

magicBESAFE

Integrity Layer over PPP Corrections for
High-Accuracy Positioning Services

Final Presentation Meeting



Agenda

- Context and Rationale for the Product Development
- Outcome of the Project
- Product Competitiveness and Market Opportunities
- Q&A Session

Context and Rationale for the Product Development

Context and Rationale for the Product Development

- High precision solutions are becoming popular for ordinary positioning applications and have the potential for further development in safety-of-life and liability-critical applications.
- Several market segments have been identified regarding the need for GNSS high-accuracy and high-integrity services: autonomous vehicles, rail, maritime and agricultural applications, timing, space users.
- The development of a PPP Safety Processor providing an additional integrity layer over the PPP corrections is considered of great value for the GNSS users.
- GMV is a known PPP service provider with high experience, especially in the automotive domain.
- GMV is looking to adapt and extend the service to other markets.

*The PPP **magicBESAFE** processor is an enabling item for an **assured PPP Correction Service**. Its objective is to provide an **integrity layer** over PPP corrections generated to provide **high-accuracy positioning services**.*

User Needs

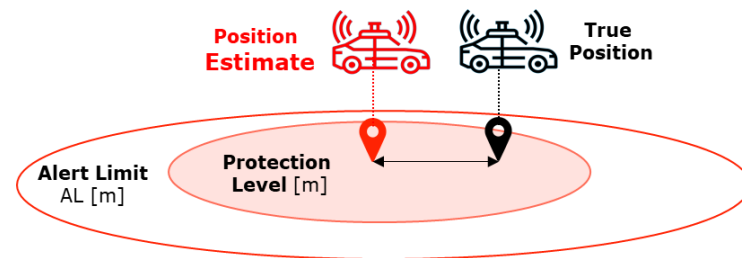
Each user applications has its own specific requirement. The common feature among the applications that motivate this project is the need for:

- High accuracy, a few cm or dm.
- High integrity of the solution, to assure a low risk that position errors lead to harmful effects at the target application.

The integrity requirements generally use the following concepts:

- **Alert Limit** for a given parameter is the error tolerance not to be exceeded without issuing an alert.
- **Protection Level (PL)** is computed by the GNSS algorithm and provides a bound on the solution error that shall not be exceeded beyond a small probability called Target Integrity Risk (TIR).

We focus on the road sector, especially **on autonomous driving**, as it is the main driver in the development of high-accuracy safe GNSS positioning and has quite demanding requirements.



Road Applications

The GNSS system must comply with automotive safety standards and application-specific KPIs.

- Safety standards:
 - ISO 26262 (Functional Safety): Avoid systematic or random failures in HW/SW.
 - ISO 21448 (SOTIF): Control performance insufficiencies and effects caused by environmental conditions. Integrity.
 - ISO/SAE 21434: Automotive Standard Security.

For road applications, we can show a representative set of magnitudes for the user requirements:

- Position accuracy (~ 20 cm).
- Convergence Time (< 30 s).
- Availability ($> 99,9\%$).
- Integrity risk ($\sim 1e-7/h$).
- Time to Alert (< 1 s).
- Alert Limit (~ 2 m).



ISO 26262

In-car
Functional
Safety



ISO/PAS 21448

Safety of the
Intended
Functionality
SOTIF



ISO/SAE 21434

Cybersecurity
and Security
Measures



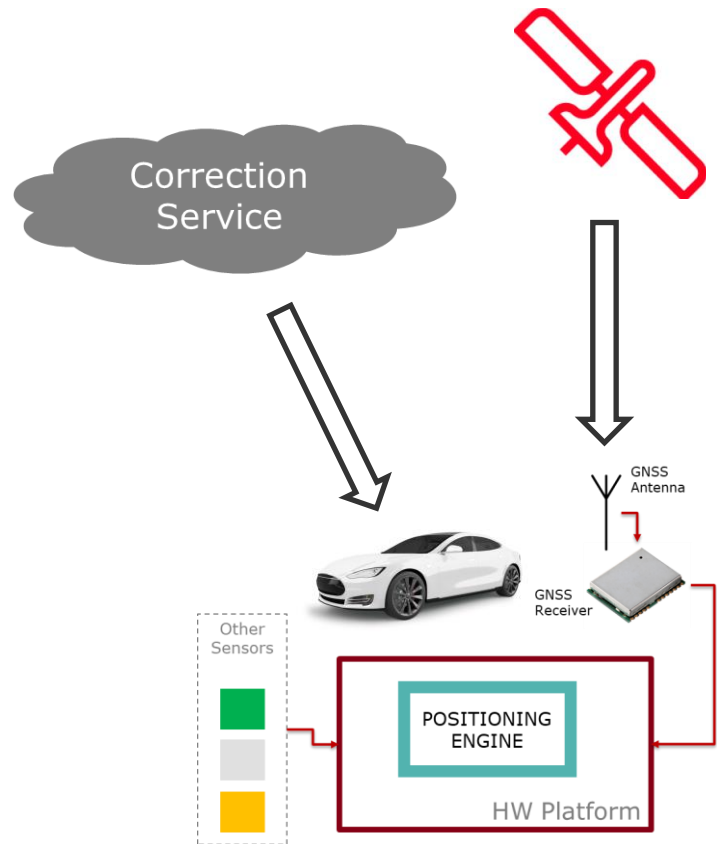
GNSS System Architecture

A typical high-accuracy GNSS positioning system consists of:

