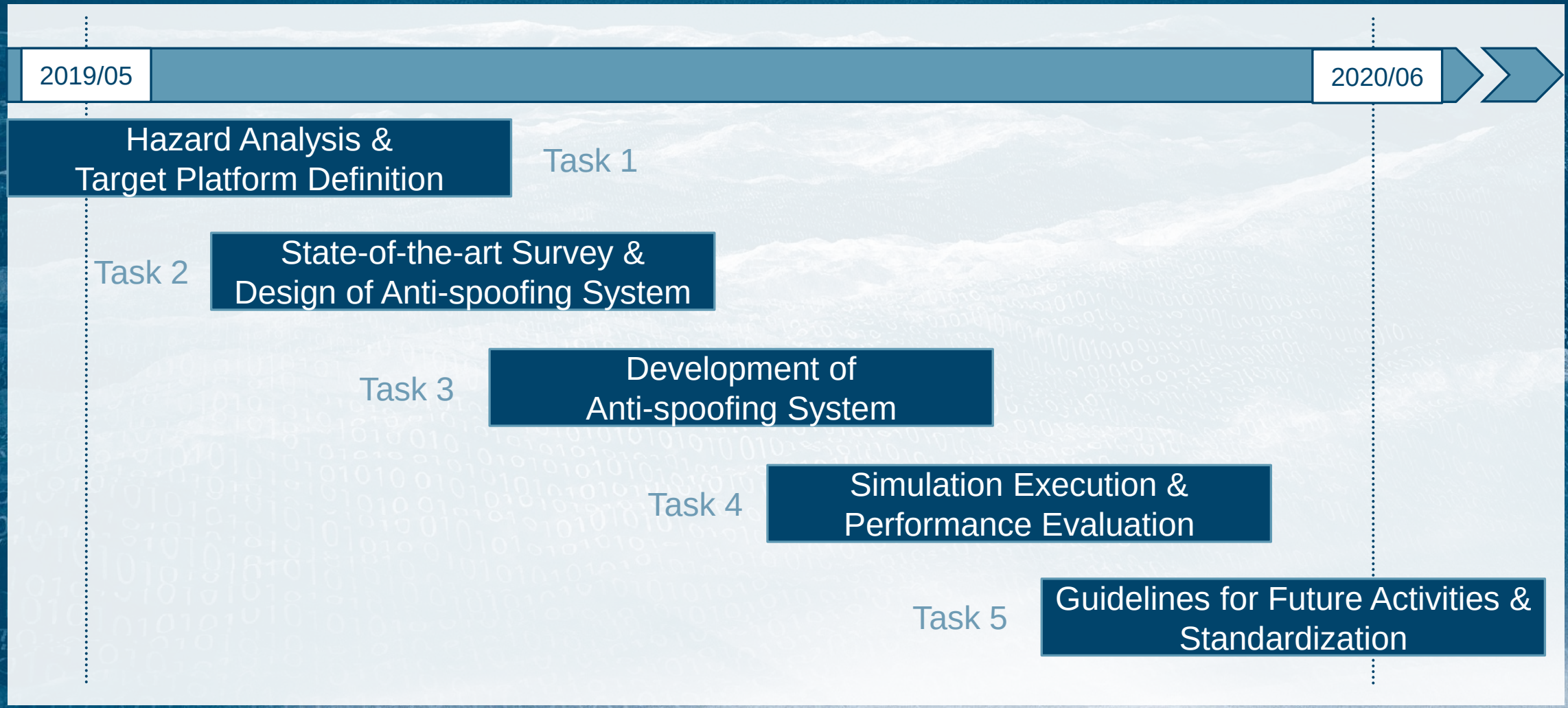
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Sp-ATM - key points of the activity

- Scheduled activity runtime: 12 months (2019/05 to 2020/06)
- Objectives:
  - Identification of hazards that may arise from GNSS spoofing events for aeronautical receivers (receiver installed in an aircraft) throughout the different phases of the mission
  - Definition of minimum requirements for any GNSS spoofing detection and mitigation technique to considerably reduce the risks
  - Based on the identified requirements
    - Exploration of different anti-spoofing solutions
    - Demonstration of their feasibility and performance using a simulation platform

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Sp-ATM - Schedule



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Hazard Analysis & Platform Definition

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS interference basics

- Unintentional interference
  - Natural causes or external systems (multipath, DME, etc.)
- Intentional interference
  - **Jamming**
    - Jamming's objective is denial of navigation service by masking GNSS signals with noise
    - Intentional transmission of RF energy to hinder a navigation service by drowning (masking) GNSS signals with noise
    - Objective to cause a receiver to lose tracking and impede signal reacquisition
  - **Spoofing**
    - Spoofing refers to the transmission of fraudulent GNSS-like signals, that force the victim receiver to compute erroneous positions (and/or time).
  - **Meaconing**
    - Interception and rebroadcast of navigation signals (like multipath)

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Aeronautical spoofing risk (1/2)

Spoofing Threat Space

“Spoofing attacks open a very broad spectrum of GNSS threat space. During this activity we identified and classified different parts of the spoofing threat space with respect to the aeronautical domain. ”

Spanned by: **Attack Type + Attack Settings**

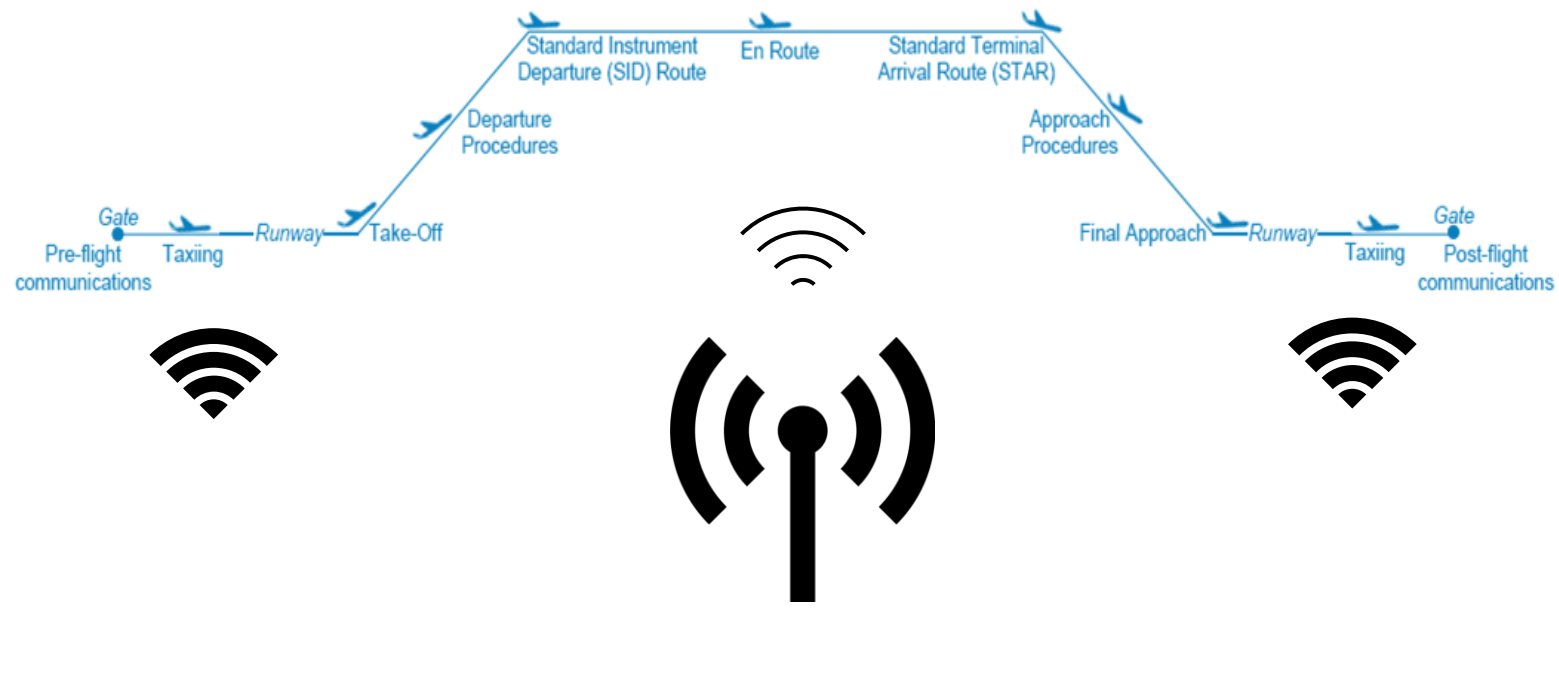
- Hardware-based classification of spoofing attacks
- Classification of spoofing attacks based on the spoofing strategy
- Transmission Power
- Multi-Frequency Multi-GNSS Spoofing Considerations

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Aeronautical spoofing risk (2/2)

Affected Flight Phases

- On ground
- In flight (TMA/airport)
- In flight (ENR)



