A Safety Processor to guarantee integrity of High-accuracy products

ION GNSS+ 2022

Session: Advances in High Precision Positioning

P.F. Navarro, I, Rodríguez, H.S. Martínez, D. Calle, F.J. Sobrero, GMV - Spain

INNOVATING SOLUTIONS

Contents

SAFE AND ACCURATE GNSS FOR ADAS

GNSS TECHNOLOGIES FOR ADAS

TECHNICAL BENEFITS

High Accuracy Positioning
Sub- decimiter Level

Absolute Positioning
Other technologies only provide differential positioning

Robust Safety Case
High maturity (SOTIF-like) reached and demonstrated in applications for civil aviation
Key for ISO26262 safety argumentation

Global Coverage
GNSS Availability EVERYWHERE

Independency
This technology is independent from other sensors in the car

Velocity
GNSS provides absolute velocity of the vehicle

Orientation
GNSS provides orientation values when integrated with IMU

<u>Setup always available</u>
Antenna and **Receiver** are already in place, due to its usage in other applications

- E-CALL
- TOLLING
- TACOGRAPH
- …

<u>Built-In AntiSpoofing & AntiJamming</u>

<u>GNSS trajectory</u>

GNSS is currently a booming technology, with years of maturity, acting as the technological solutions for a wide variety of sectors. Many countries are investing on developing their own Navigation Systems, proving its worth

SAFE & ACCURATE GNSS FOR ADAS

High Accuracy Requirements

Key Performance Indicator	Value
Horizontal Accuracy	< 10 cm RMS
Cold Convergence Time	< 30 sec
Hot Convergence Time	Almost Instantaneous
Dead Reckoning	Limited Degradation
Service Availability	> 99.9 %

Integrity Requirements

Key Performance Indicator	Value
Integrity Risk (TIR)	Up to 10-7 per hour
Horizontal Protection Levels (PLs)	2 – 5 meters (TIR dependent)

