Real-Time GNSS Data Integrity: Foundations, Challenges, and Emerging Approaches

NKG Summer school “From Struve to the Space”
August 25-29 2025 Tartu, Estonia

Kibrom Ebuy Abraha
LANTMÄTERIET

Nordic Geodetic Commission
NKG

Why GNSS Integrity Matters?

- GNSS dependent society
  - Used in aviation, farming, autonomous cars, drones etc
  - Real-time applications: high stakes, no room for undetected errors
  - Accuracy is no longer the main limitation
  - Accuracy alone is not enough – We need to trust the solution

https://scpnt.stanford.edu/

- GNSS Integrity
  - Measure of trust in PNT provided by GNSS
  - Quantification of the confidence level of PNT given by the system is correct

US Federal Rdionavigation Plan defines integrity as:

A.1.11 Integrity

Integrity is the measure of the trust that can be placed in the correctness of the information supplied by a PNT system. Integrity includes the ability of the system to provide timely warnings to users when the system should not be used for navigation.

No integrity = no trust

Position ≠ Safe unless integrity is assured

GNSS Quality Dimensions

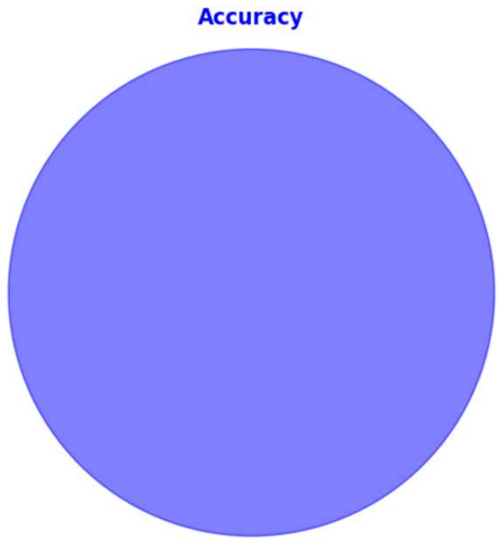
Accuracy:

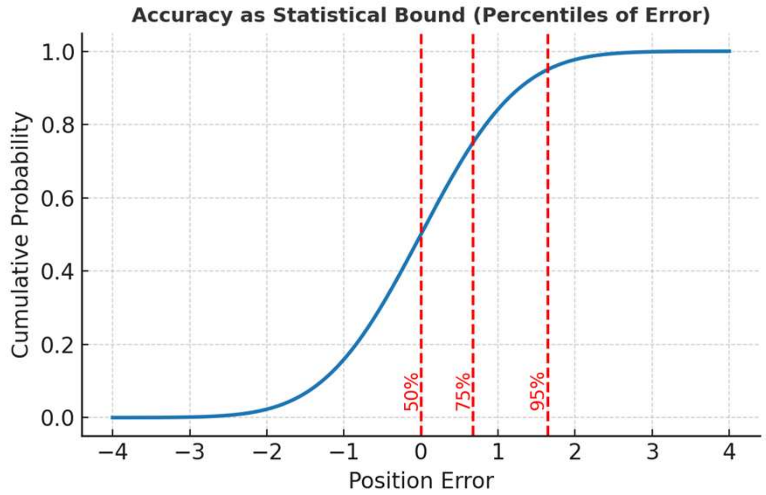
Closeness of estimated position/velocity to the true value

Achieving Accuracy?

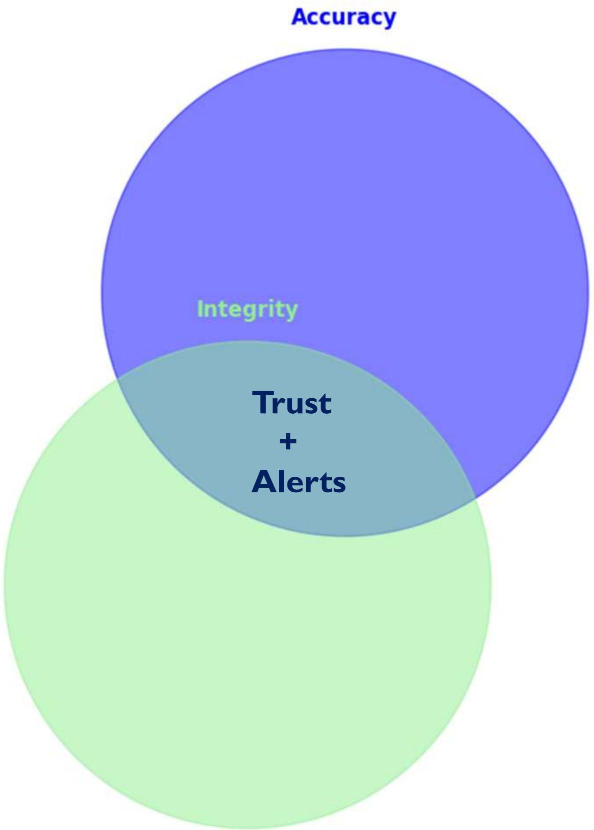
Depends on modeling and or precisely estimating sources of errors

- Space-related error
- Atmospheric errors
- Station/receiver errors

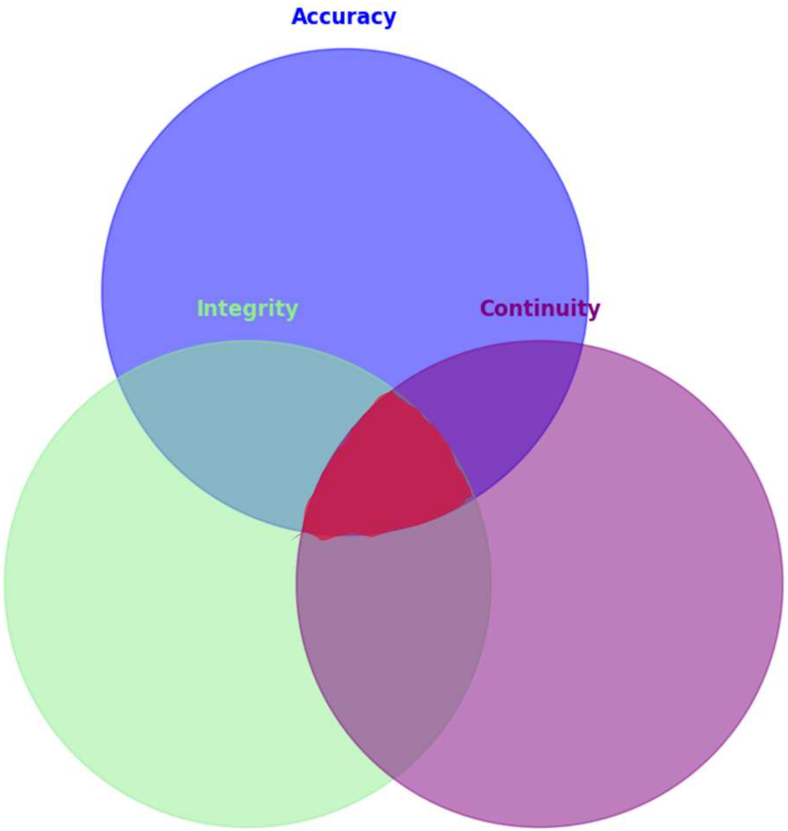




GNSS Quality Dimensions



GNSS Quality Dimensions

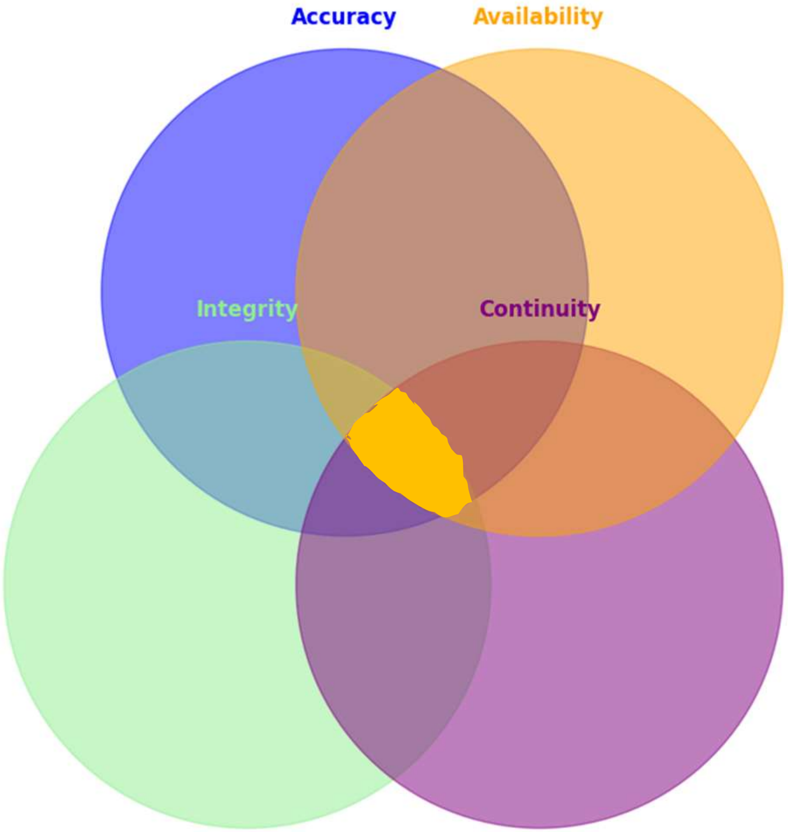


Continuity:

Pr{Integrity + Accuracy maintained over interval T}

GNSS Quality Dimensions

Four dimensions that define the overall quality of GNSS for safety-critical applications.