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

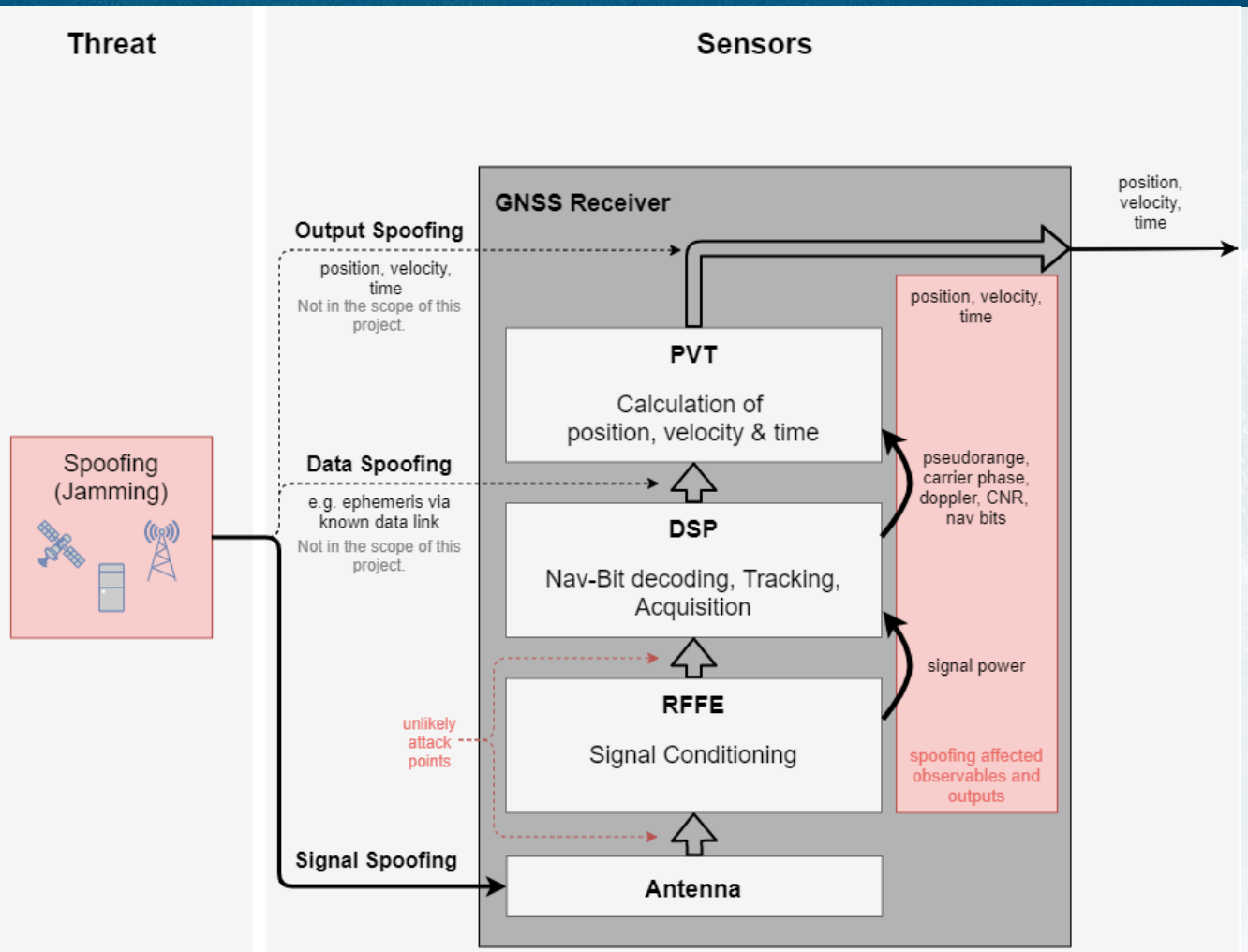
Potential attack scenarios

- Most vulnerable flight phases are during approach/landing and take-off/departure. Easily attackable with stationary, ground-based attackers.
- “Silent” spoofing, without interrupting GNSS service, is quite complex. It requires some knowledge of the target position.
- The higher the complexity of a spoofing attack, the higher the success rate of the attack. On the other hand, the complexity decreases the likelihood of an attack.
- It is important to note, that the spoofing threat space is permanently evolving, and that it can never be covered entirely by one single anti-spoofing system. This understanding has to be considered during design decisions.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Aeronautical spoofing risk – attack vectors

Spoofing Impact Overview



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Hazard analysis - summary

- Versatile, multi-dimensional threat space to cover for aeronautical anti spoofing systems.
- The threat space will evolve over time, thus a flexible design approach is favourable.
- Different threats are not equally likely to occur. Very complex and/or costly attacks might be neglected in design decisions.
- Different flight phases have different requirements in terms of flight procedures and are not equally vulnerable to a spoofing attack.
- Jamming detection is an essential part of spoofing detection.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Target platform definition and decision

IntegriCom

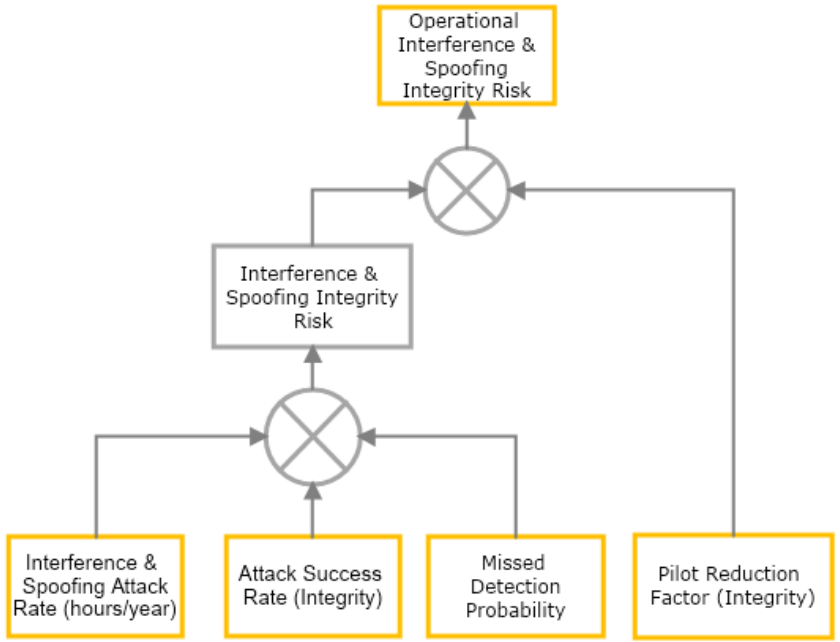
Target Platform Definition and Decision

- We selected the TSO-C145/146/196 receivers
  - Much higher accuracy than TSO-C129(a) receivers, so larger impact of disturbances
  - Some mitigation features (smoothing, ‘light’ SQM, jump detection) available
  - SBAS corrections were not used
    - Lower the HPL, but no mitigation of interference

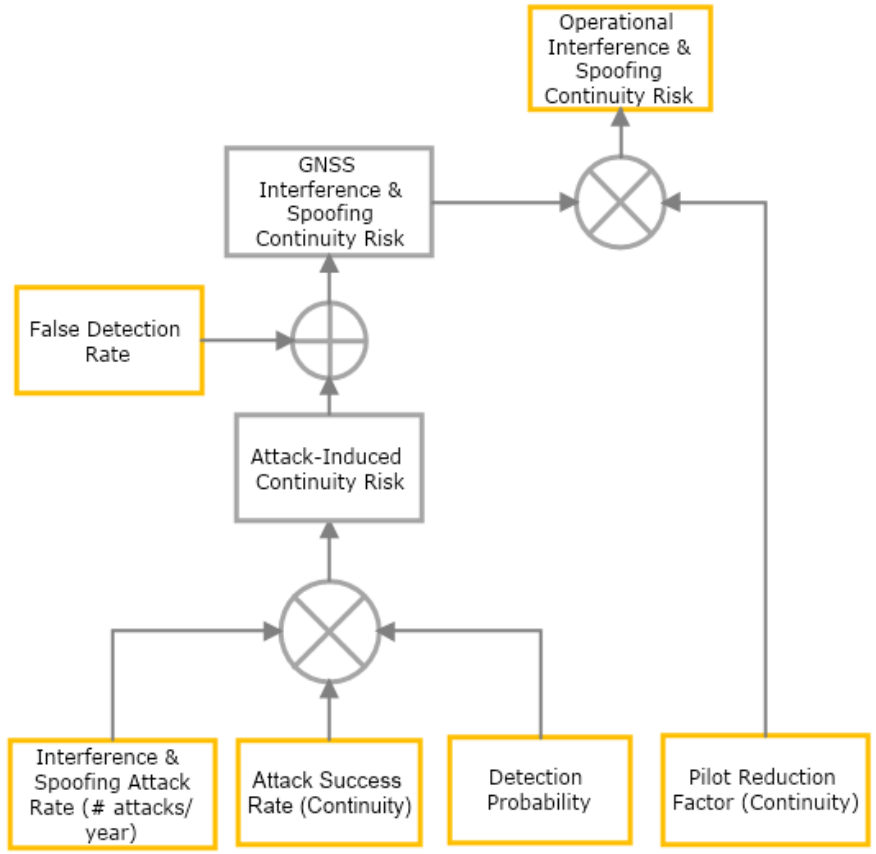
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Integrity and continuity risk (single attack)

- Risk Trees were used to:
  - Derive detector requirements
  - Rank attacks from high-risk to low-risk



Integrity Risk



Continuity Risk

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS anti-spoofing system requirements

- These considerations lead to requirements per attack in terms of
  - P_{MD} .. probability of missed detection per attack (range from $\sim 10^{-2}$ to $\sim 10^{-5}$)
  - P_{FA} .. probability of false alarm per hour ($= 10^{-5}$)
  - TTD .. time to detection ($= 6\ [s]$)

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS anti-spoofing state-of-the-art (1/2)

- Spoofing detection
  - Position/Velocity/Time (PVT) estimate consistency checks
  - Navigation data consistency checks
  - Monitoring the Automatic Gain Control (AGC)
  - Monitoring for multiple correlation peaks and distortions of the Auto-Correlation Function (ACF)
  - Signal spatial correlation
  - Inertial Navigation Systems (INS)
  - Correlation between two civil GPS receivers
  - C/N0 monitoring
  - Observable monitoring
  - Signal polarization
  - Spoofing detection with multi-antenna arrays

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS anti-spoofing state-of-the-art (2/2)

- Spoofing mitigation
  - Spatial correlation based on Doppler
  - Antenna array direction of arrival estimation (DOA)
  - Time difference of arrival estimation (TDOA)
  - Navigation message authentication (NMA)
  - (A)RAIM – Fault Detection and Exclusion (FDE)
  - Flight management systems & crosschecks with other navigation sensors
  - PVT from vestigial authentic signals

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS spoofing detection techniques selection

- The selection of suitable detection techniques was done in a multi-level approach.
  1. Selection based operational limitations
     (e.g. feasible in moving aircraft considering its dynamics)
  2. Selection based on detailed analytical analysis and empirical preliminary testing
     (each technique has been analytically x-rayed; selected techniques have been empirically tested preliminary)
  3. Selection based on suitability to detect identified attack scenarios
     (the target was to cover as much as possible of the threat space)

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS Anti-Spoofing System Architecture

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS anti-spoofing system design

- The system was designed following a flexible, modular approach in order to consider the evolving threat space.
- The first design driver was to cover as much as possible of the identified, multi-dimensional threat space.
- Another main design driver was to reduce the complexity to ease future certifiability.
- Separate modules for jamming and spoofing detection.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

GNSS anti-spoofing system design (spoofing)