ROAD STANDARDS

ISO26262

In-car Functional Safety

ISO/PAS 21448

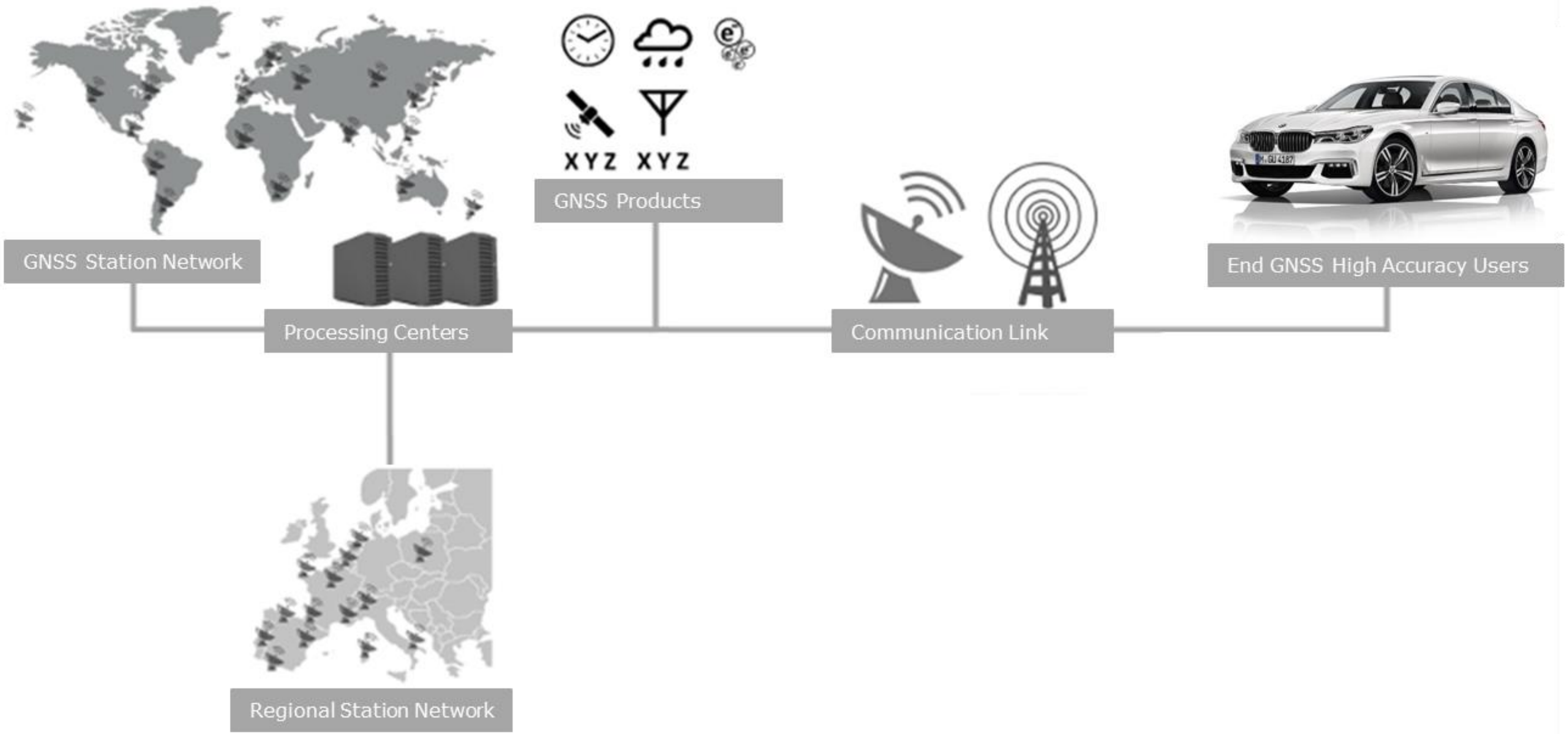
Safety of the Intended Functionality

SOTIF

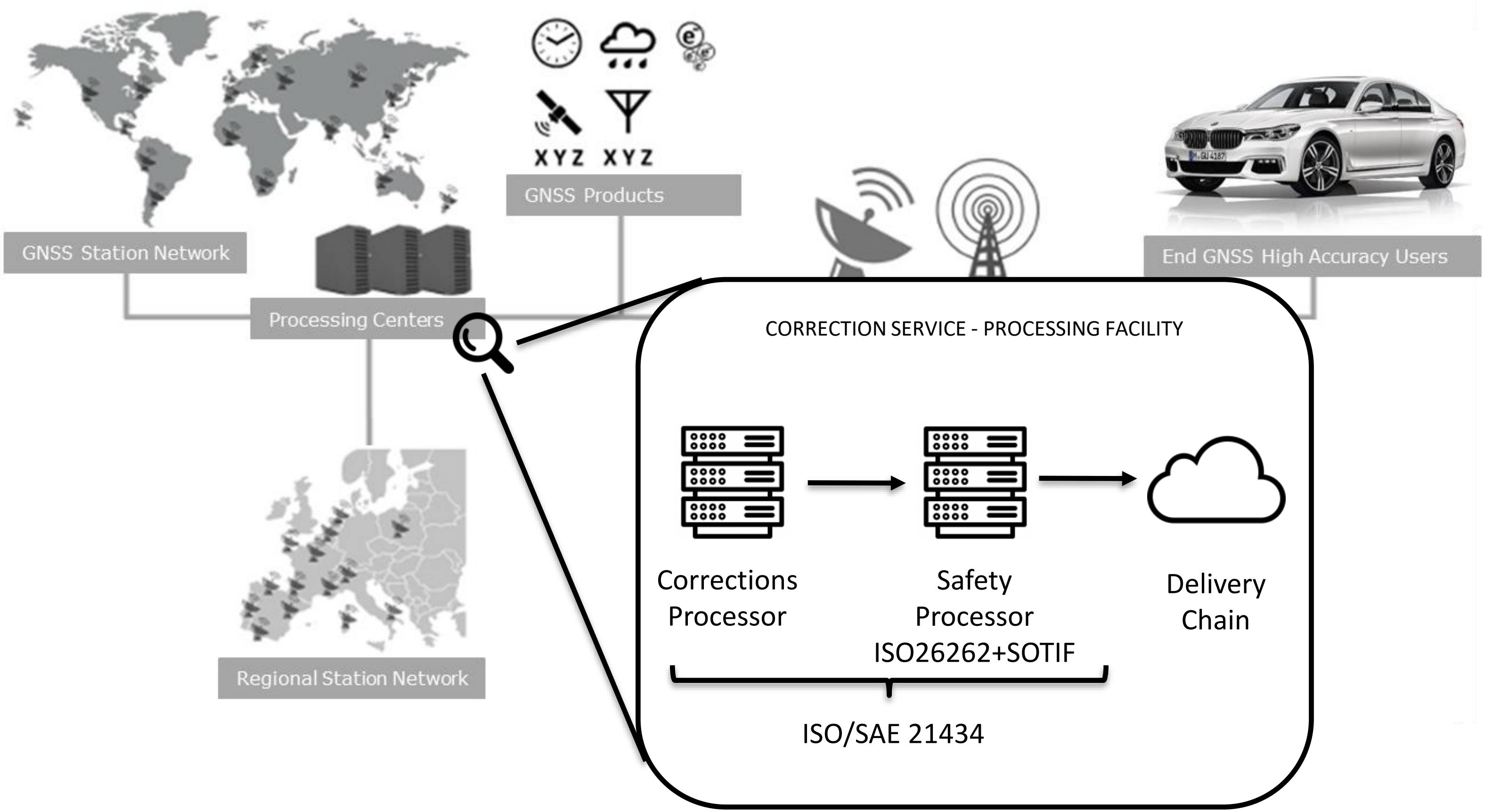
ISO/SAE 21434

Cybersecurity and Security Measures

E2E SOLUTION FOR ADAS



SAFE AND ACCURATE GNSS FOR ADAS

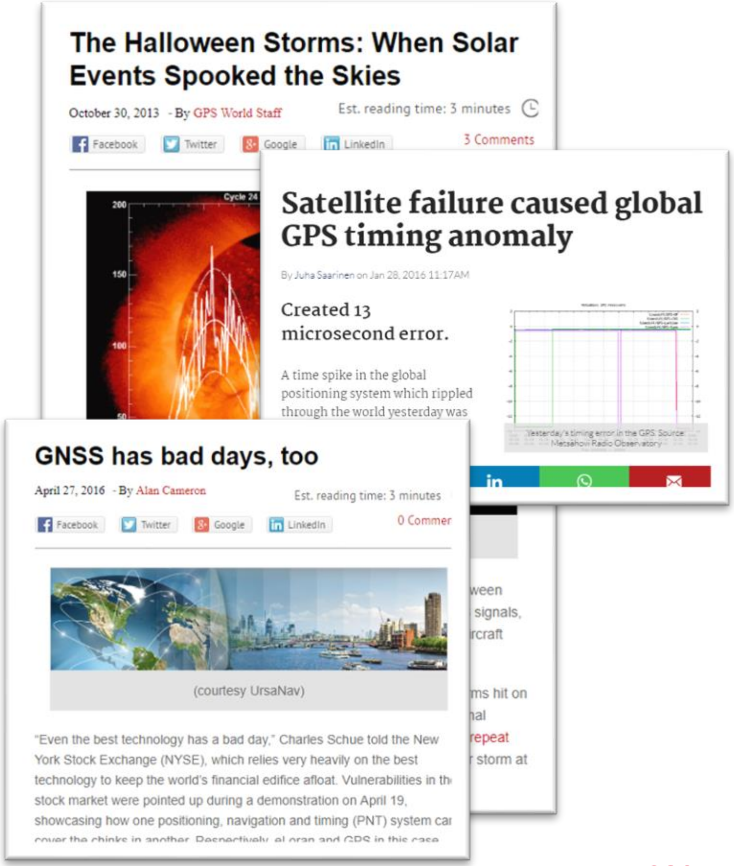


gmv

CORRECTIONS SERVICE INTEGRITY

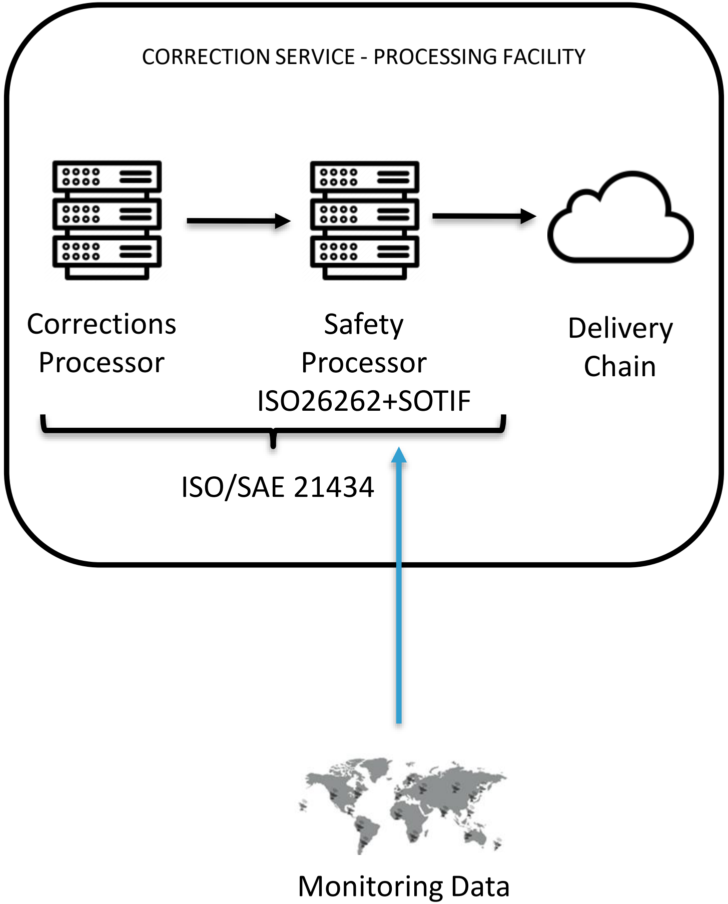
CS CONTRIBUTION TO GNSS INTEGRITY

- Failure modes affecting the corrections are detected and removed so that corrections transmitted to users are fault-free.