Availability:

Pr{GNSS service meets accuracy, integrity, and continuity requirements when it is needed}

Availability:
Can I use the service when I want to start?

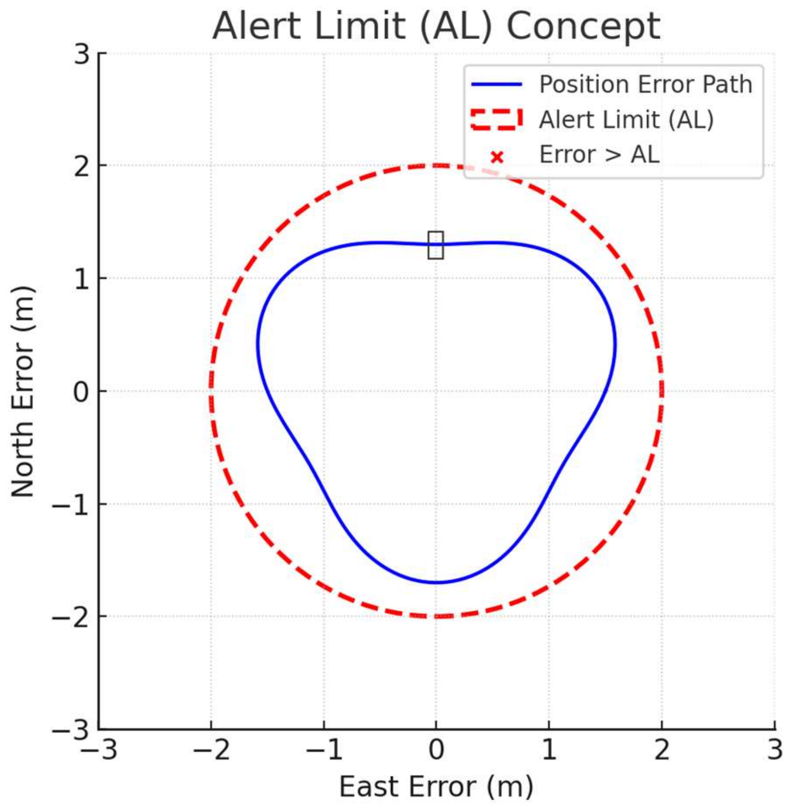
Continuity:
Once I start, will the service stay reliable until I finish?

GNSS Integrity Parameters

- Integrity is the measure of trust and the ability to warn users when the data is unreliable for safe navigation.

Integrity = Trust + Timely Alerts

GNSS Integrity Parameters



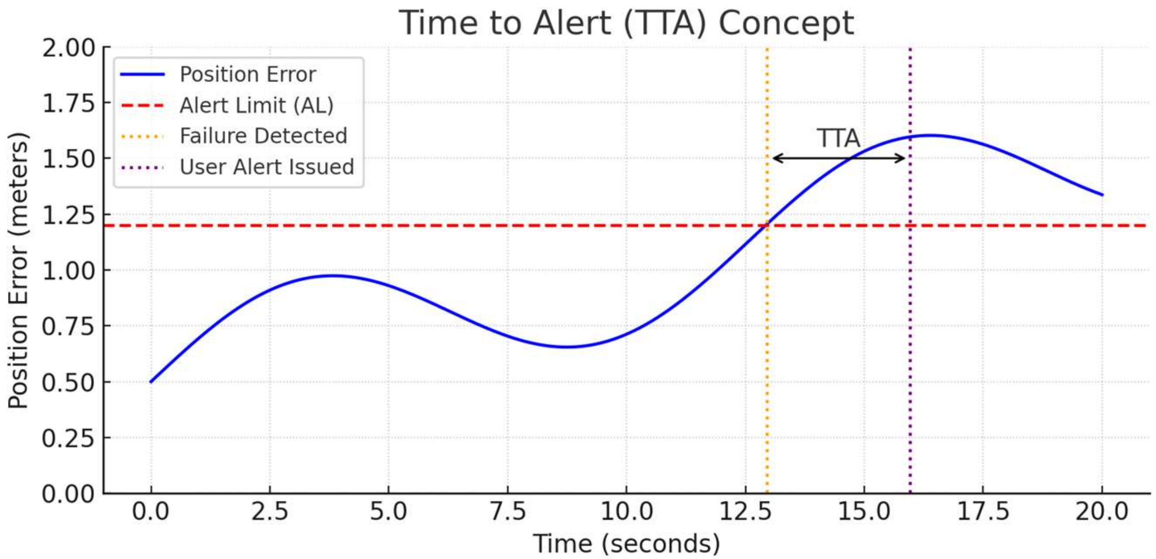
Alert Limit (AL)

The maximum position error that can be tolerated without compromising safety.

Examples:

- Aviation (LPV-200 approach): Horizontal AL = 40 m, Vertical AL = 35 m
- Automotive (SAE/ASIL-D, ISO 26262): 0.5 – 1.5 m for lane-keeping in highways

GNSS Integrity Parameters



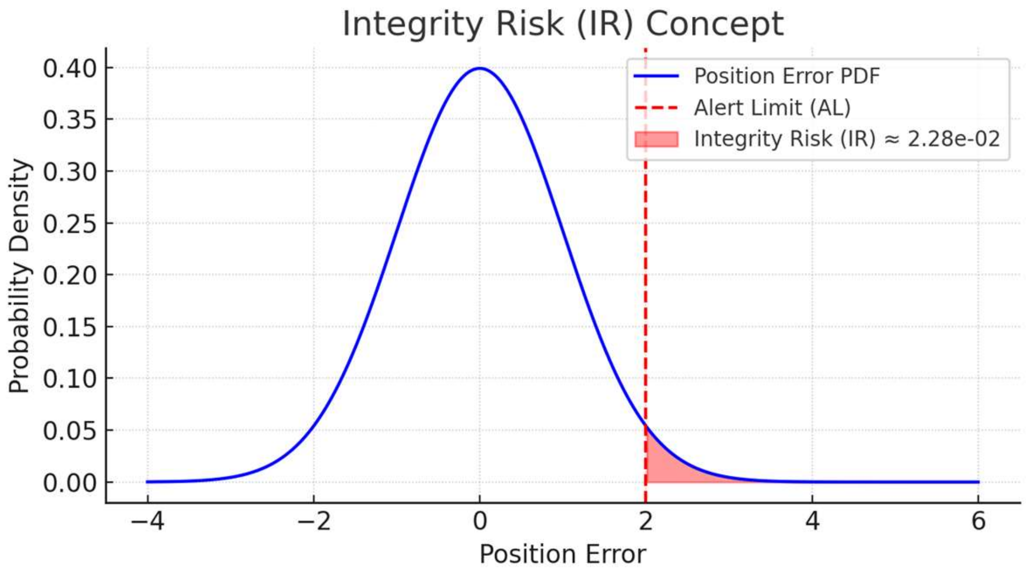
Time to Alert (TTA)

Maximum allowable time between a positioning failure and when the system alerts the user

Examples:

- Aviation (LPV-200): TTA = 6 s
- Automotive (lane-keeping): TTA = 1–2 s

GNSS Integrity Parameters



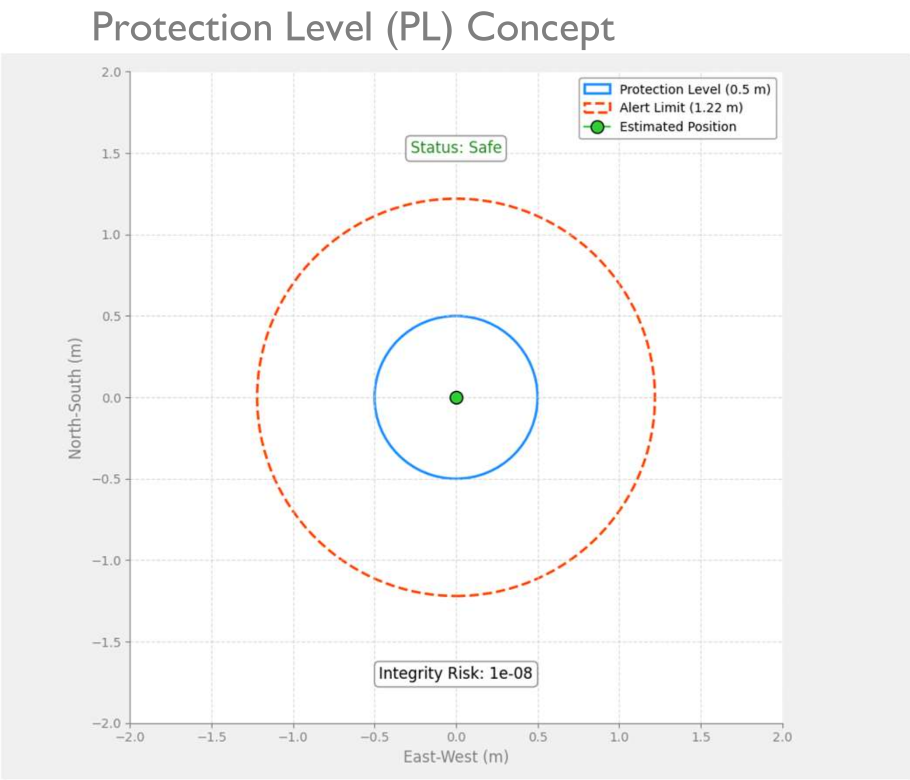
Integrity Risk (IR)

- The probability that the positioning system provides a solution that exceeds the Alert Limit (AL) without issuing an alert within TTA
- The the chance of Hazardously Misleading Information (HMI)

Examples:

- Aviation (LPV-200): IR ≤ 10^{-7} per approach
- Automotive (ASIL-D): IR ≈ 10^{-8} per hour

GNSS Integrity Parameters



Protection Level (PL)

A statistically computed bound on the position error.

- AL is set for a given application
- PL is computed by the system
- PL > AL, PL < AL comparison makes a decision on alerts

GNSS Integrity Parameters - Protection Level (PL)

PL is a function of pseudorange error and satellite-user geometry

GNSS Error Sources

- Satellite Orbit and clock errors
- Troposphere & ionosphere residual errors
- Multipath residual error
- Receiver noise residual error

Model the User Equivalent Range Error (UERE) as a Gaussian random variable.
URE – Combined effect of all residual errors

Satellite geometry affects measurement errors.
Compute Geometric Dilution of Precision (GDOP)

$$GDOP = \frac{\sqrt{\sigma_x^2 + \sigma_y^2 + \sigma_z^2 + \sigma_t^2}}{\sigma_{UERE}}$$

$$\sigma^2_{\mathrm{UERE}} = \sigma^2_{\mathrm{orbit}} + \sigma^2_{\mathrm{clock}} + \sigma^2_{\mathrm{tropo}} + \sigma^2_{\mathrm{iono}} + \sigma^2_{\mathrm{multipath}} + \sigma^2_{\mathrm{noise}}$$

$$\sigma_{pos} = \boxed{\sigma_{UERE}} \times GDOP$$

Compute Position Confidence (position error standard deviation)

PL is a function of geometry, UERE, and target integrity risk (IR)

$$\mathrm{PL} = k \cdot \sigma_{\mathrm{pos}}$$

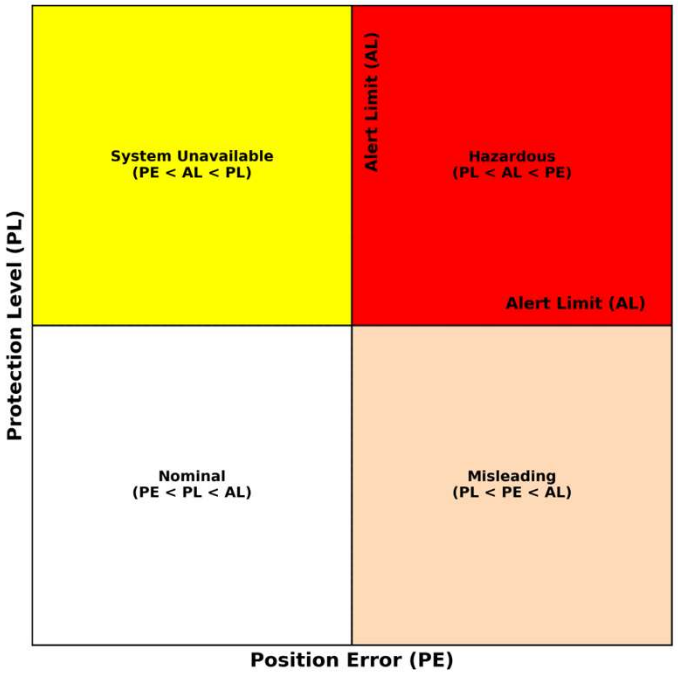
k is a scaling factor based on IR target.

PL is a protection bound: choose *k* so that *P(PE>PL) ≤ target IR*

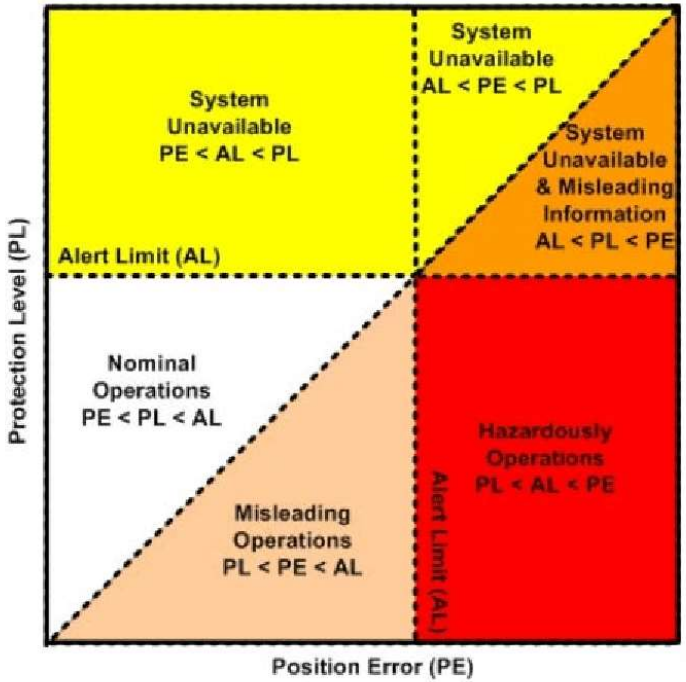
GNSS Integrity Parameters – The Stanford integrity diagram