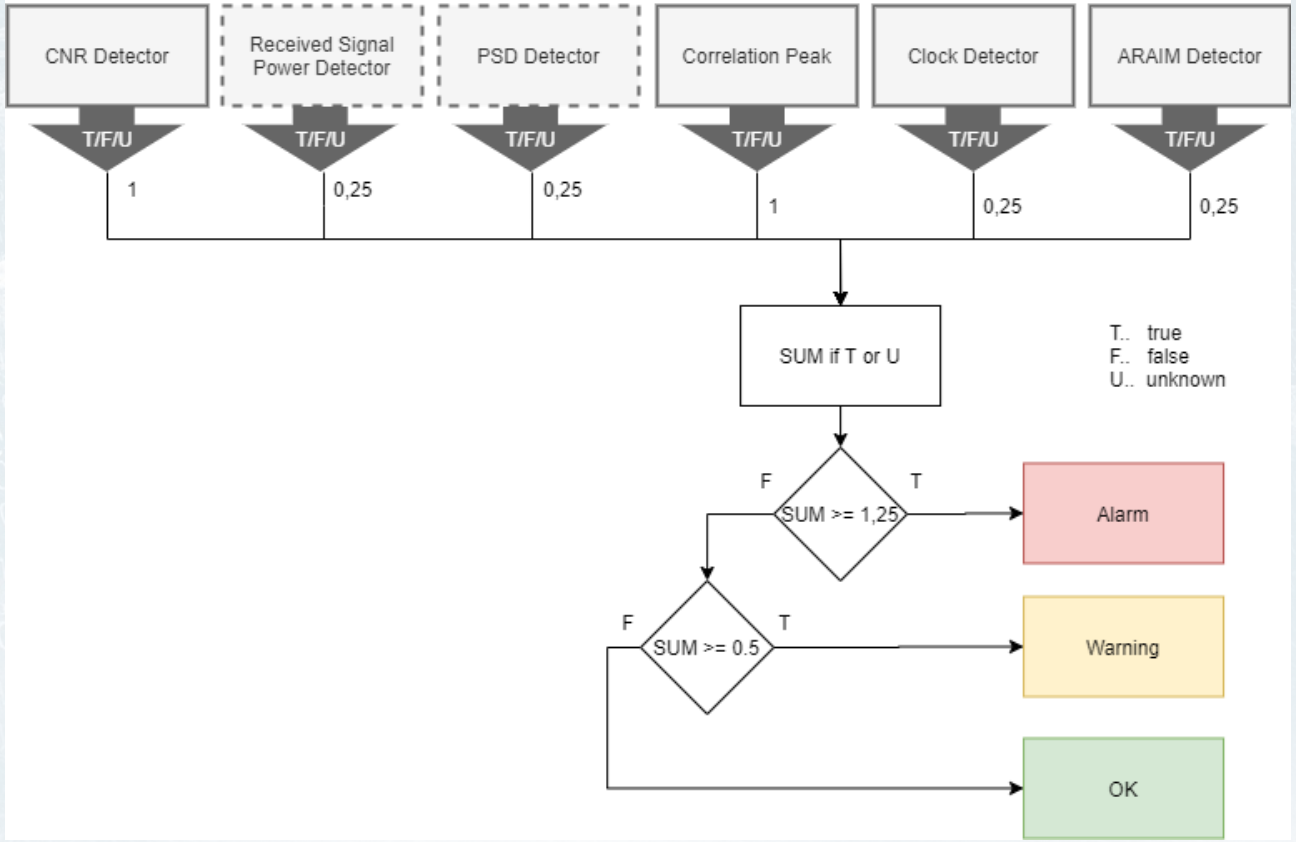
- Combined, weighted spoofing detection system

✓ Modularity

✓ Simple approach to favour certifiability

✓ Output per constellation+band

✓ Easy tuning for different attack types



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

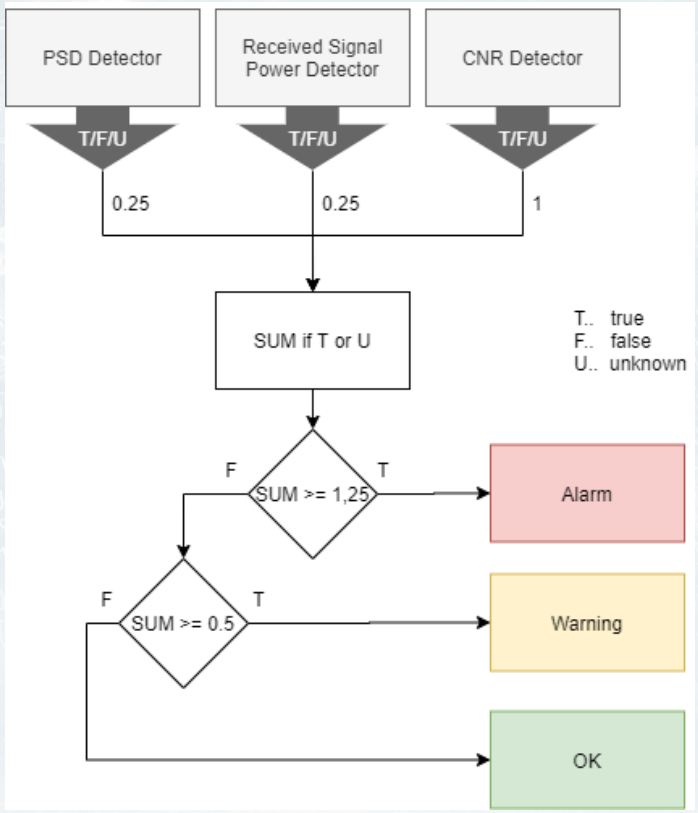
GNSS anti-spoofing system design (jamming)

- Combined, weighted jamming detection system

✓ Modularity

✓ Output per frequency band (e.g. L1)

✓ Distinction between spoofing and jamming



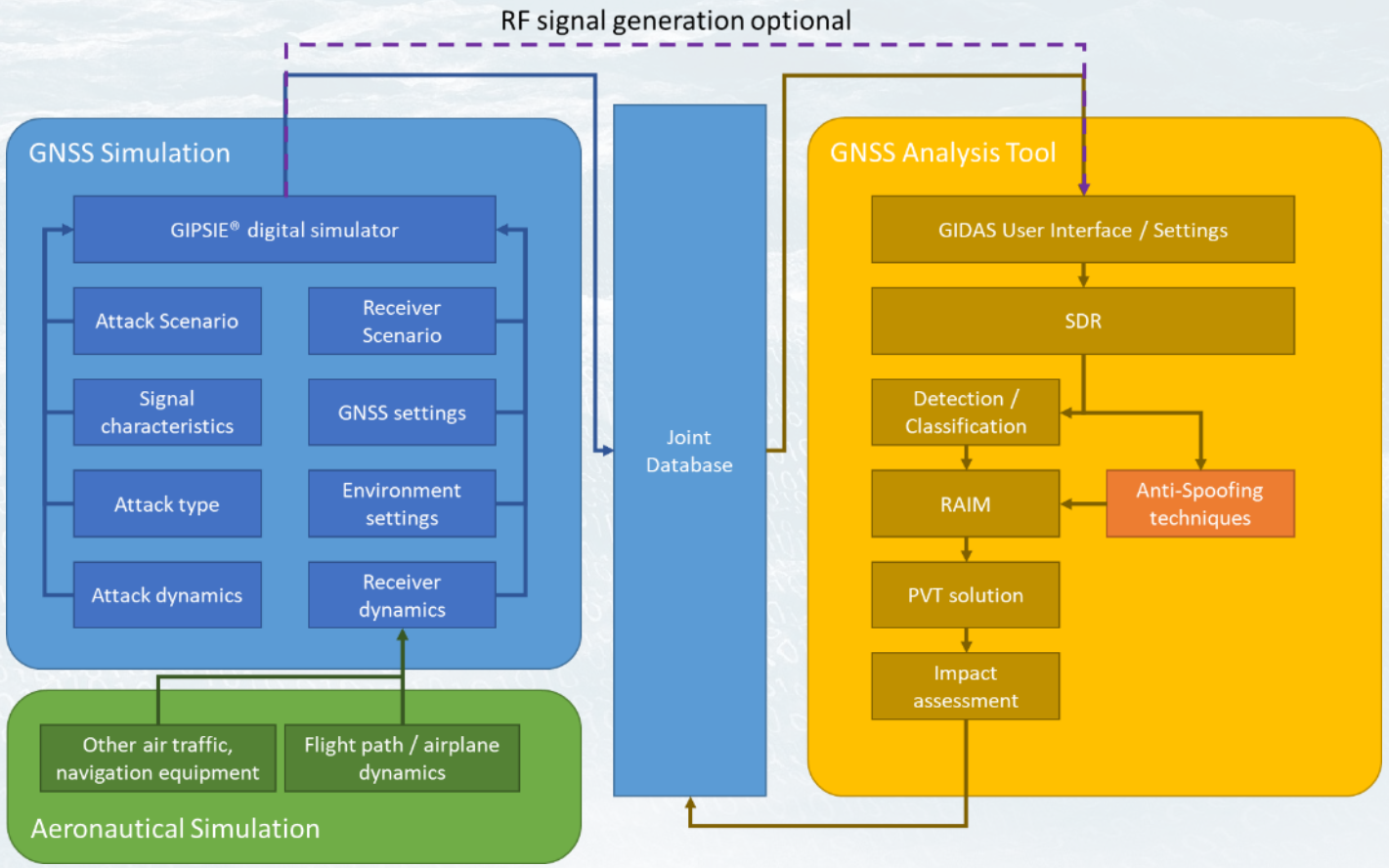
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Simulation Results

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Sp-ATM simulation environment

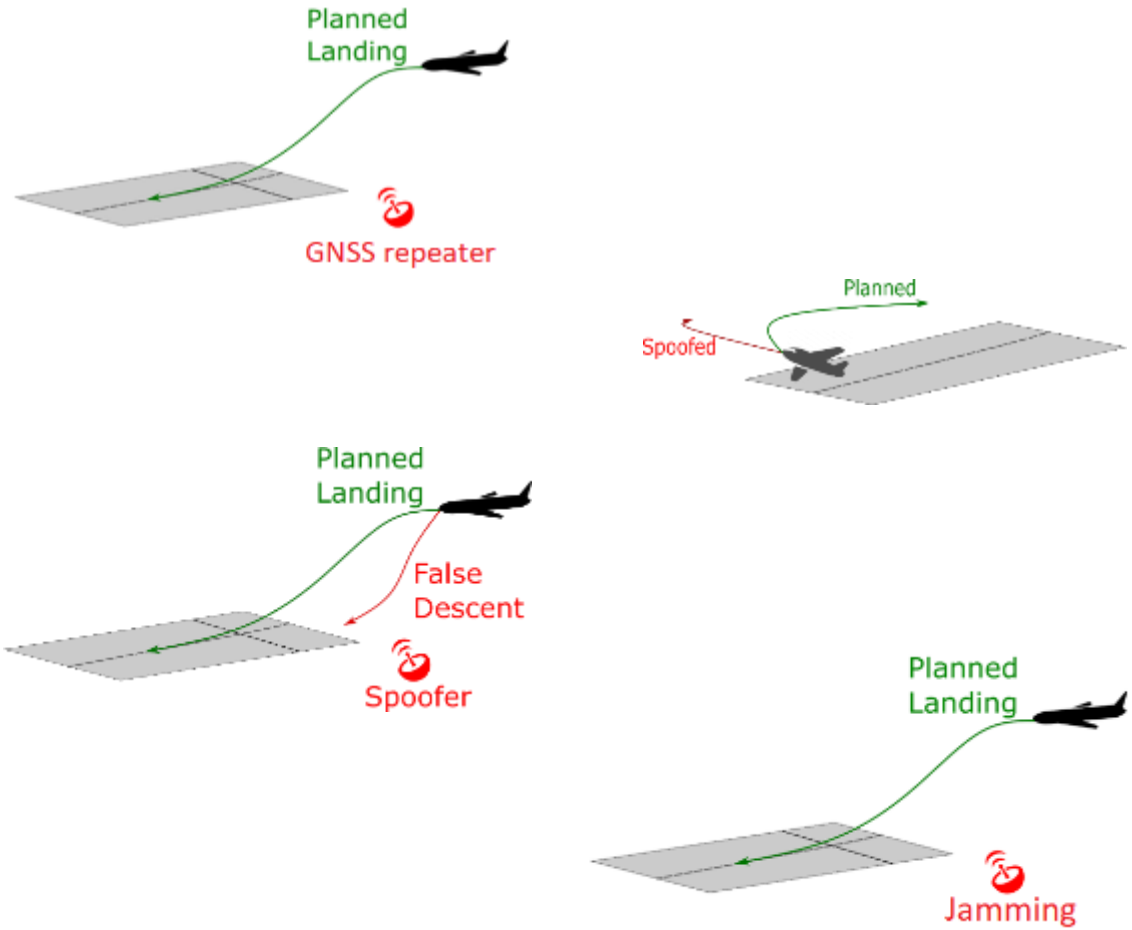
- Based on
  - GIPSIE® (OHB)
  - GIDAS® (OHB)
  - Flight path simulator (PLUS)
  - (A)RAIM (IC)