- GNSS satellite or constellation failures, degraded ionospheric conditions (e.g. ionospheric storms) are detected and users warned
- Corrections Service contributes to Positioning Engine PL computation through integrity bounds on the corrections errors.
- Corrections Service sends integrity flags to users within the corrections message



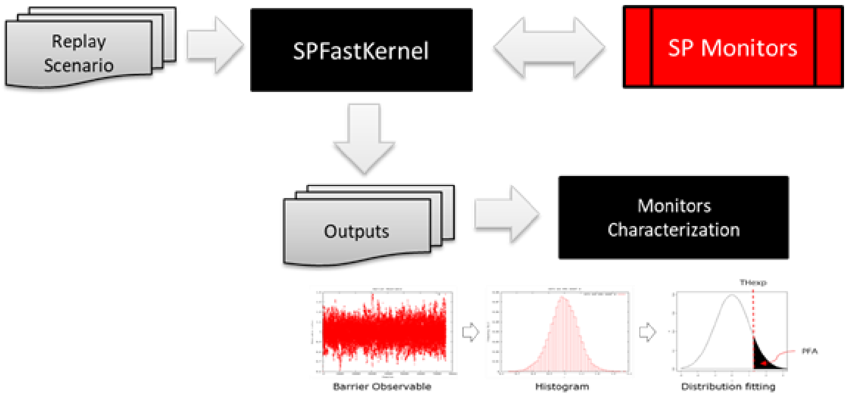
CS SAFETY ARCHITECTURE

- CS uses "correct then monitor" approach
  - Corrections Processor computes corrections but does not assures its integrity
  - Safety Processor checks the corrections generated by the Corrections Processor and computes integrity bounds
- Safety Processor follows safety development standards (**ISO26262** ASIL-B)
- Safety case developed for CS to assure it meets the integrity requirements
- Safety Processor implements monitors to detect the feared events affecting orbit and clock, phase bias and ionospheric corrections
- Safety Processor uses GNSS data from monitoring stations to check corrections



SAFETY PROCESSOR VALIDATION

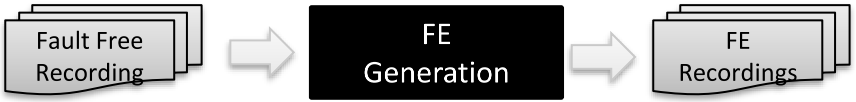
- Safety Processor validation based on:
  - Fault-free scenarios (real data) to characterize monitors observables and set thresholds
  - Simulated faulty-scenarios to test detection of failure modes
  - Analytical argumentation