In use by SBAS

My Simplified version

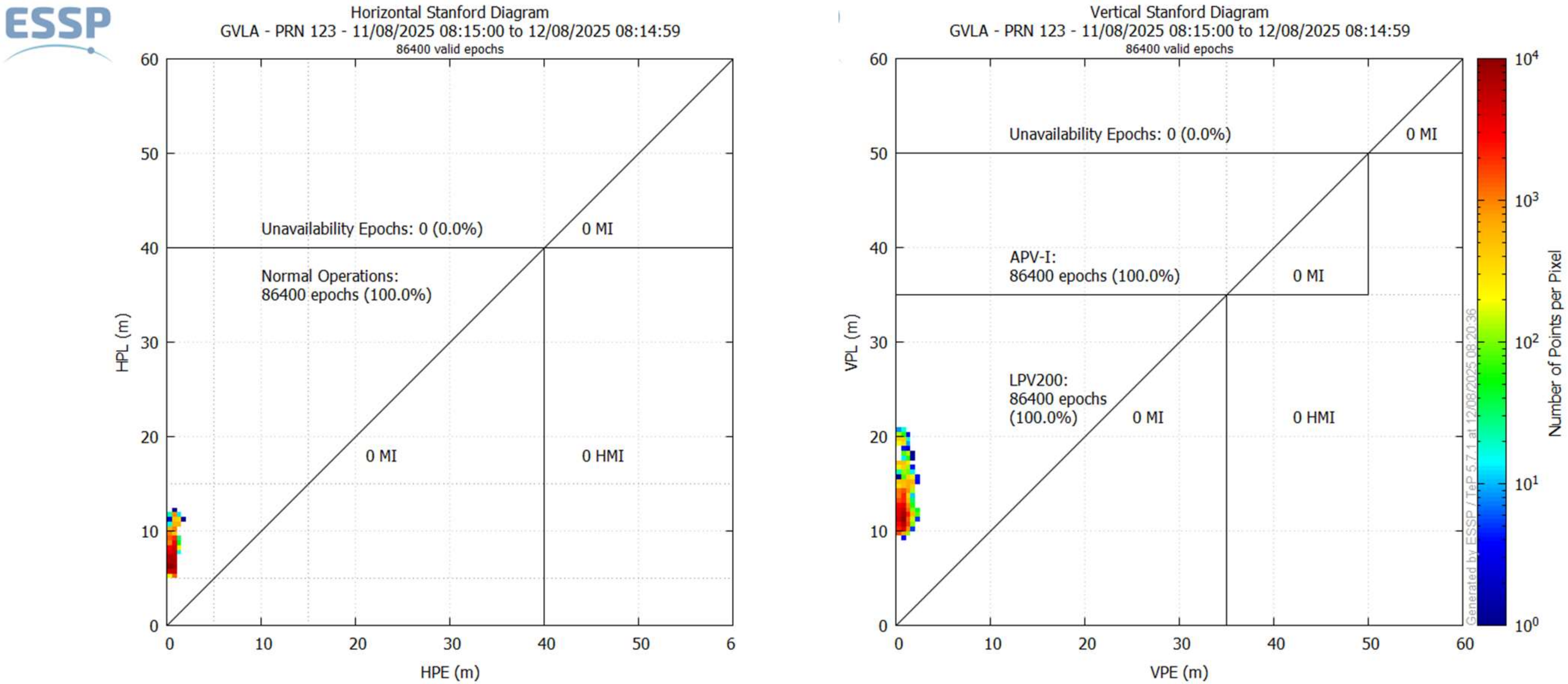


The Stanford version



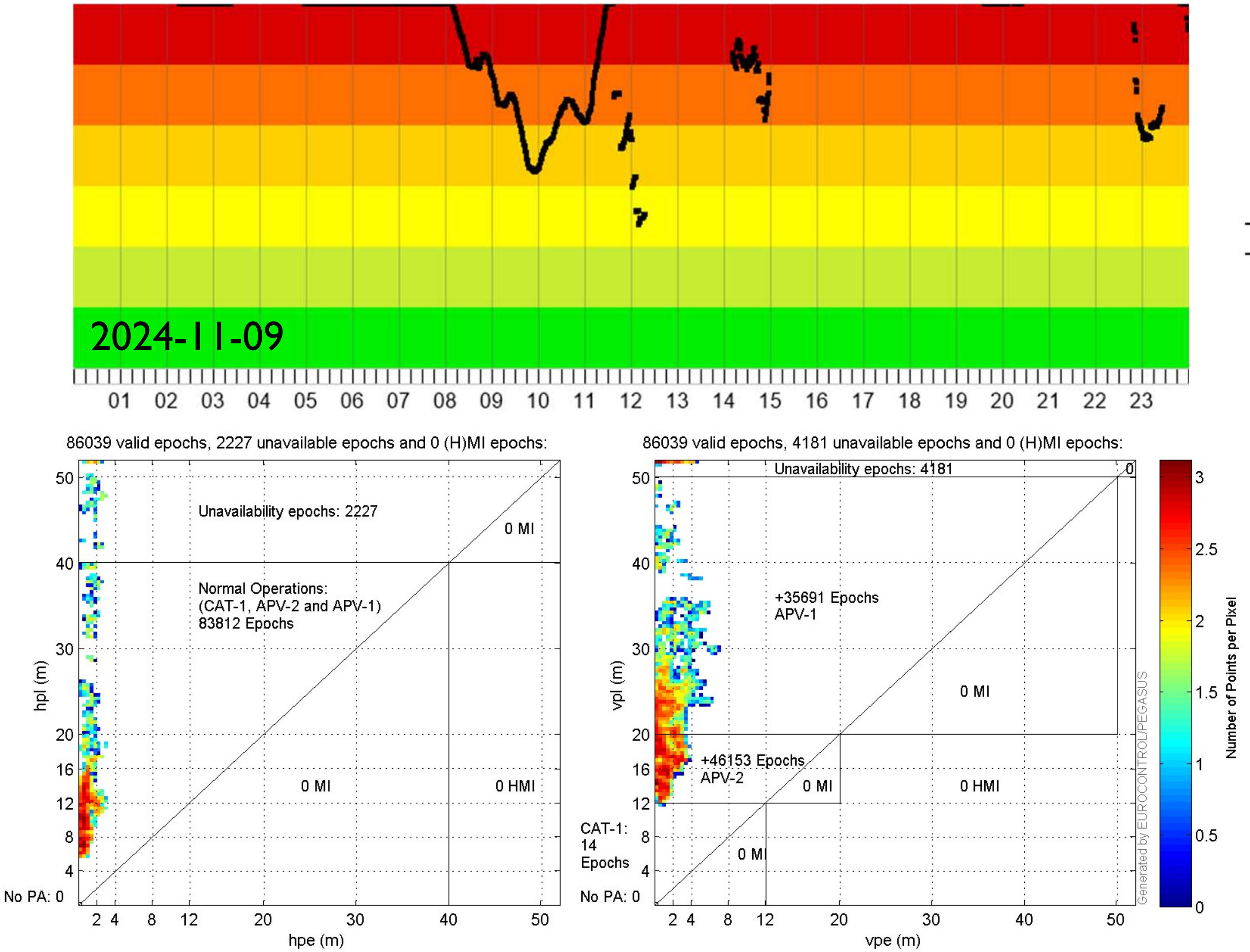
Use of the Stanford integrity diagram – EGNOS RIMS stations

RIMS station: Gävle, Sweden (GVLA)

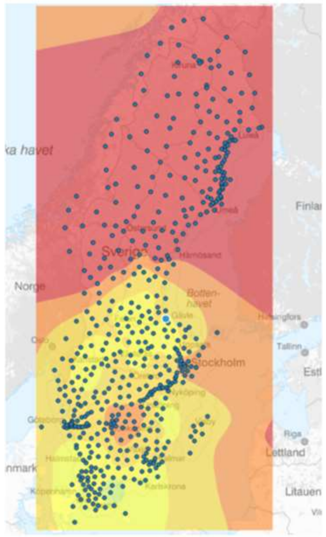


https://egnos.gsc-europa.eu/

Ionospheric Effects on GNSS integrity



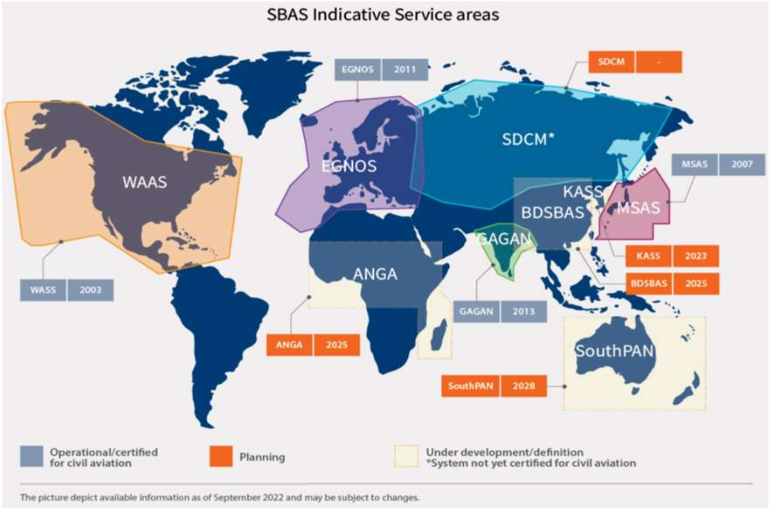
Modernized SWEPOS Ionospheric Monitoring Service