- Positioning Engine, which computes the solution from GNSS receiver other sensors data.
- HW Platform, GNSS antenna and receiver.
- Corrections Service, delivering high-accuracy corrections.

Orbit & clock corrections complement navigation messages to get very accurate positions and clock biases of the satellites. Other corrections (ionospheric, phase biases) allow fast convergence of the solution.

The accuracy and safety of the GNSS position depends on each of these elements reaching the required level of performance and integrity.



Corrections Service Integrity

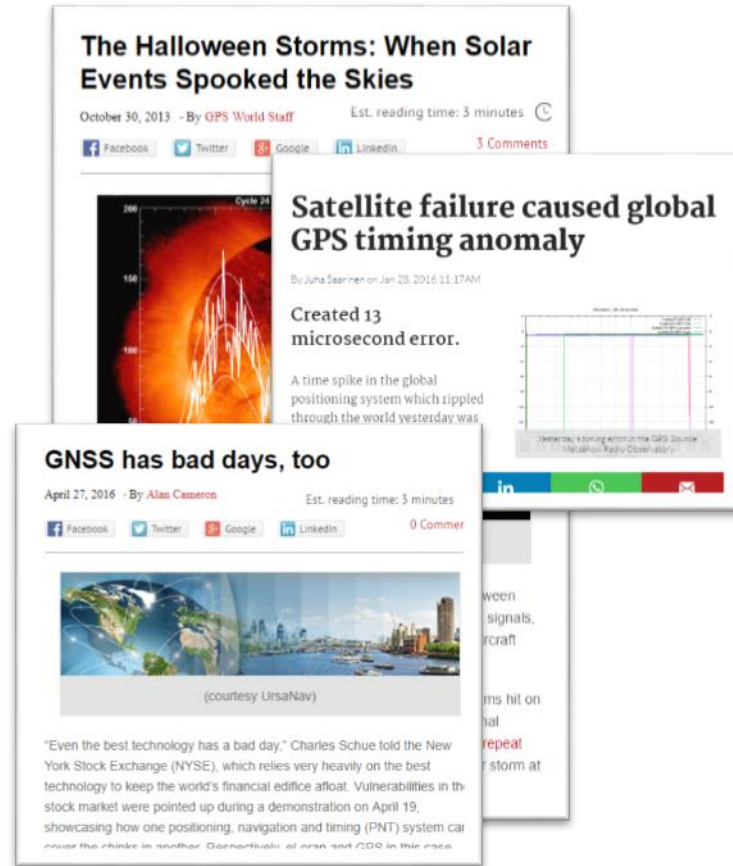
There are some hazards / failure modes that should be better mitigated by the Corrections Service:

- Failure modes affecting the computation of the corrections.
- GNSS satellite or constellation failures.
- Degraded ionospheric conditions (e.g. ionospheric storms).

The Corrections Service shall guarantee that these failures do not jeopardize the safety of the user application.

- It sends integrity flags to users within the corrections message, to indicate which data can be safely used.
- It contributes to Protection Level computation at the Positioning Engine through integrity bounds.
- It detects satellite and ionospheric adverse events.

The safety requirements applicable to the Corrections Service are derived from the safety case of the complete GNSS system.



Comparison with SBAS Systems

- Integrity of GNSS positioning is a concept initially developed by the civil aviation community and successfully applied for their purposes.
- Specific technologies (such as SBAS, GBAS or RAIM) were developed which enabled safety-critical aircraft operations.
- Many of them are useful to develop a safe high-accuracy GNSS system (e.g., Protection Levels).
- However:
 - Above technologies designed for a very specific type of environment, clean of obstacles and interferences.
 - Accuracy and size of PLs is at least one order of magnitude bigger than needed in high-accuracy applications.
 - They don't consider the application of carrier-phase and IAR techniques.

High-accuracy and safe GNSS systems require **new developments**.