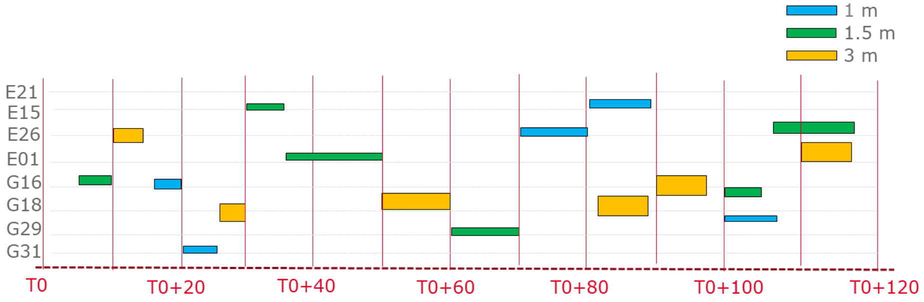


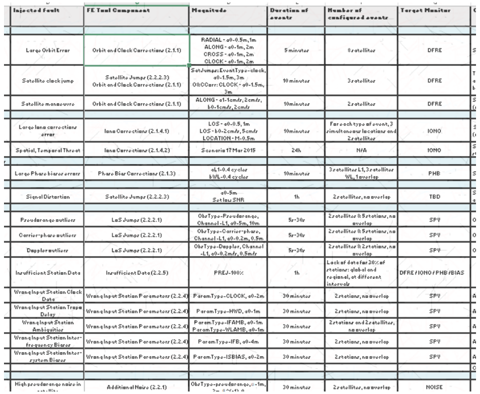
- Fault-free validation:
  - Based on real GNSS data
  - Replay tool (SPFastKernel) used to process recorded scenarios
  - Monitor Characterization tool used to tune the monitors and check the test observables

SAFETY PROCESSOR VALIDATION

- Faulty scenarios validation:
  - FE Genration tool has the capability to introduce failure modes (Feared Events):
    - Large errors in orbit & clock, ionospheric, phase bias corrections France
    - Ionospheric Storms
    - Satellite failures
    - Wrong monitoring data





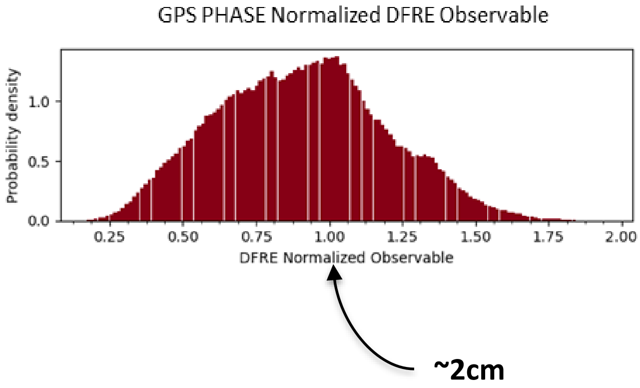


Injected fault	FE Tool Component	Magnitude	Duration of events	Number of configured events	Target Monitor
Large Orbit Error	Orbit and Clock Corrections (2.1.1)	RADIAL - a0-0.5m,1m ALONG - a0-1m, 2m CROSS - a0-1m, 2m CLOCK - a0-1m, 2m	5 minutes	8 satellites	DFRE
Satellite clock jump	Satellite Jumps (2.2.2.3) Orbit and Clock Corrections (2.1.1)	SatJumps: EventType-clock, a0-1.5m, 3m O&CCorr: CLOCK - a0-1.5m, 3m	10 minutes	3 satellites	DFRE
Satellite manoeuvre	Orbit and Clock Corrections (2.1.1)	ALONG - a1-1cm/s, 2cm/s, b0-1cm/s, 2cm/s	10minutes	2 satellites	DFRE
Large Iono corrections error	Iono Corrections (2.1.4.1)	LOS - a0-0.5, 1m LOS - b0-2cm/s, 5cm/s LOCATION - M-0.5m	10minutes	For each type of event, 3 simultaneous locations and 2 satellites	IONO
Spatial, Temporal Threat	Iono Corrections (2.1.4.2)	Scenario 17 Mar 2015	24h	N/A	IONO
Large Phase biases errors	Phase Bias Corrections (2.1.3)	aL1-0.4 cycles bWL-0.4 cycles	10minutes	3 satellites L1, 3 satellites WL, 1 overlap	PHB
Signal Distortion	Satellite Jumps (2.2.2.3)	a0-5m Set low SNR	1h	2 satellites, no overlap	TBD
Pseudorange outliers	LoS Jumps (2.2.2.1)	ObsType-Pseudorange, Channel-L1, a0-5m, 10m	5s-30s	2 satellites & 5 stations, no overlap	SPV
Carrier-phase outliers	LoS Jumps (2.2.2.1)	ObsType-Carrier-phase, Channel-L1, a0-0.2m, 0.5m	5s-30s	2 satellites & 5 stations, no overlap	SPV
Doppler outliers	LoS Jumps (2.2.2.1)	ObsType-Doppler, Channel-L1, a0-0.2m/s, 0.5m/s	5s-30s	2 satellites & 2 stations, no overlap	SPV
Insufficient Station Data	Insufficient Data (2.2.5)	PREJ-100%	1h	Lack of data for 30% of stations: global and regional, at different intervals	DFRE / IONO / PHB / BIAS
Wrong Input Station Clock Data	Wrong Input Station Parameters (2.2.4)	ParamType-CLOCK, a0-2m	30 minutes	2 stations, no overlap	SPV
Wrong Input Station Tropo Delay	Wrong Input Station Parameters (2.2.4)	ParamType-HWD, a0-1m	30 minutes	2 stations, no overlap	SPV
Wrong Input Station Ambiguities	Wrong Input Station Parameters (2.2.4)	ParamType-IFAMB, a0-1m ParamType-WLAMB, a0-1m	30 minutes	2 stations and 2 satellites, no overlap	SPV
Wrong Input Station Inter-frequency Biases	Wrong Input Station Parameters (2.2.4)	ParamType-IFB, a0-4m	30 minutes	2 stations, no overlap	SPV
Wrong Input Station Inter-system Biases	Wrong Input Station Parameters (2.2.4)	ParamType-ISBIAS, a0-2m	30 minutes	2 stations, no overlap	SPV
High pseudorange noise in	Additional Noise (2.2.1)	ObsType-pseudorange, -1m,	30 minutes	2 satellites, no overlap	NOISE