https://swepos.lantmateriet.se/services/ionomonitor.aspx

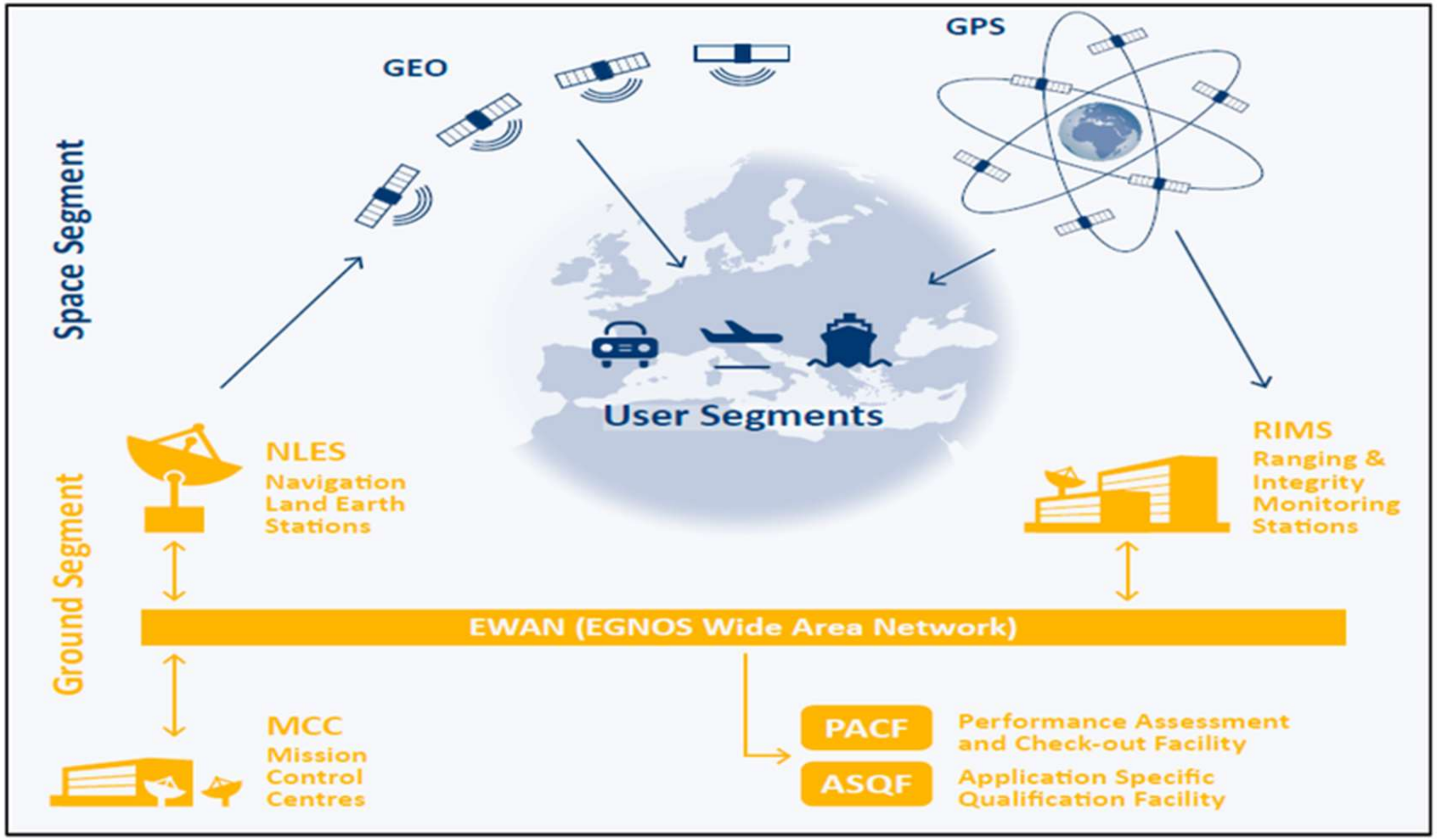
Integrity Systems

- Originated in aviation: defined and standardized integrity for safety-critical flight operations.
- Still emerging on the ground: ground-based GNSS lacks standardized and mature integrity measures.
- SBAS (Satellite-Based Augmentation Systems)
  - WAAS (USA)
  - EGNOS (Europe)
  - MSAS (Japan)
  - GAGAN (India)
  - SDCM (Russia)
- GBAS (Ground-Based Augmentation Systems)
- RAIM (Receiver Autonomous Integrity Monitoring) — Receiver-based method for fault detection.

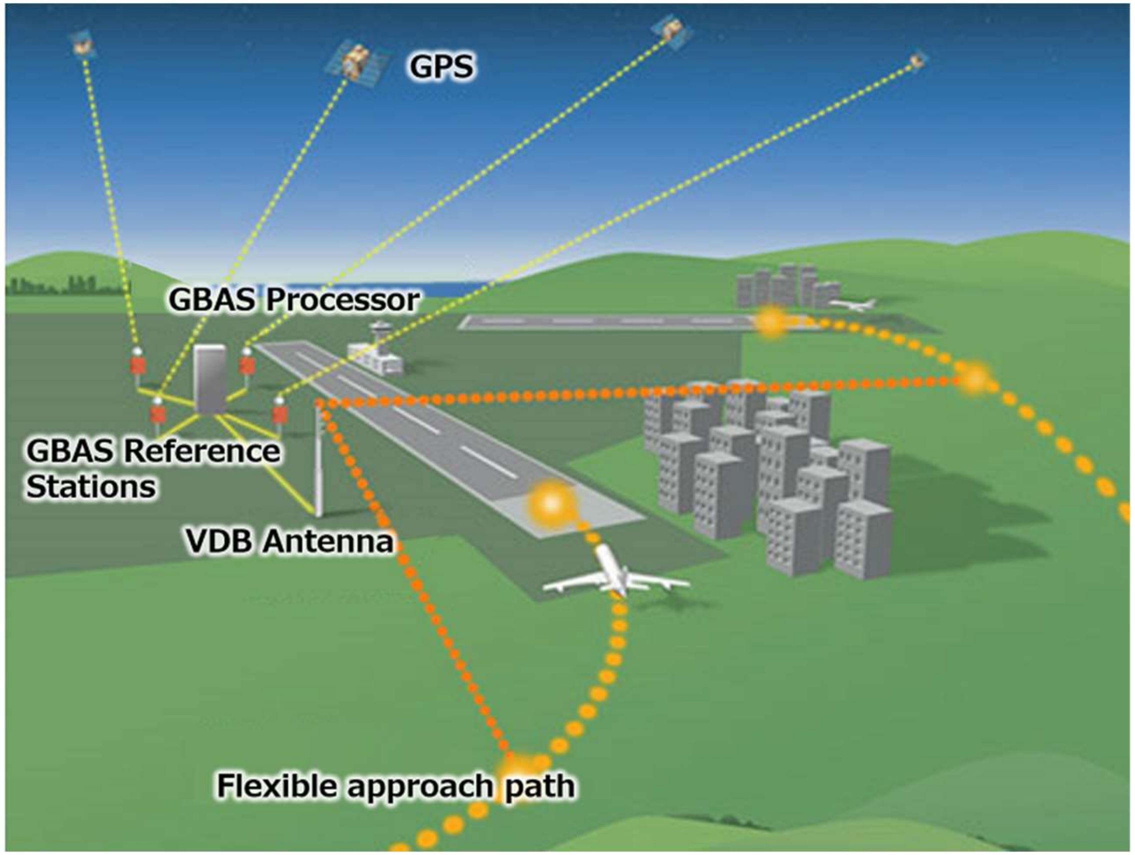


Satellite-Based Augmentation Systems (SBAS)

