GNSS Under Attack

Workshop Summary

Budapest – 5-6 Feb 2026

IntegriCom Hungary

IntegriCom Hungary

Workshop's Main Message(s)

GNSS is vulnerable

- GNSS can be inaccurate
- GNSS can be unavailable
- GNSS can be deceiving
- GNSS can be attacked

Workshop Summary

- Day 1 –Part 1
- GNSS is part of critical infrastructure
  - Used for internet, telecom, power grids, transportation
  - Huge impact of disturbances…
  - … hence an attractive target for attacks
- Overview of how GNSS works
  - Mechanism to obtain range measurements
  - Obtain position and/or time from these

Workshop Summary

- Day 1 –Part 1
- GNSS is vulnerable
  - Low power, not designed for safety originally
  - Spoofing attack using low-cost hard- and software
- High-end simulator
  - Essential to test equipment as testing in the field is prohibited

Workshop Summary

- Day 1 –Part 2
- Use of GNSS for timing and safety critical applications
  - Stressed aviation as the first and best organized user community
- Brief overview of all ‘normal’ error sources
  - Satellite clock and orbit
  - Atmosphere (ionosphere and troposphere)
  - Multipath, receiver noise

Workshop Summary

- Day 2 –Part 1
- Data formats and data processing
  - Give some feeling on tooling and data processing chains power
- High-end simulator
  - Software-defined receiver technology for jamming, spoofing generation and detection
- Receiver technology
  - Currently developing improved resilience

Final Words

- Part of European Space Agency (ESA)'s RPA initiative to strengthen space competencies in Hungarian companies.
- RPA Activity for Hungarian Industry
  - New call for tender and info day mid-March 2026
  - Includes GNSS and many other space related activities
- NAVISP information day is in the works
  - GNSS and other navigation topics