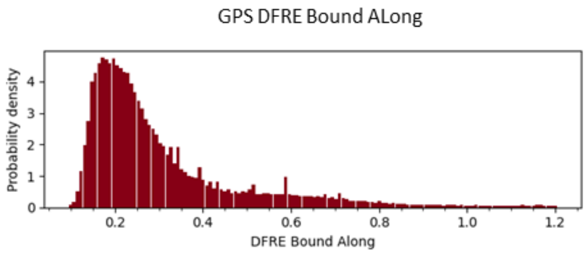
MONITORS RESULTS EXAMPLES

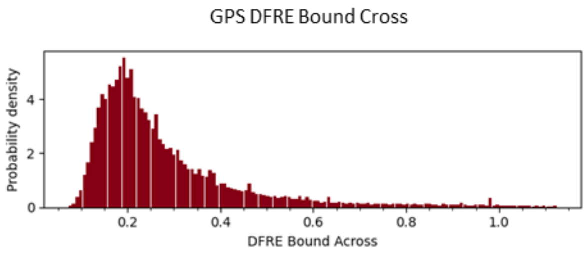
ORBIT & CLOCK MONITOR

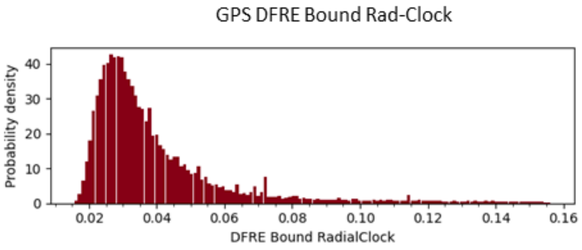
- ❑ Main goal is to detect faulty orbit & clock corrections
- ❑ Main test observable based on GNSS residuals
  - ➢ Very good sensitivity to corrections errors, as required for high-accuracy applications



- ❑ Integrity bounds computed for radial+clock, along-track and cross-track corrections
  - ➢ Bound projected to user range < 10cm