E.g., EGNOS Architecture: Delivering Integrity via SBAS

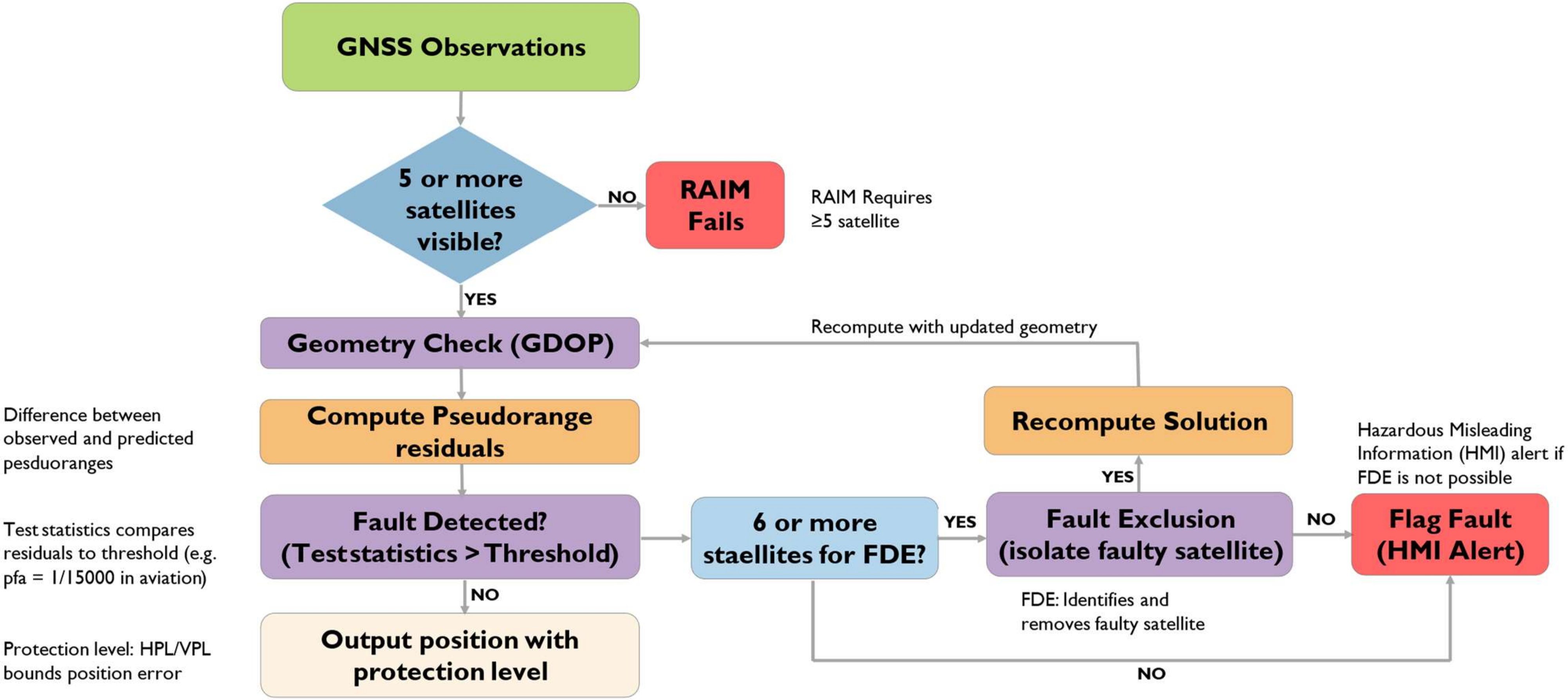


Ground-Based Augmentation System (GBAS)



https://www.nec.com/en/global/solutions/cns-atm/navigation/gbas.html

Receiver Autonomous Integrity Monitoring (RAIM)



RAIM variants

RAIM type	Measurement	FDE / Tolerated faults	External input	Navigation Constellations	Frequencies
Classical RAIM	Code	FDE / Single fault Solution separation (SS)	No Integrity data from Integrity Support Messages	LNAV	GPS 1
Advanced RAIM	Code	Real time FDE / Multiple faults	LPV-200	Multiple	Multiple
Relative RAIM	Carrier	FDE / Multiple faults SS method	External monitors	LPV-200	GPS -
Extended RAIM	Code	FDE / Multiple faults	Multiple sensors	Multiple	-
Carrier based RAIM	Carrier	FD (no exclusion) / Multiple faults	No	LNAV	Multiple Multiple
Time RAIM	Code and doppler	Forward backward FDE /	No	Multiple	-
Vision-Aided RAIM	Code	Fault detection / single fault assumption in [58] but multiple faults could be detected	Vision system provided landmarks RTK required corrections	LPV-200	GPS -

Based on Zabalegui et al., 2020

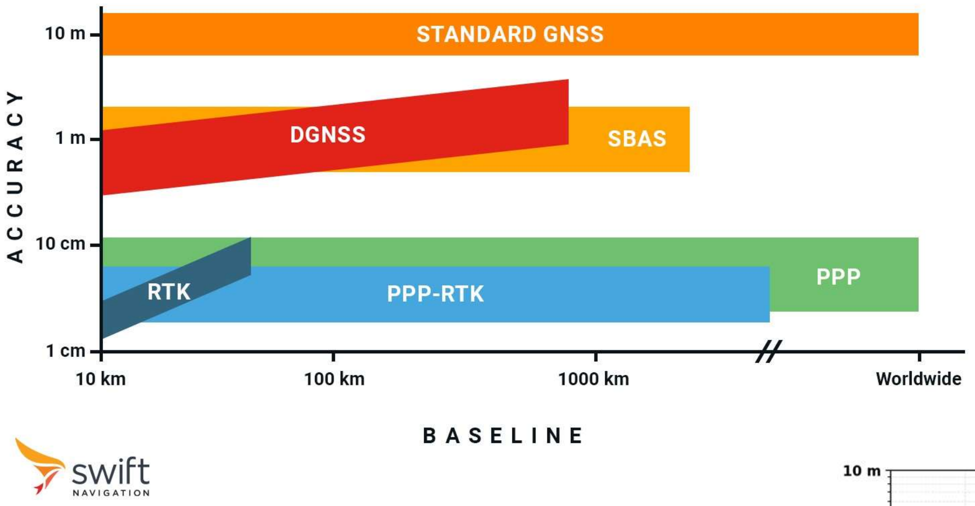
Integrity is Easy in the Sky… Hard on the Street

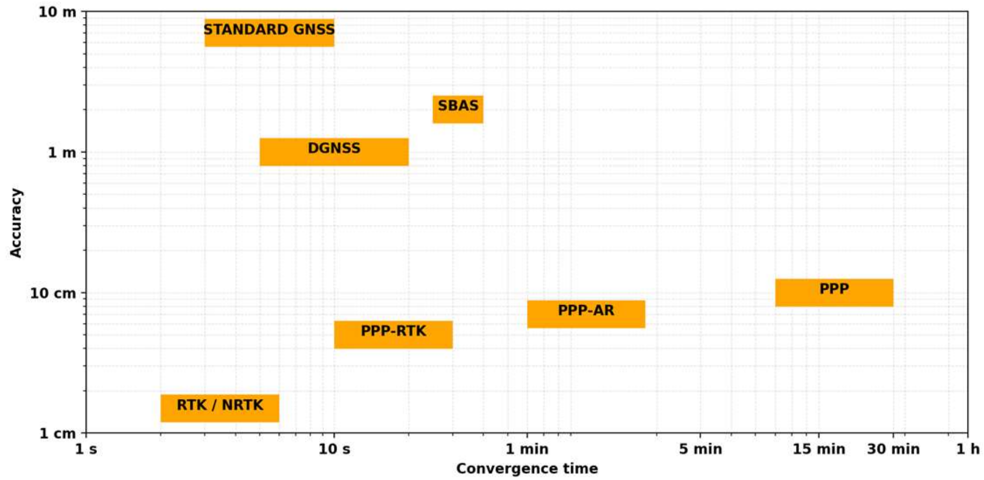
Aviation ☞ Only one failure occurs at a time

GNSS integrity

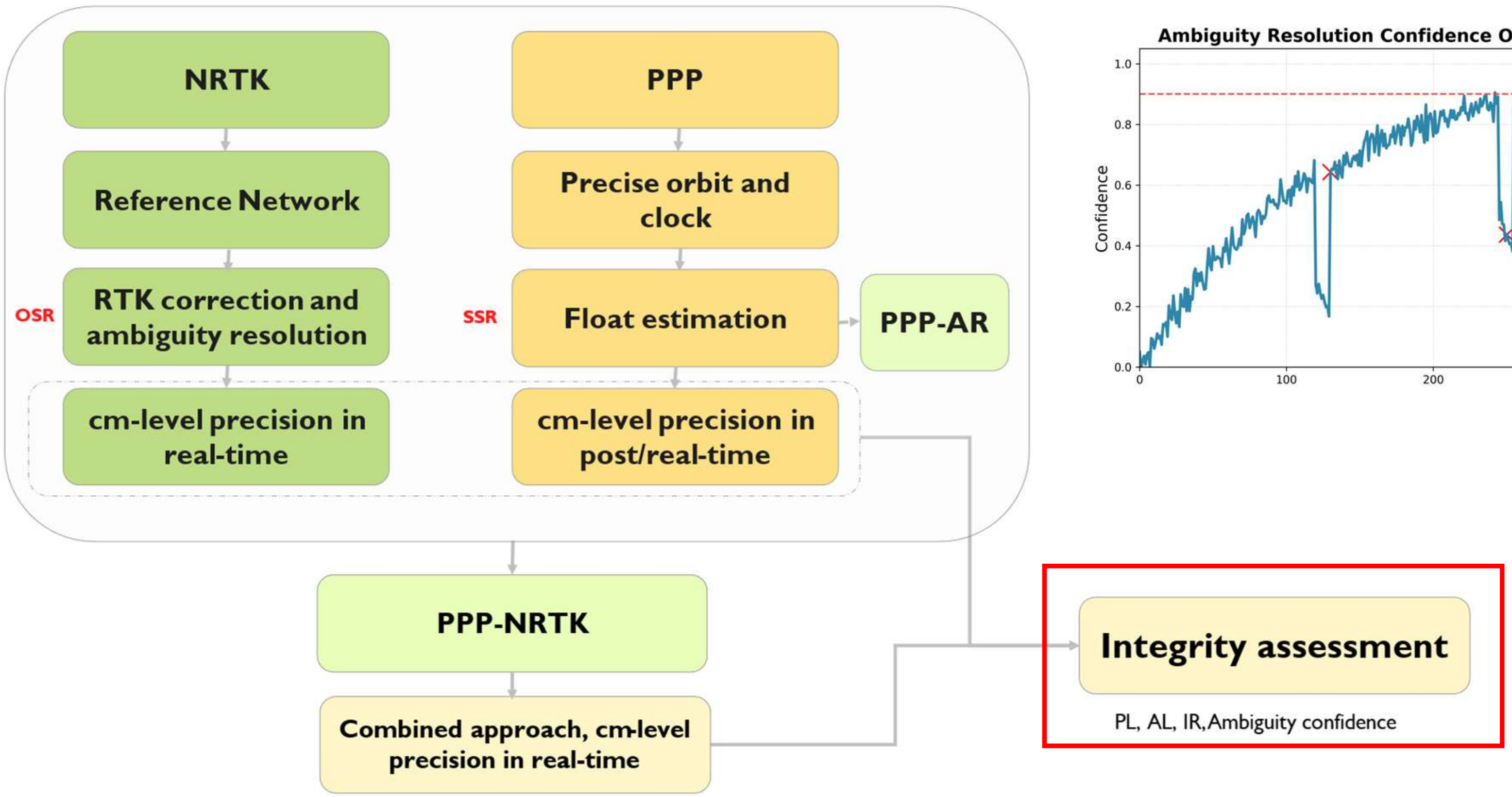
Urban land environment ☞ Multiple failures are managed in unison