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Considered attack scenarios

- Considered attack scenarios
  - Scenario 1 – Re-radiation
  - Scenario 2 – Pin-point airborne
  - Scenario 3 – Ground-based
  - Scenario 4 – Jamming
- Most hazardous and likely attacks
  - attack cost
  - attack detectability
  - hazard analysis
  - effects on the defined flight phases



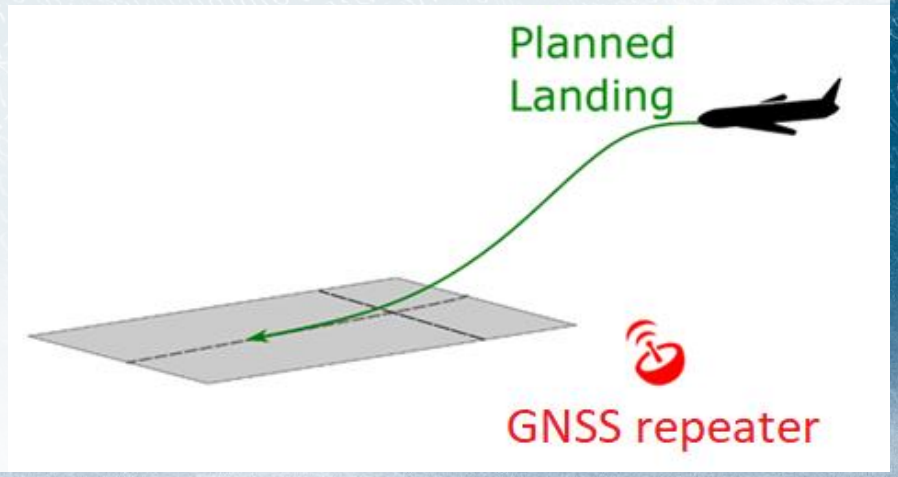
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 1

- **Scenario 1 – Ground-based, malfunctioning GNSS repeater**

Setup:

- One ground-based, malfunctioning GNSS repeater at the airport premises
- Rebroadcasting of authentic signals with higher power (-40dBW) and 1 millisecond time delay
- No active spoofing attack, thus the spoofing signals are rebroadcasted without the consideration of the current airplane position. (in terms of received signal power or signal delay)



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of Simulation Execution – Scenario 1

- **Scenario 1 – Ground-based, malfunctioning GNSS repeater**

Approach of A320 to VIE/LOWW.

Source:
Google Earth

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

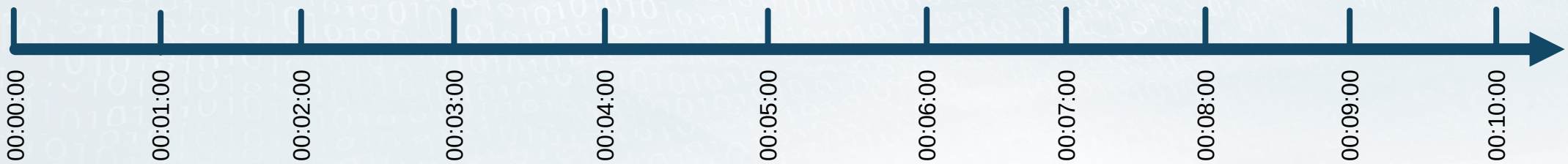
Results of Simulation Execution – Scenario 1

- **Scenario 1 – Ground-based, malfunctioning GNSS repeater**

Spoofing attack timeline:

Presence of time delayed, authentic GNSS signal from malfunctioning GNSS repeater with transmission power of 100dBW

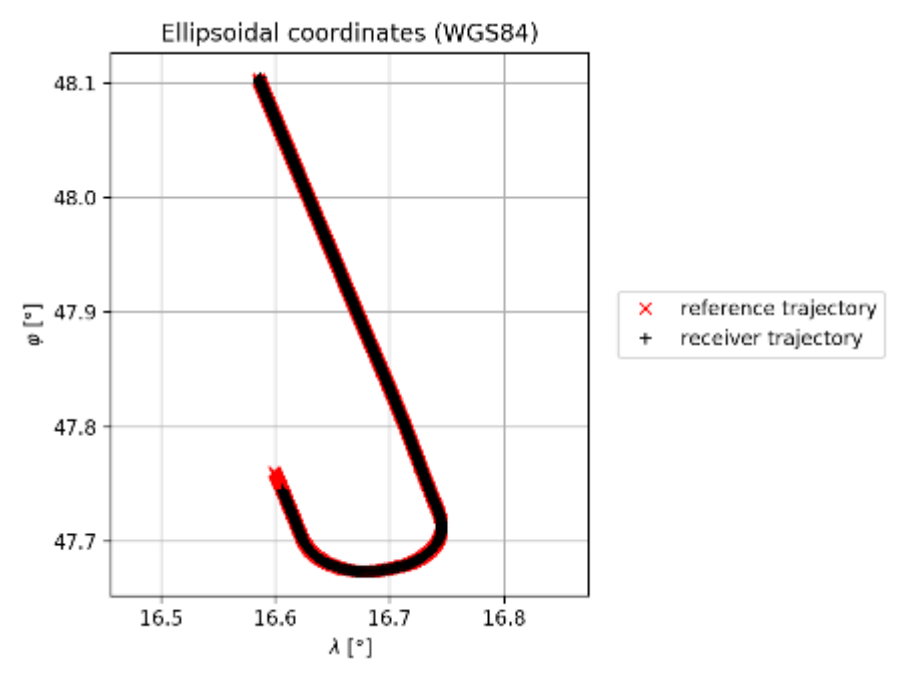
Received signal power with respect of free space path loss;