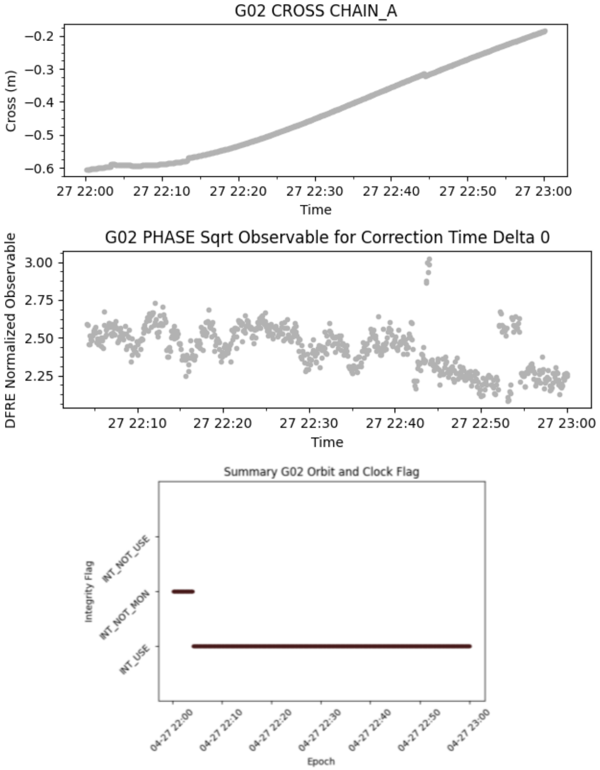




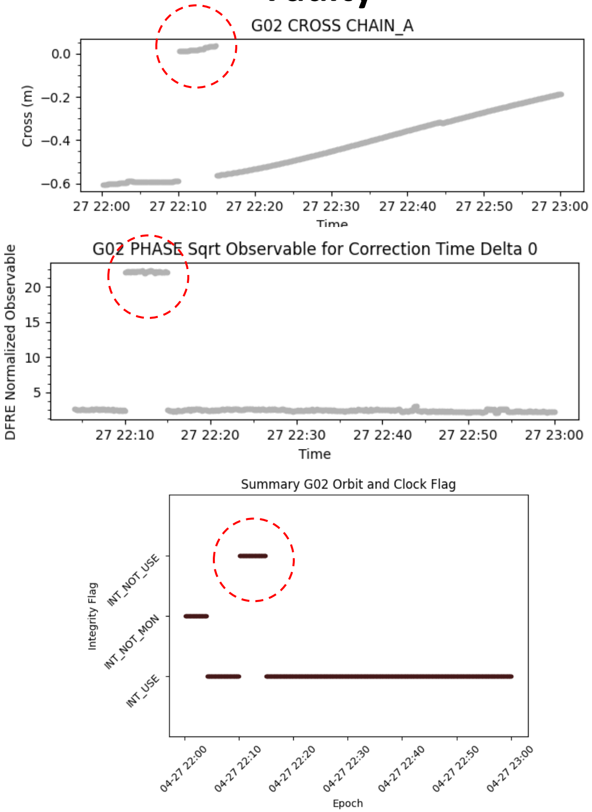
ORBIT & CLOCK MONITOR

- Example of detection in faulty corrections: Cross-track correction component offset during 5 minutes