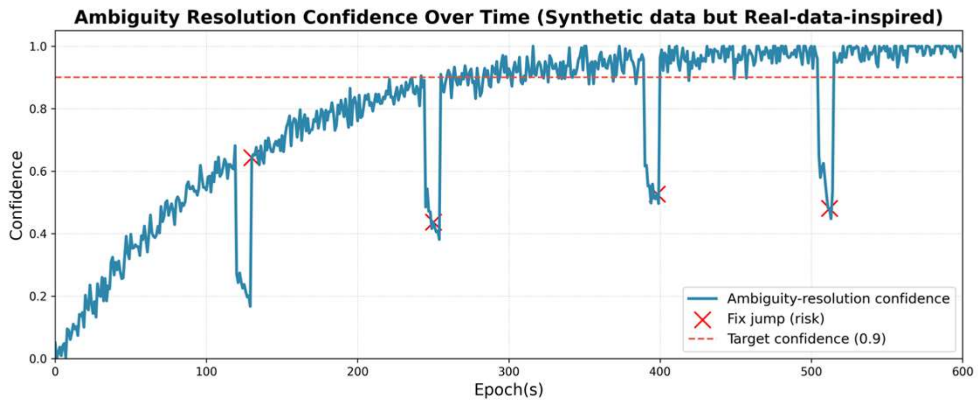
High Precision GNSS & Integrity





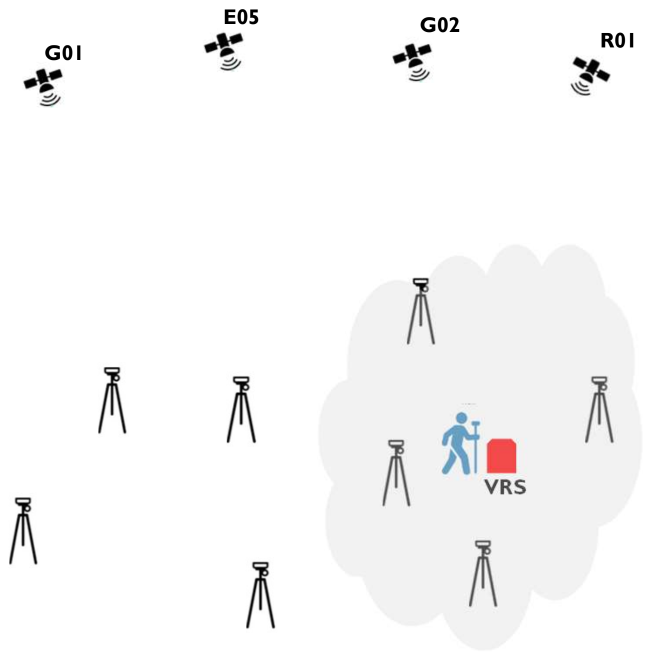
High Precision GNSS & Integrity





Fixing quickly ≠ fixing correctly

Monitoring Network RTK Integrity



As NRTK adoption grows for autonomous navigation and other mass market applicaitions, **integrity** is key to meeting standards like ASIL D (IR ≈ 10^{-8})

CORS → **Server (NRTK Software)** → **Rover**

CORS

Risk
- Ionosphere
- Signal Interference
- Multipath, snow, antenna

Server (NRTK Software)

Safe
- Reliable VRS interpolation

Risk
- Latency
- Network Failure

Rover

Safe
- Successfull Ambiguity resolution

Risk
- Cycle slips, Integer Error
- Poor GDOP
- Interference

NRTK (E.g., Trimble Pivot Platform (TPP))

- Manages CORS and generates VRS corrections

- **Includes integrity monitoring to ensure reliability of the corrections**
  - **ARAIM/RAIM Integration (receivers)**
    - **Alloy – RAIM, MAXWELL, IonoGaurd**
    - **Septentrio PolarX5 – RAIM+, AIM+, IONO+, APME+**
  - **Trimble Integrity Manager App**
  - **Trimble Rover Integrity App**
  - **VRS3Net App**
  - **Pivot RTX App**

- Doesn't broadcast integrity messages via Ntrip and RTCM containing
  - Parameters to compute Protection level (PL)
    - User Differential Range Error (UDRE)
    - Grid Ionospheric Vertical Error (GIVE)
  - Fault flag or risk indicator

Challenges of Providing Integrity Messages in Today's NRTK Services

Standardization Gaps

- No unfied messages for integrity as in SBAS
- RTCM needs to be extended for VRS-specific PL/AL/UDRE messaging

Latency & communication Issues

- bandwidth vs. detailed integrity info
- Sending SBAS-like messages over NTRIP adds delay, which may exceed time-to-alert requirements

Network Dependency

- Dependency on ground networks which are vulnerable to outages
- Detecting and removing a faulty station in a large network is challenging

Error Propagation

- Network errors (e.g., atmospheric biases in VRS) must be bounded in messages in broadcastable formats.

Scalability

- For mass adoption (e.g., autonomous vehicles), certifying NRTK messages to ICAO/RTCA standards can be challenging.

Multi-GNSS / Multi-Frequency Complexity

- Generering SBAS like PL for multi-GNSS is complex, due to differing error models, for example.

Challenges of Providing Integrity Messages in Today's NRTK Services

User Equipment Limitations

- Many rovers can not use PL-AL-type messages today – would require firmare upgrades

Security & Spoofing Risks

- Integrity messages could also be spoofed unless authenticated

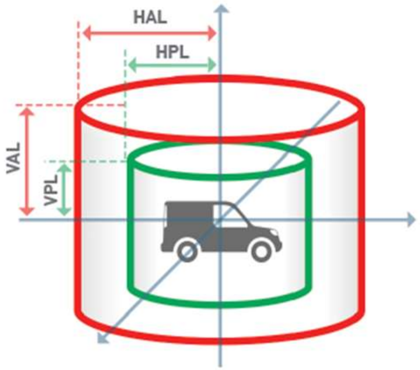
Proprietary data stream bypasses the RTCM limit

But then interoperability is limited to systems that understand a specific system's API

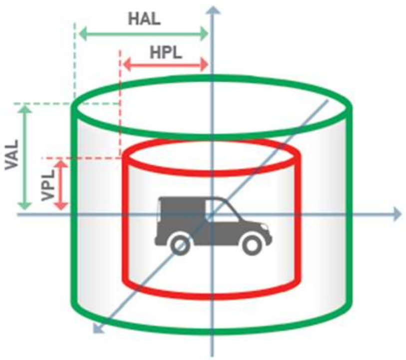
E.g., Swift Navigations SBAS-style integrity messages

- Integrity parameters between Starling positioning engine (rover) and Skylark (PPP-RTK) correction service.
- Protection Limit (PL) is computed by Starling
- Alert Limit (AL) and Time-to-Alert (TTA) are set at the application/system level.
- Starling outputs **position + PL + integrity status**
- The application compares PL against AL

PL < AL
Safe operation



PL > AL
Unsafe operation



Commercial PPP-RTK/NRTK services that send integrity messages (Outside of SBAS)

Provider / System	PL/AL Broadcast	
Swift Navigation – Skylark	✅ Yes – HPL/VPL + integrity flags	Proprietary SBP/RTCM; ASIL-D automotive & rail focus
Hexagon / NovAtel – TerraStar X / Apollo	✅ Yes – for OEM safety-critical configs	Proprietary; NDA with OEMs
Sapcorda – SAPA Premium (pre-u-blox)	✅ Yes – in premium service	Proprietary format; safety-critical GNSS corrections
Fugro – Starfix / Marinestar	✅ Yes – maritime dynamic positioning	Proprietary Format
Trimble RTX Integrity (Automotive mode)	✅ Yes – in automotive safety-certified mode	ISO 26262 certified; proprietary closed protocol
Trimble RTX (Standard)	❌ No – PL computed internally in receiver	Commercial RTX service; no explicit PL output
u-blox PointPerfect	❌ No – metadata only, receiver computes PL	SPARTN format includes variances but no PL