ICAO Annex 10 - SBAS

Typical operation	Horizontal alert limit	Vertical alert limit
En-route (oceanic/continental low density)	7.4 km (4 NM)	N/A
En-route (continental)	3.7 km (2 NM)	N/A
En-route, Terminal	1.85 km (1 NM)	N/A
NPA	556 m (0.3 NM)	N/A
APV-I	40 m (130 ft)	50 m (164 ft)
APV- II	40.0 m (130 ft)	20.0 m (66 ft)
Category I precision approach	40.0 m (130 ft)	15.0 m to 10.0 m (50 ft to 33 ft)

Outcome of the Project

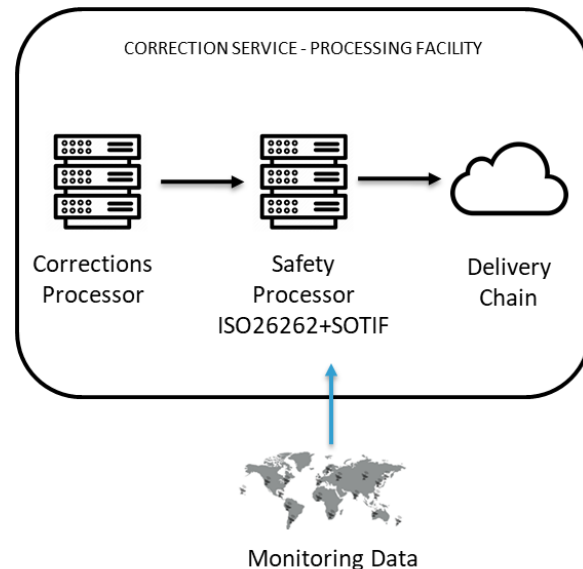
Corrections Service Architecture

Our Corrections Service safety approach is “correct then monitor”:

- The Corrections Processor computes corrections but does not assure its integrity.
- The Safety Processor checks the corrections generated by the Corrections Processor and computes the integrity data to be included in the broadcast message.

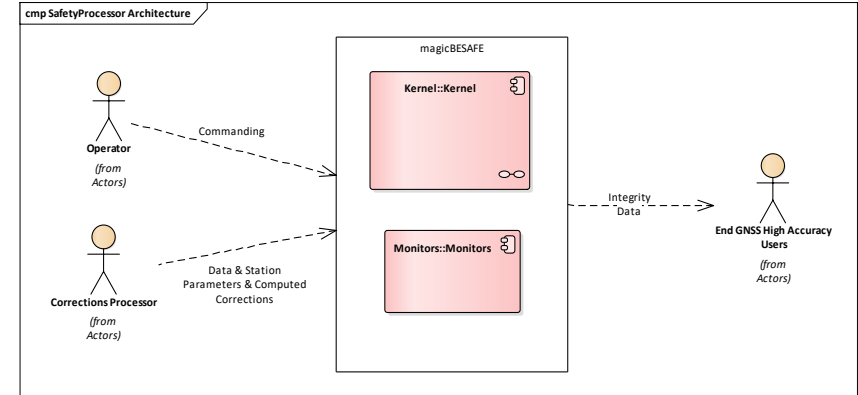
The Safety Processor follows automotive safety development standards (ISO 26262, ISO 21448).

The goal of the **magicBESAFE** project is to develop a **Safety Processor** that fulfils the defined integrity requirements.



Safety Processor Architecture

- The Safety Processor is a **safety-critical real time** SW.
- Two main SW components:
 - The **Kernel** implements the core part: threads, scheduling, data acquisition and message provision. It manages the Safety Processor nominal cycle.
 - The **Monitors** part implements monitors to check each correction type and compute the integrity bounds. They are designed to detect feared events identified in the safety analysis.
- Safety Processor (SP) inputs:
 - SP receives commands from the operators.
 - SP receives the corrections message generated by Corrections Processor.
 - SP processes GNSS data from a network of sensor stations, independent of corrections generation.
- The Safety Processor outputs consist of:
 - Integrity data.
 - Monitoring dashboards.