Fault-free



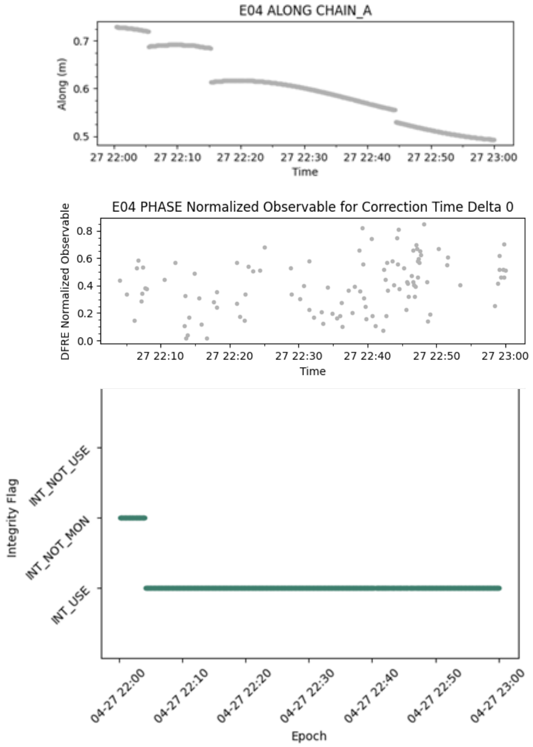
Faulty



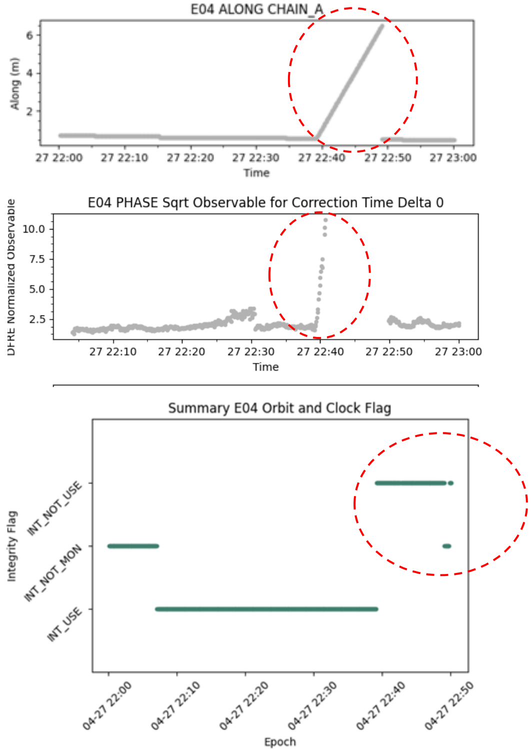
ORBIT & CLOCK MONITOR

- Example of detection in faulty corrections: Along-track ramp error during 10 minute

Fault-free



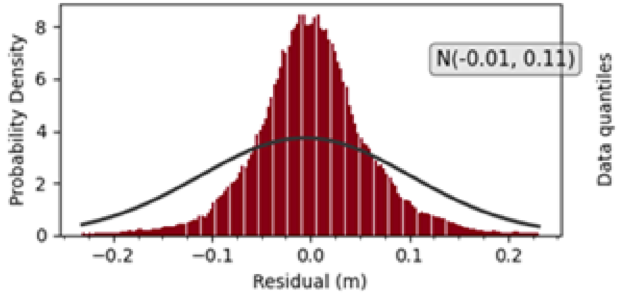
Faulty



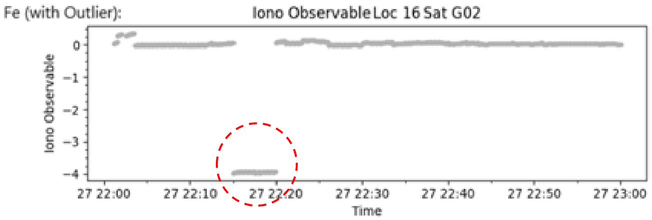
IONO MONITOR

- The goals of the IONO monitor are:
  - Detect faulty ionoispheric corrections from CP
  - Detect degraded ionospheric conditions

- Showing: Test residuals of observations from monitoring stations
  - Good sensitivity to correction errors



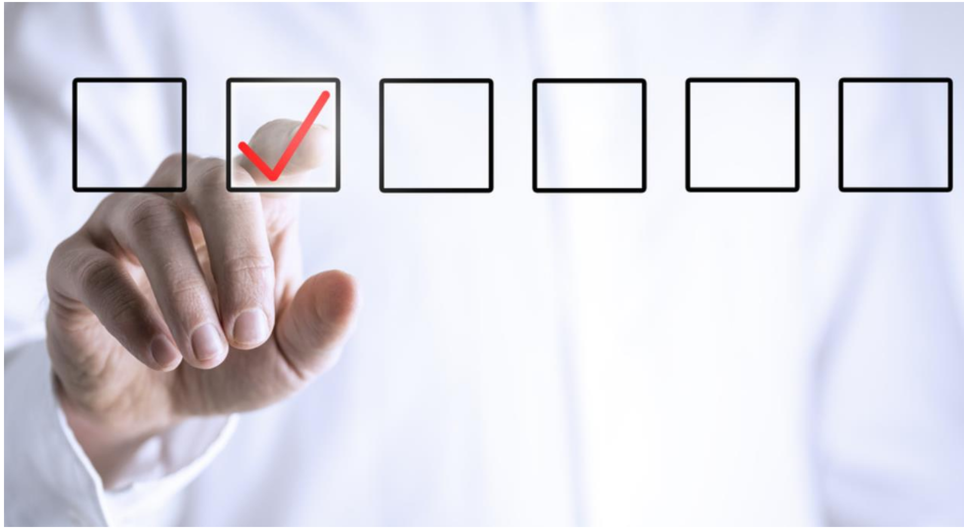
- Showing: Detection of faulty corrections with test observable



CONCLUSIONS

CONCLUSIONS

- ❑ GMV has developed a Safety Processor to assure the integrity of its Corrections Service
- ❑ Stringent development process and safety standards (ISO26262, SOTIF) followed
- ❑ Safety Processor has capability to detect errors in the required range for High-accuracy applications
- ❑ Ongoing activities:
  - ✓ More testing
  - ✓ Certification (TÜV-SÜD)



Thank you!!

INNOVATING SOLUTIONS