Proprietary Format - *Limited Interoperability, Vendor lock-in, costly, Slower Industry Standardization*

There is an RTCM committee working on integrity messages for both NRTK and PPP-RTK

Development of RTCM SC-134 Messages for High-Integrity Precise Positioning

- Work in progress to include integrity messages for both NRTK and PPP-RTK in RTCM
  - RTCM established a committee (SC-134) in 2018 to create integrity standards for high-accuracy GNSS applications
  - Unlike SBAS or GBAS, the SC-134 standard must cover a wide range of applications, augmentation technologies, and both current and future GNSS systems
  - The standard is designed to be multimodal, multiservice, and technology-agnostic.
  - It provides a generalized definition of Protection Level, so integrity parameters can be used across different monitoring methods (SBAS, GBAS, ARAIM, etc.).
    - $IR \equiv P(|X\ Position\ Error| > XPL, No\ Alert)$
  - Data fields and messages are being defined to support different user needs, augmentation systems, and monitoring approaches.
  - First release of the SC-134 standard is expected in 2025

RINEX
RTCM
SINEX
IONEX
SP3
ANTEX

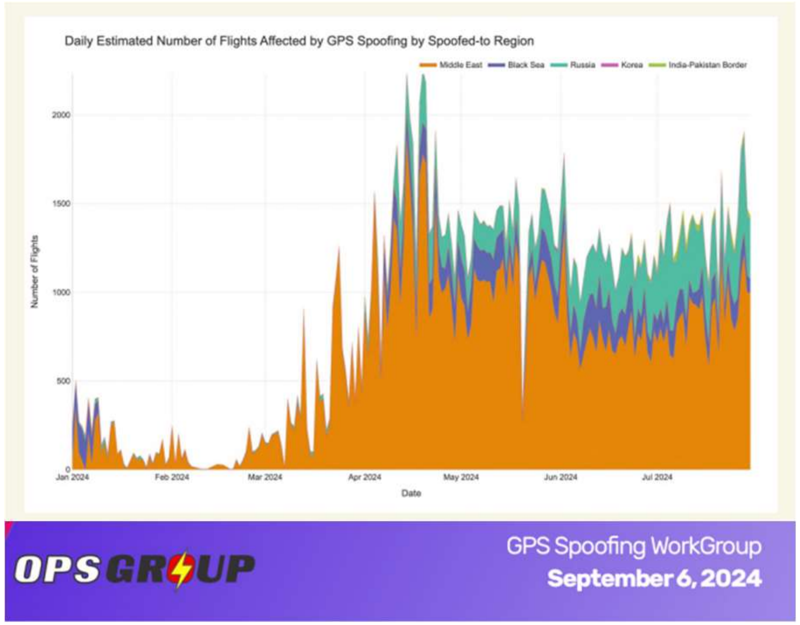
→ Standardization is what made GNSS processing and interoperability possible worldwide

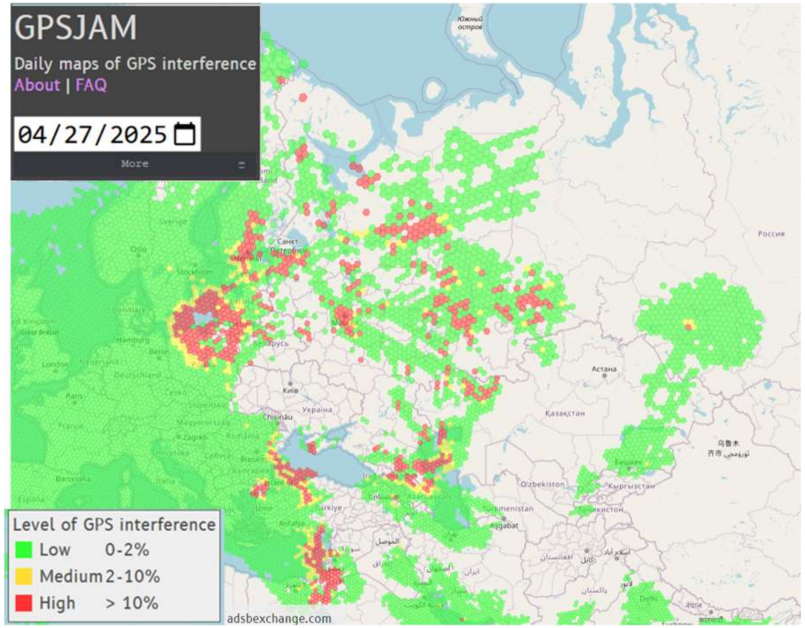
RTCM SC-134 → Would lead proprietary solutions to converge into common, standardized framework for integrity messaging

Emerging Integrity Threats

- Increased jamming and spoofing events globally
  - International interference is increasing
  - Spoofing 500% increase in 2024
  - Some systems do not easily recover
  - Some erroneously report recovery

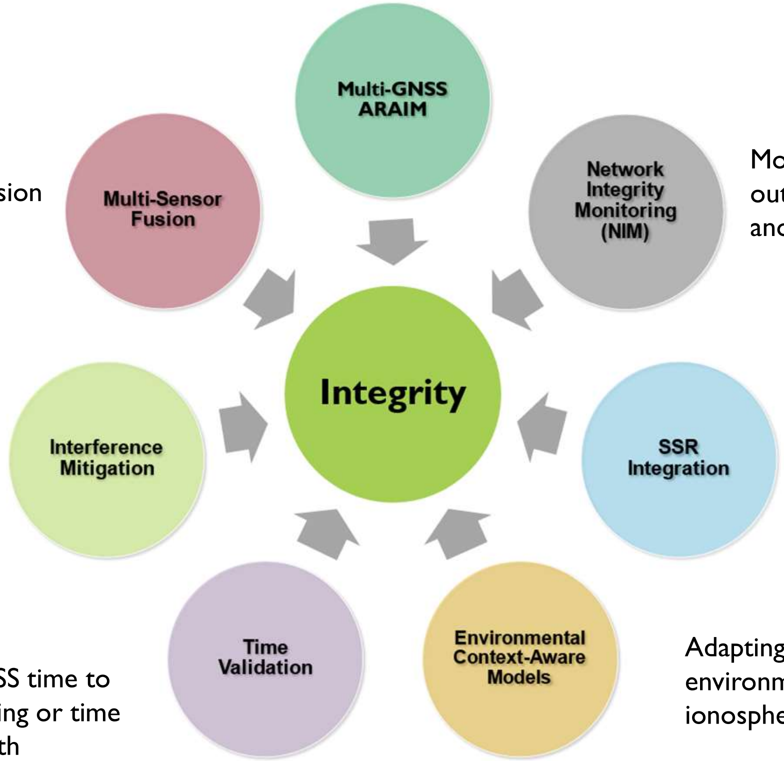
- RTK and PPP are vulnerable to both time and signal spoofing. Their trust model assumes
  - All satellite signals are genuine
  - Corrections are valid





Integrity Enhancement Techniques

MultiGNSS to compute Protection Levels (PL) and detect faults at the rover



GNSS + INS, odometry, and vision for continuity during GNSS outages.

Monitor reference stations, flagging outages, interpolation errors, and anomalies in real time

Detects and mitigates jamming/spoofing

SSR would improve robustness of corrections and integrity checks.

Validate GNSS time to detect spoofing or time shifts, e.g. with NTP/network time sources

Adapting PL and alerts based on environment (urban canyons, ionospheric disturbancesl)

Takeaways!

- No integrity = no trust
  - Detect errors and warn users in time
- Aviation sucess story
  - Mature frameworks (SBAS, ARAIM, PL/AL) proven in safety-critical operations.
- On Land: still immature 🚗 🚆
  - Multipath, low redundancy, and complex environments make integrity harder.
- Why it matters now?
  - Rise in GNSS threats: jamming, spoofing, interference.
  - Growing demand from autonomous cars, rail, maritime, drones, etc.
- What we need to do?
  - Develop standardized integrity messages (for RTK/PPP-NRTK).
  - Advance network integrity monitoring for real-time detection.
  - Encourage open research & student projects to develop integrity tools

No integrity = no trust

THANKS! WE ARE AVAILABLE AT…

WEBSITE	www.lantmateriet.se
CONTACT	www.lantmateriet.se/kontakt
PHONE	0771-63 63 63
LINKEDIN	www.linkedin.com/company/lantmateriet
FACEBOOK	www.facebook.com/lantmateriet
INSTAGRAM	www.instagram.com/lantmateriet

LANTMÄTERIET