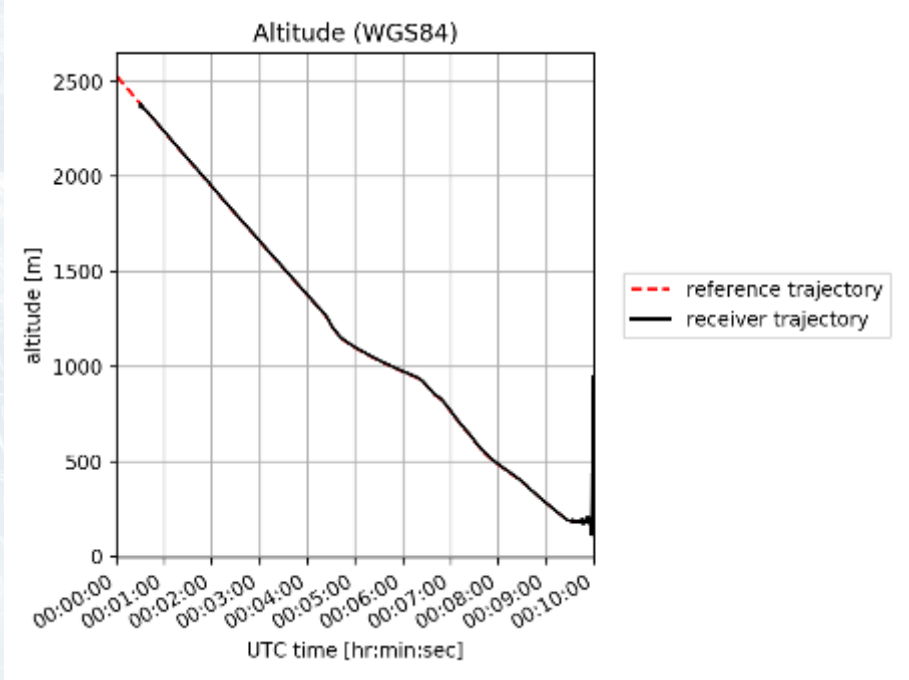


OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

PVT solution – scenario 1

- PVT solution of GNSS receiver on-board the airplane





OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

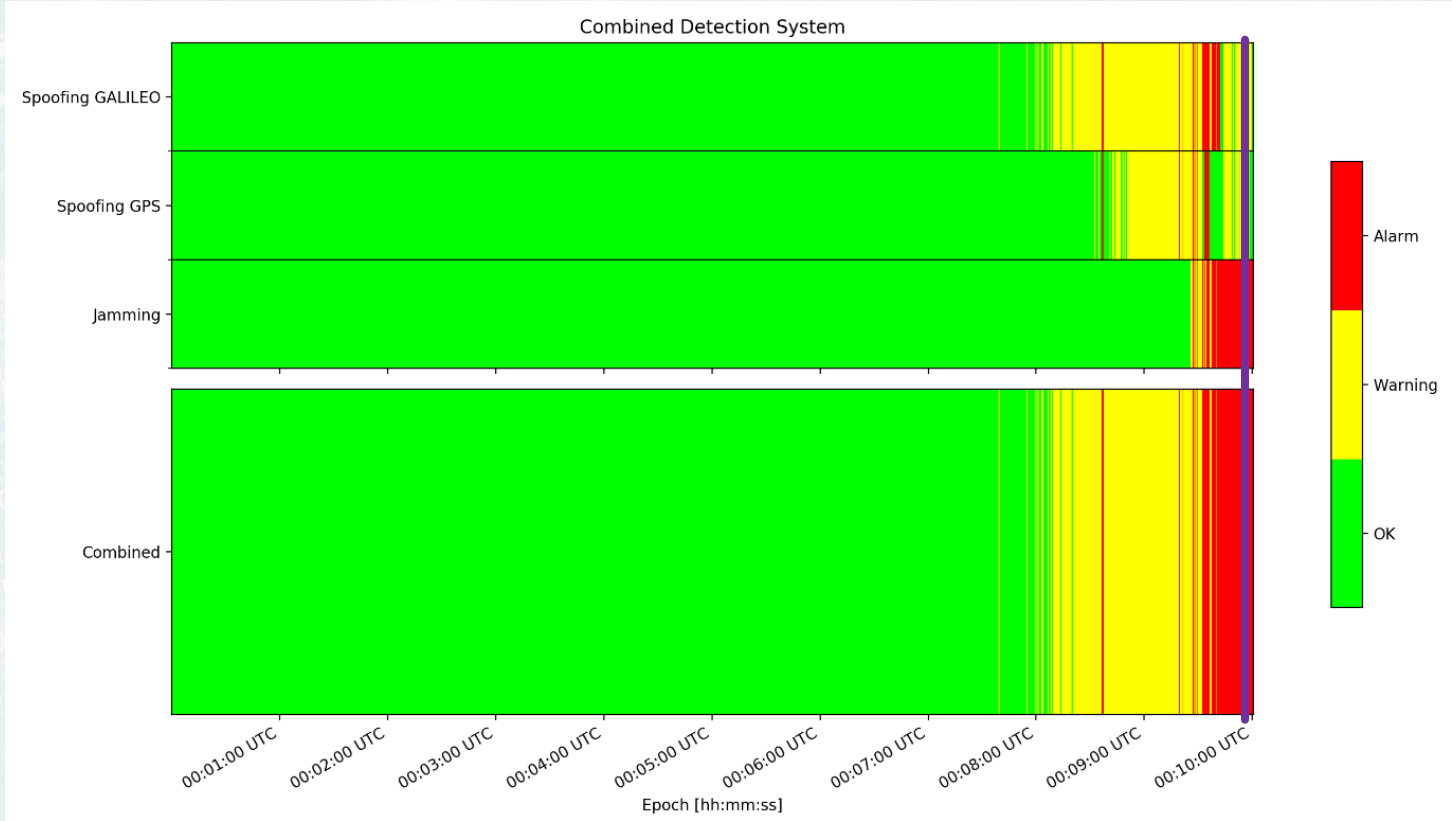
Results of simulation execution – scenario 1

- Combined detection system output

✓ Multiple correlation peaks visible

✓ High powered spoofing equals jamming

✓ Early detection (over 80 seconds before position affected)



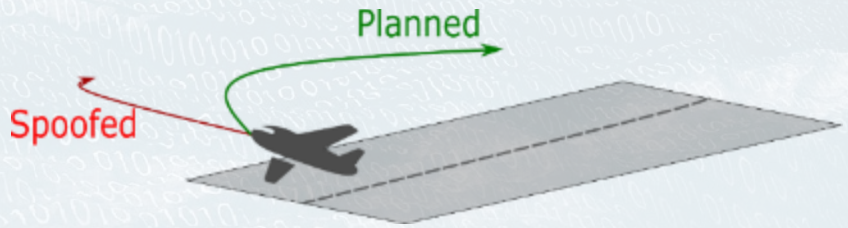
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 2

- **Scenario 2 – Airborne spoofing by escorting drone / false flight path**

Setup:

- One airborne, drone-mounted spoofer escorting the departing airplane
- Reference receiver and internet for ephemeris.
- Target position approximated with close drone-position
- Distance between target airplane and attacker drone approximately 250m. (± 10 m)



- Transmission of spoofing signal leading the target airplane position onto a false path
- Due to over-compensation of the misleading GNSS position the airplane will likely drift off course to the opposite direction.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 2

- **Scenario 2 – Airborne spoofing by escorting drone / false flight path**

Departure of A320
from VIE/LOWW.

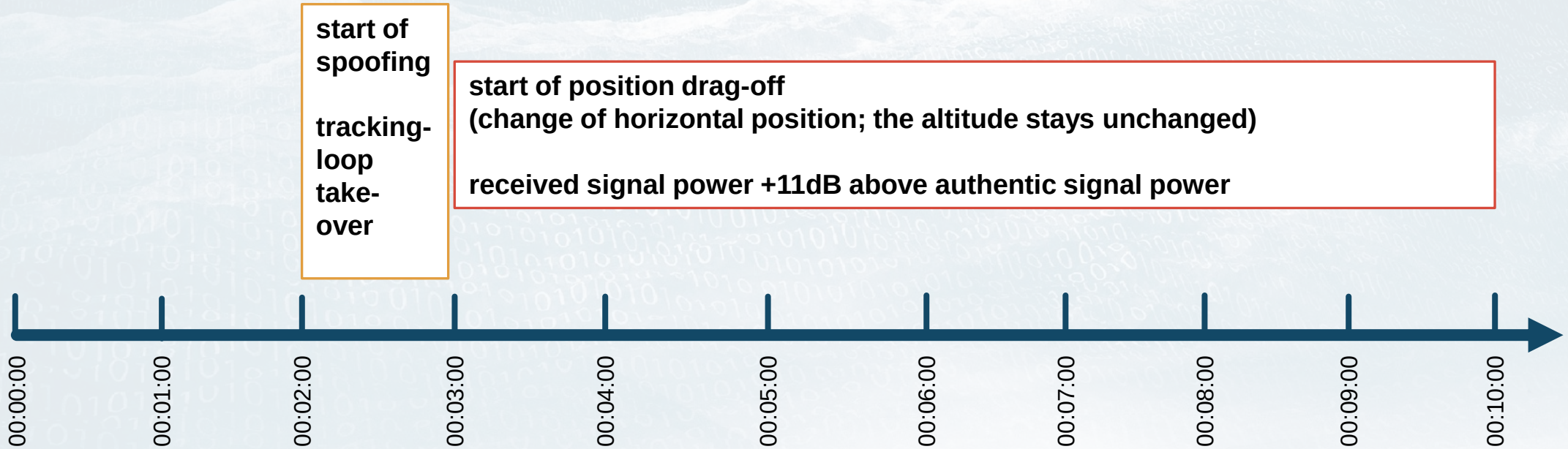
Source:
Google Earth

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 2

- **Scenario 2 – Airborne spoofing by escorting drone / false flight path**

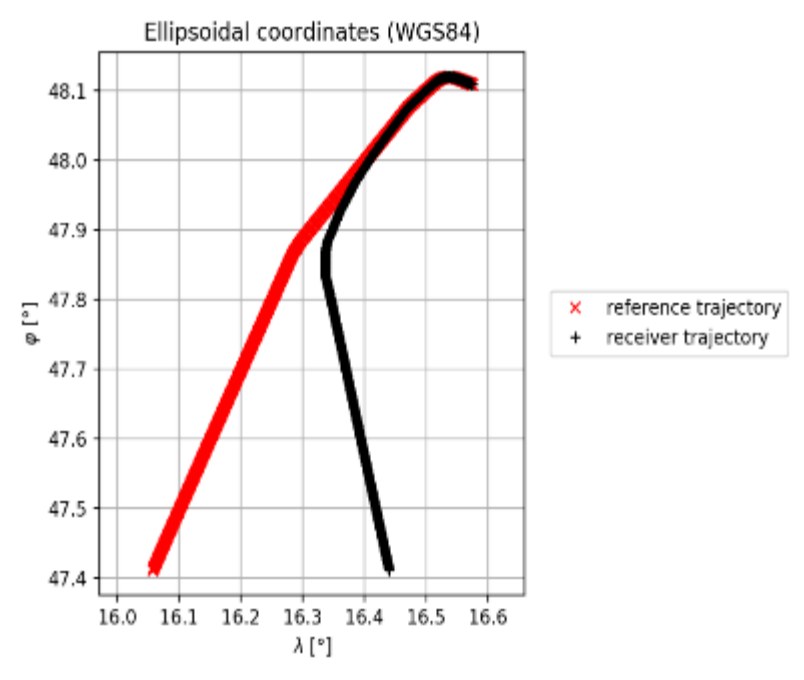
Spoofing attack timeline:

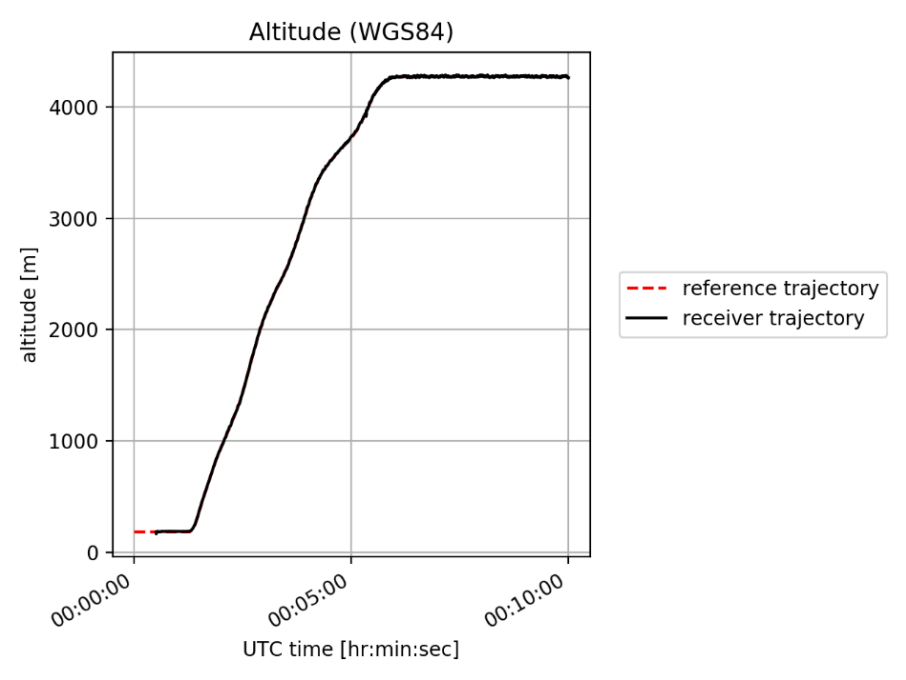


OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

PVT solution – scenario 2

- PVT solution of GNSS receiver on-board the airplane





OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

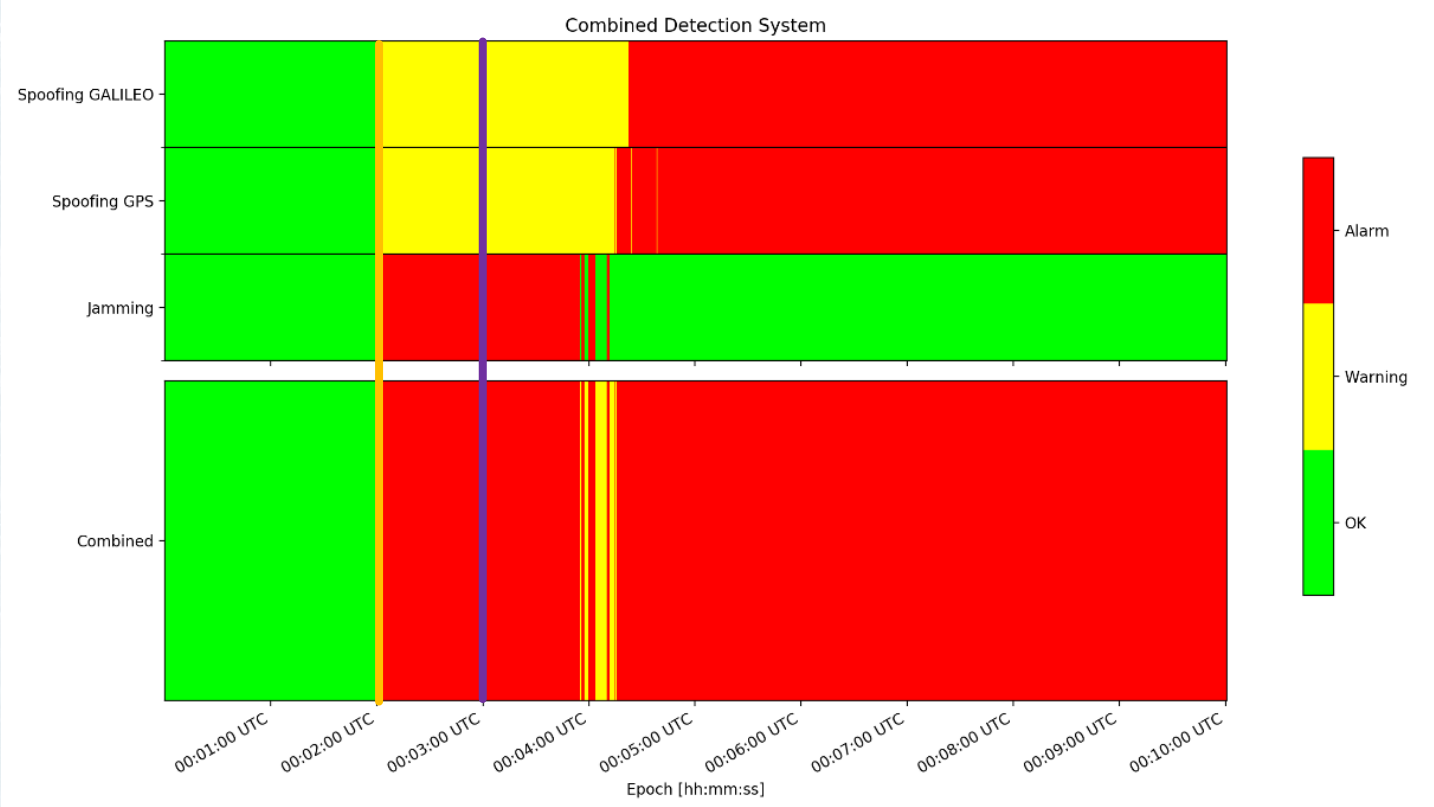
Results of simulation execution – scenario 2

- Combined detection system output

✓ Spoofing attack detected 2.3 s after signal presence

✓ Initial take-over phase detected as jamming

✓ Permanent detection



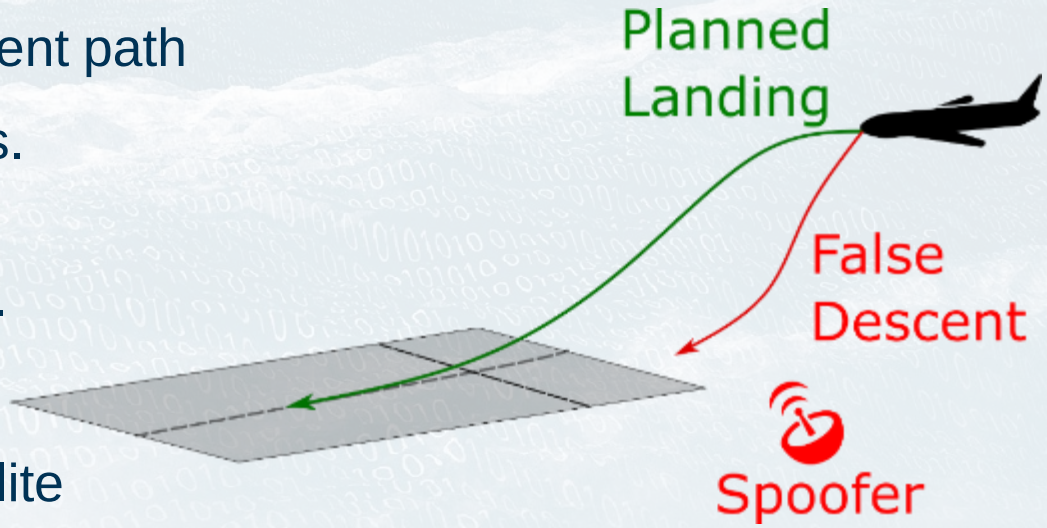
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 3

- **Scenario 3 – Ground-based spoofing / false descent**

Setup:

- One ground-based spoofer located near descent path
- Reference receiver and internet for ephemeris.
- Distance to plane and plane position for a pinpoint attack (synchronous spoofing attack).
- ± 10 m knowledge of the plane's position
- Code-Delay and Doppler values to each satellite
- Due to over-compensation of the misleading GNSS positioning information the airplane will very likely face a missed approach. Faking a false ascent could lead to a plane crash in the fields before the runway.



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 3

- **Scenario 3 – Ground-based spoofing / False Descent**

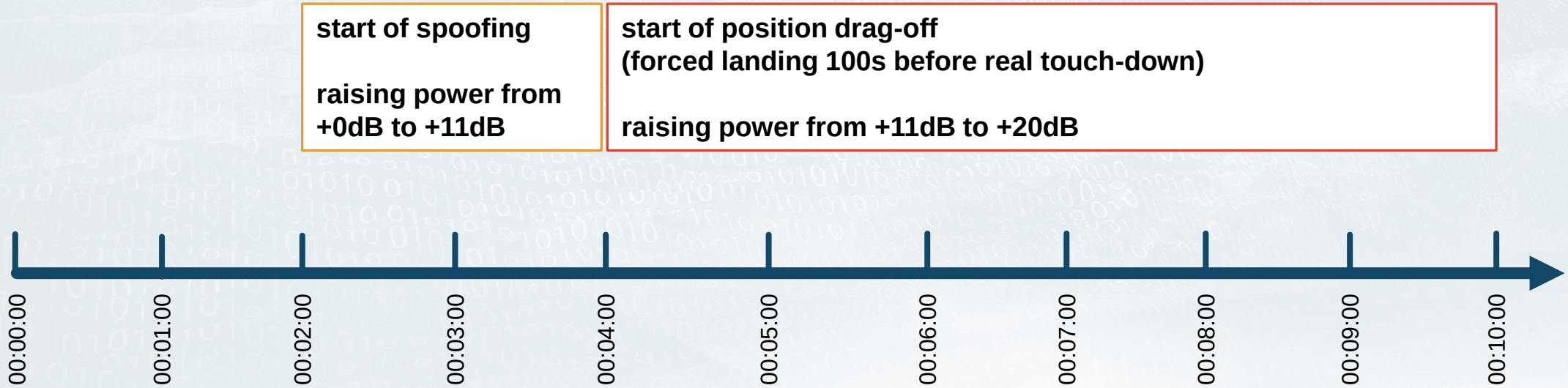
Approach of A320 to VIE/LOWW.

Source:
Google Earth

Results of simulation execution – scenario 3

- **Scenario 3 – Ground-based spoofing / False Descent**

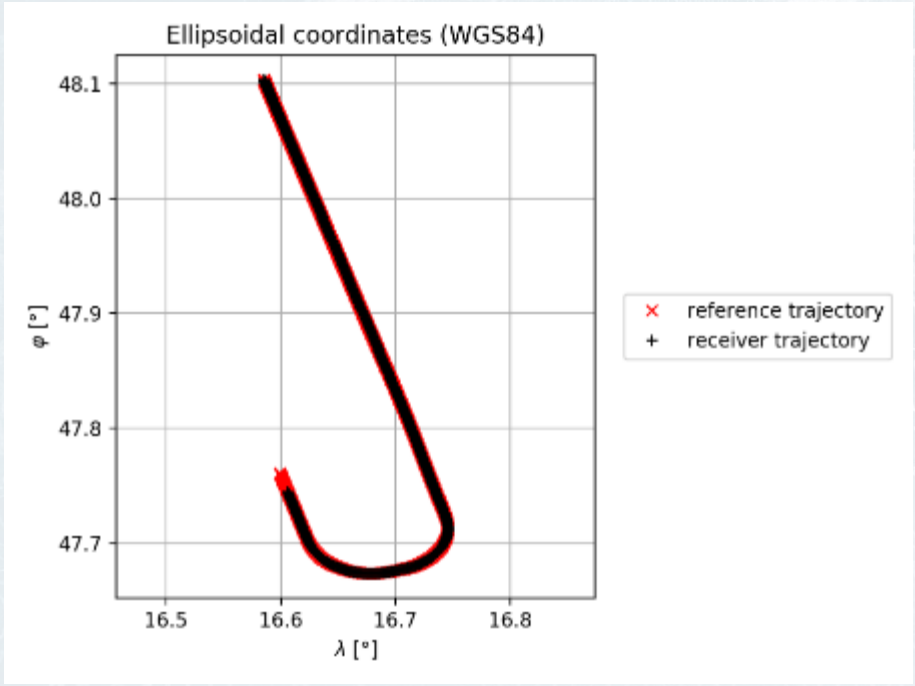
Spoofing attack timeline:

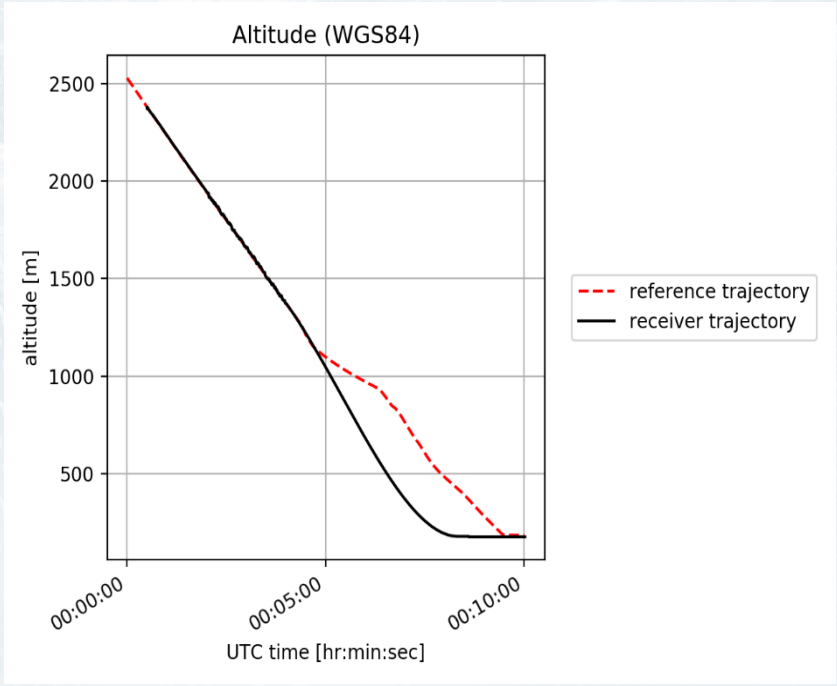


OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 3

- PVT solution of GNSS receiver on-board the airplane





OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

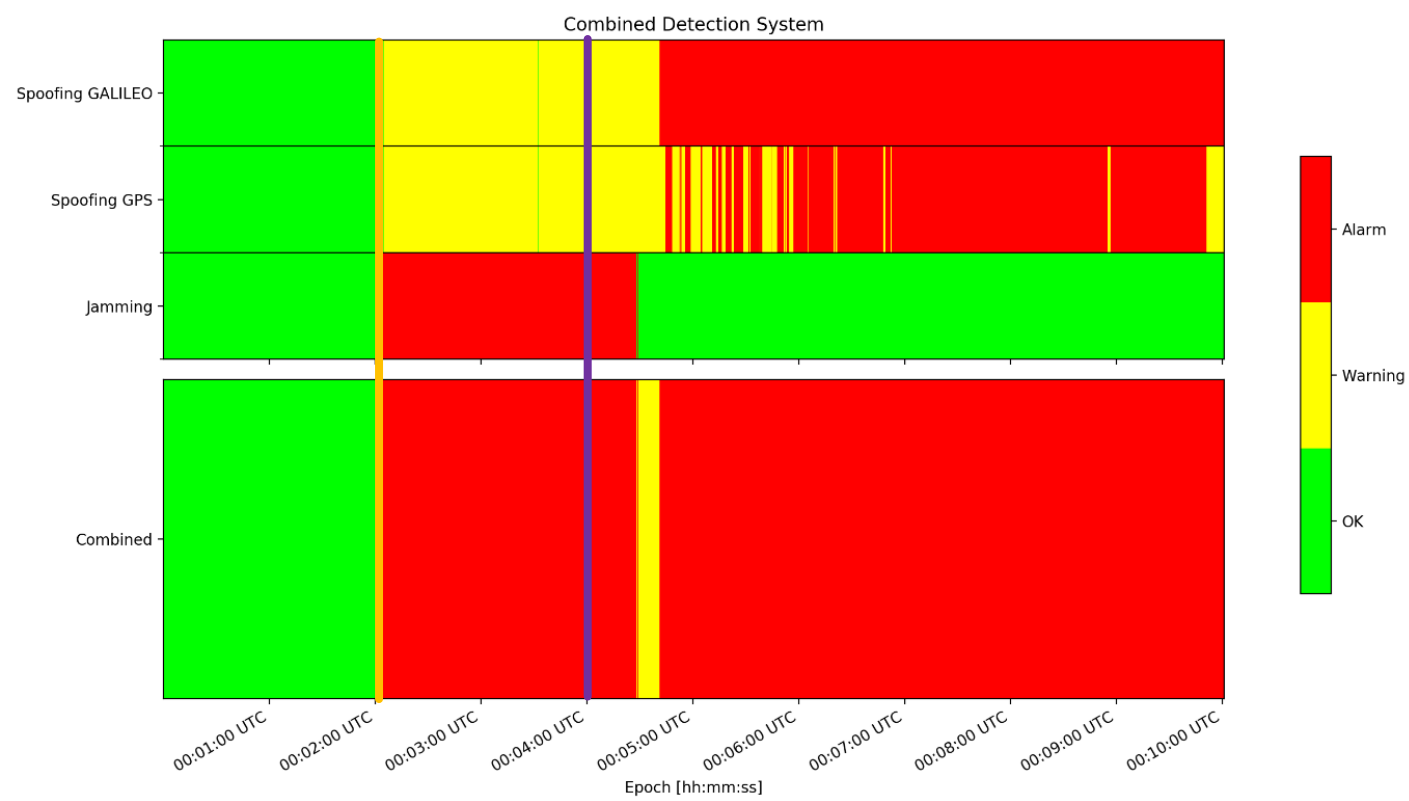
Results of simulation execution – scenario 3

- Combined detection system output

✓ Spoofing attack detected 2.3 s after signal presence

✓ Initial take-over phase detected as jamming

✓ Permanent detection



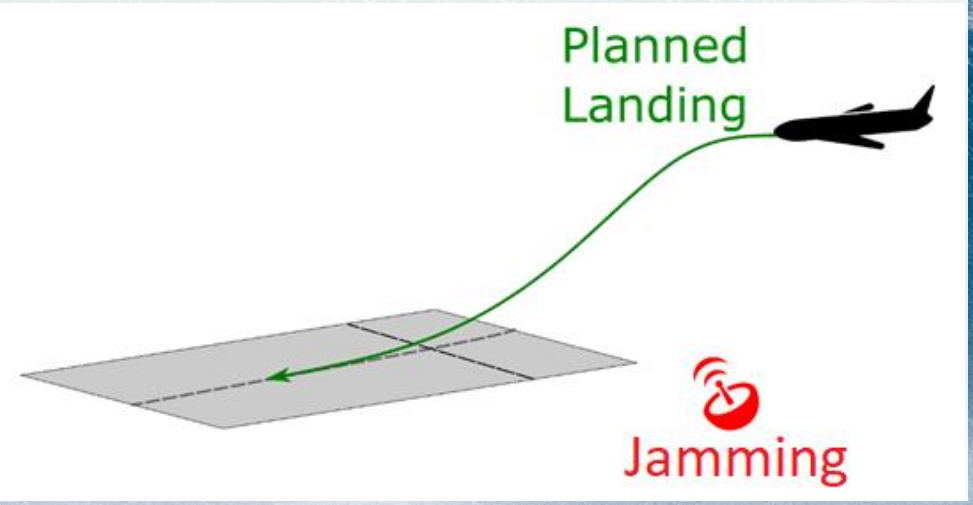
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 4

- **Scenario 4 – Ground-based jamming / local GNSS service outage**

Setup:

- One ground-based jammer located near descent path
- High powered FM jammer
  - Centre Frequency: 1575.42 MHz
  - Modulation Frequency: 1.0 MHz
  - Frequency Deviation: 1.0 MHz
- Hazardous effect exponentially increasing with decreasing distance.
- Introducing signal tracking noise up to the point of tracking loss and GNSS service loss.



Results of simulation execution – scenario 4

- **Scenario 4 – Ground-based jamming / local GNSS service outage**

Source:
Google Earth

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

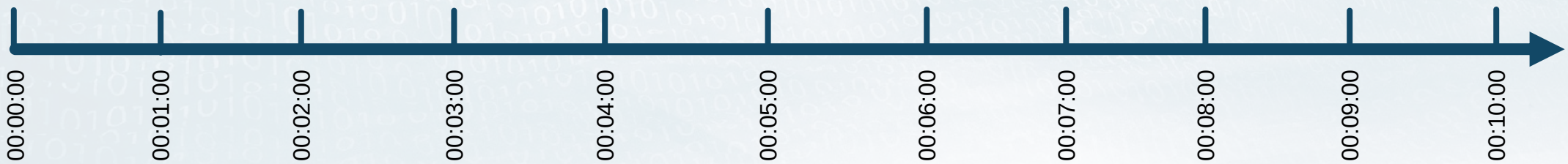
Results of simulation execution – scenario 4

- **Scenario 4 – Ground-based jamming / local GNSS service outage**

Jamming attack timeline:

Presence of high-powered FM jamming signal
(local outage of GNSS service)

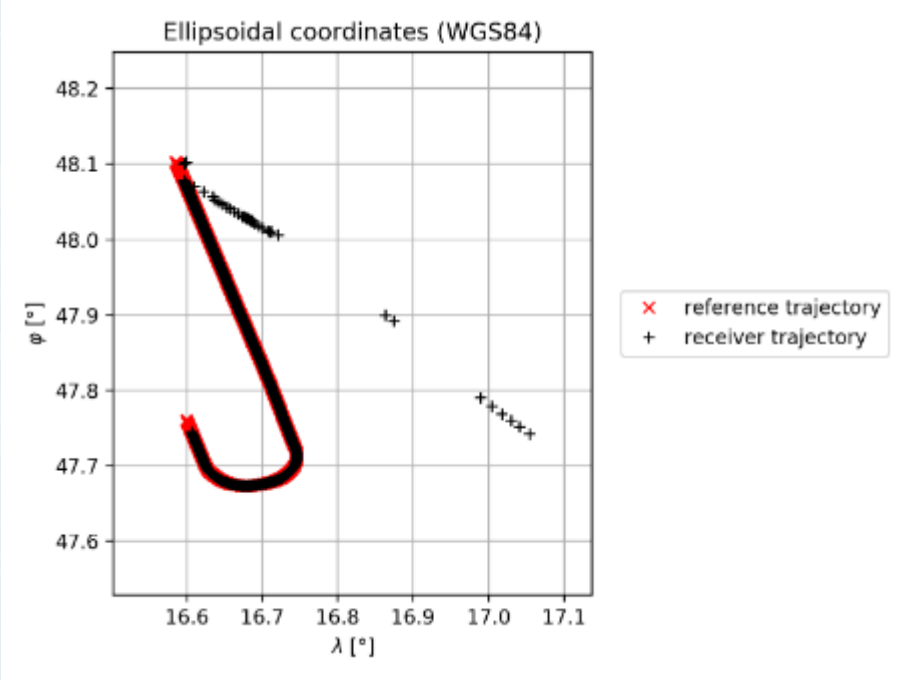
transmission power -30dB

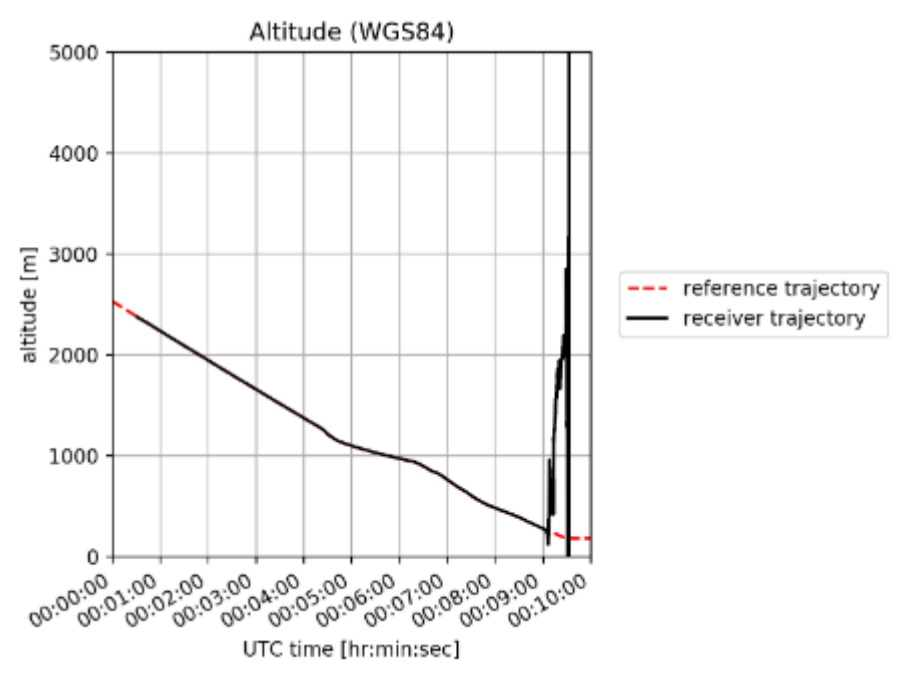


OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 4

- PVT solution of GNSS receiver on-board the airplane





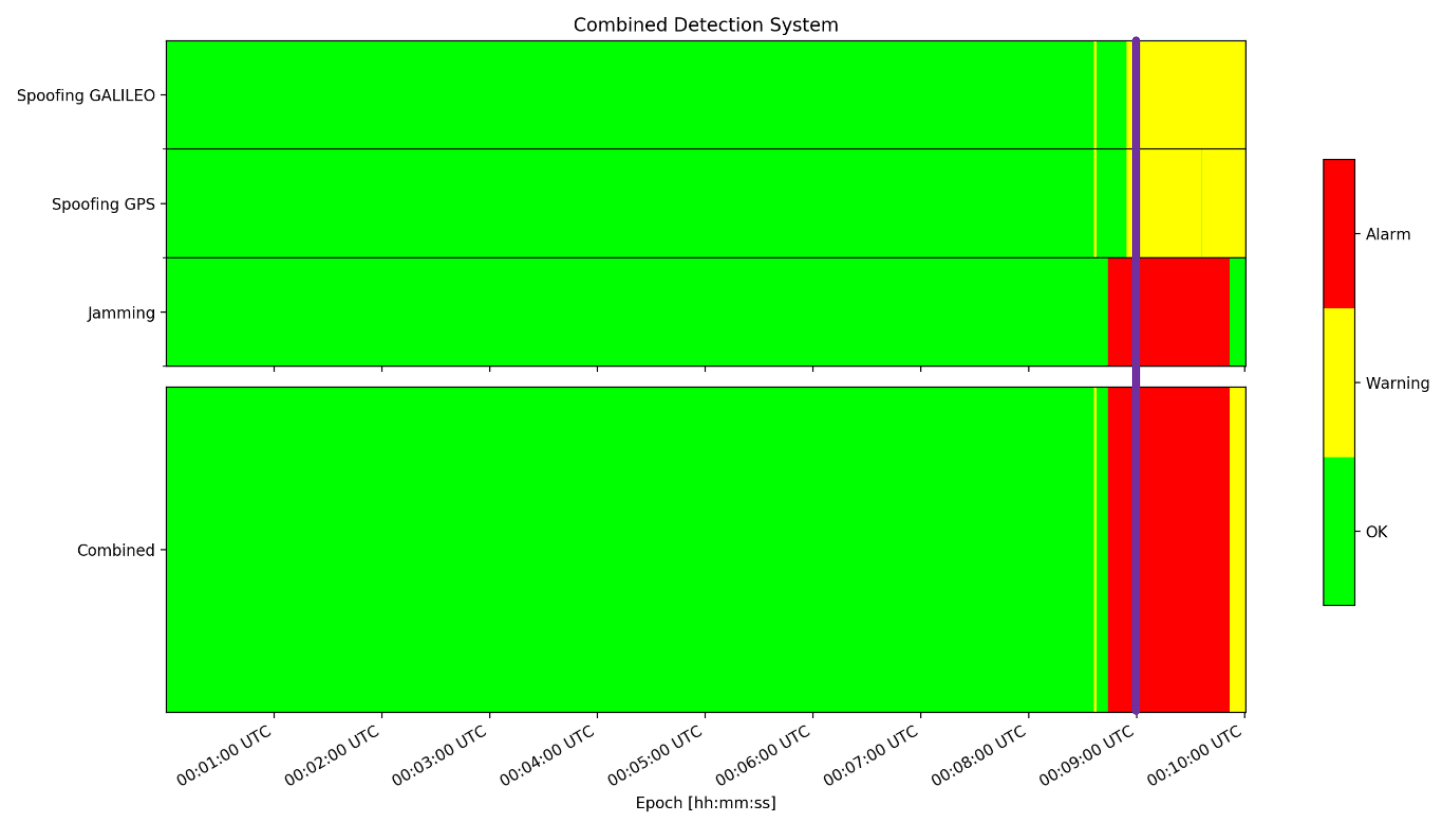
OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Results of simulation execution – scenario 4

- Combined detection system output

✓ Classification of jamming possible

✓ Detection approximately 30 s before position being affected



OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Summary on test execution

- The combined detection system proved its performance during the conducted simulations as expected.
- All types of defined attack setups have been successfully detected.
- Depending on the specific scenario we achieved very early detection. (Even in the takeover phase of an attack, without the position being affected already.)
- 72h testing and validation of interference-free simulation to ensure the system does not falsely interfere with existing systems or procedures.
- 20+h testing of simulation data to prove the detection performance.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines for Future Activities

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines - recommendations for standardization

General considerations

- **The threat space**

Our study has shown that we are dealing with a huge high-dimensional threat space:

- There are many different types of attack
- Each type of attack is associated with a number of ‘configuration parameters’ that can vary from attack to attack, and will drive both the performance of the detector and the impact of undetected errors on the position solution.

This implies that there is essentially an infinite amount of potential attacks to be considered.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines - recommendations for standardization

General Considerations

- **Relating the threat space to detector performance**

The probability of missed detection will depend on:

- Attack characteristics (type and attack parameters)
- Detector’s design, including the tuning of its detection threshold.

- The approach taken is to assess the performance under some near-worst-case assumption.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines - recommendations for standardization

General considerations

- Impact of spoofing and interference need to be considered explicitly in receiver standards
- Risks need to be allocated
  - Consolidated risk trees will have to be developed
- Standards will need to cope with change:
  - Complexity: attack will be simpler over time.
  - Likelihood of attacks might depend greatly on location.
- Therefore: we need a flexible solution that accommodates technological advances and varying likelihood of attacks.
- We recommend to start with mitigation techniques that are relatively simple and impactful, but realize things might not stop there

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines - recommendations for standardization

Our recommendations

- Huge threat space, many detection/mitigation techniques: complexity is high!
  - Standardization roadmap can help to prioritize the work based on urgency of measures in the receiver
  - Need for flexibility in requirements: maybe allow 'updating' of tunings/settings
- Current study can serve as input to this process
- ARAIM needs to monitor the most likely 'spoofed satellite sets' regardless of satellite and constellation fault rates

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines - Roadmap for GALILEO and EGNOS Evolutions

Although this has not been at the core of our study, we have identified some generic ‘nice-to-haves’ that could be taken into consideration for future Galileo and EGNOS evolutions.

- Increasing the signal power of satellite signals: more is always better
  - In contradiction with ITU and available power at satellite
- Improving signal design
  - Significant differences in the behaviour of some detectors observed. Spoofing and interference considerations could be a part of future signal design
- Authentication is highly beneficial
- Additional signals and signal components
- EGNOS evolution
  - Providing additional features to increase the robustness against intentional spoofing attacks by means of adding authentication (either signal encryption or navigation message content authentication) on e.g. L5

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Guidelines - Roadmap for GALILEO and EGNOS Evolutions

- In general, not limited to the aviation domain, it is necessary to further raise the awareness on spoofing attacks.
- Thus it is important to continue the work anti-spoofing techniques as well as on the dual-frequency multi-constellation topic.
- Furthermore the standardization of this topic has to be driven to ensure a proper implementation of anti-spoofing techniques to provide further resilience.

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Conclusions

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Conclusions

- Developed software and algorithms:
  - Tuning of already available SDR for MOPS conformity
  - Detection techniques (modules)
    - CNR detection technique
    - Correlation peak detection technique
    - ARAIM detection technique
    - Estimated clock detection technique
  - Weighted and combined jamming/spoofing detection system
  - GNSS analysis tool

- Thanks to ESA (especially to Gianluca) for the support throughout the activity

OHB Digital Solutions GmbH
info@ohb-digital.at; www.ohb-digital.at

Outlook

- Assessment of RFI threat-space and mitigation from ATM (AOC) point of view (ECAC)
- Extended simulation driven study by using:
  - OHB's sophisticated spoofing/jamming simulation tools and
  - ("NAVSIM") ECAC/worldwide air traffic and air traffic management simulation framework
- Assess and further analyse threat-space and impact area:
  - RFI effects might be considered as local threat only,
    but might impact ATM on European level!

- Providing:
  - Assistance, guidance to ATM / AOC to ensure safe and
    efficient operation under RFI threats (e.g. new/modified procedures)
  - Support the development and effectiveness analysis of enhanced (collaborative-) detection and mitigation technologies / procedures

We are the Navigation Experts

Philipp Berglez

CTO

OHB Digital Solutions GmbH

Rettenbacher Straße 22

8044 Graz, Austria

Mail: philipp.berglez@ohb-digital.at

Tel: +43-316-890971-14

Manuel Kadletz

Research Engineer

OHB Digital Solutions GmbH

Rettenbacher Straße 22

8044 Graz, Austria

Mail: manuel.kadletz@ohb-digital.at

Tel: +43-316-890971-18

We are the Navigation Experts

Bastiaan Ober

Owner

IntegriCom

Tjalkenwerf 30,

2317-DD Leiden - Netherlands

Mail: p.b.ober@integricom.nl

Tel: +31-71-8795620

We are the Navigation Experts

Carl-Herbert Rokitansky

Head Aerospace Research

Aerospace Research Salzburg

University of Salzburg

Jakob Haringer Straße 2

5020 Salzburg, Austria

Mail: roki@cs.sbg.ac.at

Tel: +43 664 85 25 347

Kurt Eschbacher
Fritz Zobl
Robert Marschallinger

Senior Scientists

Aerospace Research Salzburg

University of Salzburg

Jakob Haringer Straße 2

5020 Salzburg, Austria

Mail: kurt.eschbacher@sbg.ac.at

Mail: fritz.zobl@sbg.ac.at

Mail: robert.marschallinger@sbg.ac.at