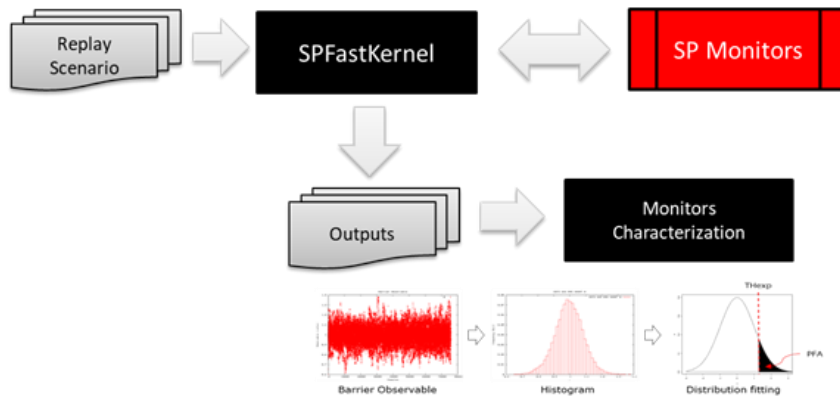


Safety Processor Development

- GMV has developed a Safety Processor that runs in real-time.
- The design, development and validation has followed a rigorous safety process to guarantee the integrity of the corrections message.
- In parallel, GMV has developed a validation platform consisting of the following elements:
 - **SPFastKernel** to run the Safety Processor in replay mode (offline) from recordings of real-time executions.
 - **Monitor Characterization Tool** to analyze and validate the observables used by the monitors.
 - **Feared Event Generation Tool** to introduce Feared Events into existing recordings to test the detection capability of the monitors.

Safety Processor Validation

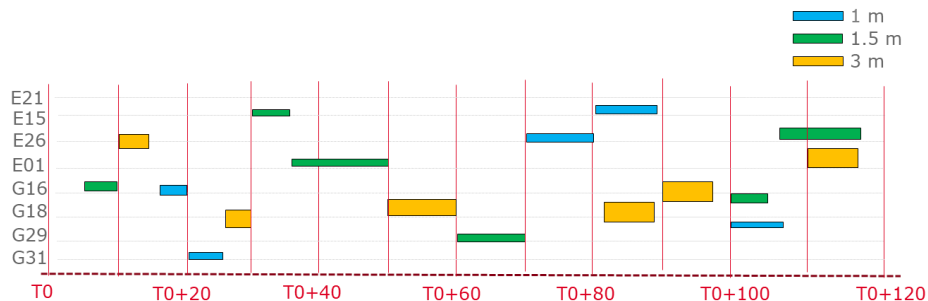
- Safety Processor validation based on:
 - Fault-free scenarios (real data) to characterize monitor observables and set thresholds.
 - Simulated faulty-scenarios to test detection of failure modes.
 - Analytical argumentation.
- Fault-free validation:
 - Based on real GNSS data.
 - Replay tool (**SPFastKernel**) used to process recorded scenarios.
 - **Monitor Characterization Tool** used to tune the monitors and check the test observables.
 - Comply both with integrity and availability requirements.



Safety Processor Validation

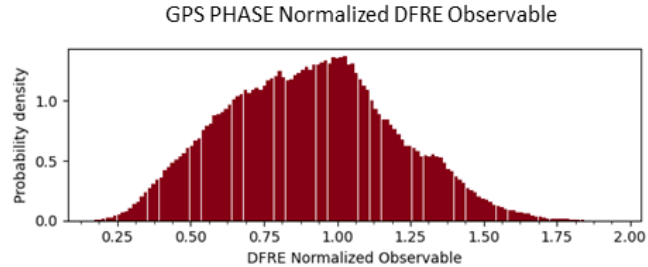
Faulty scenarios validation:

- **FE Generation Tool** has the capability to introduce failure modes (Feared Events):
 - Large errors in orbit & clock, ionospheric, phase bias corrections.
 - Ionospheric storms.
 - Satellite failures.
 - Corrupted monitoring data.
- Run the **SPFastKernel** to check that the Feared Events are detected and mitigated.

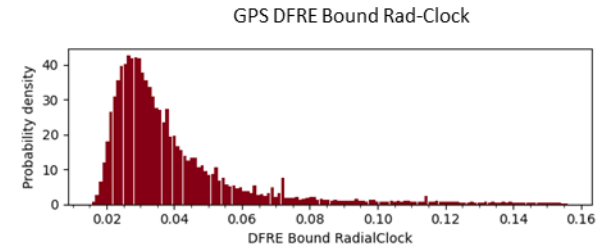
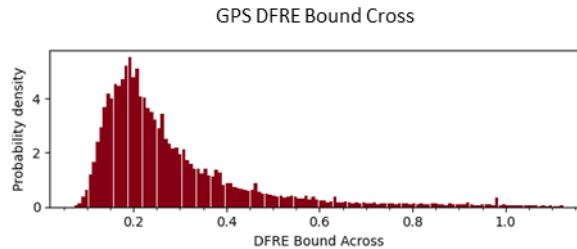
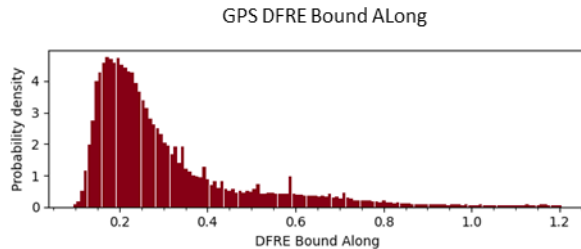


Orbit & Clock Monitor

- Main goal: detect faulty orbit & clock corrections.
- Main test observable based on GNSS residuals:

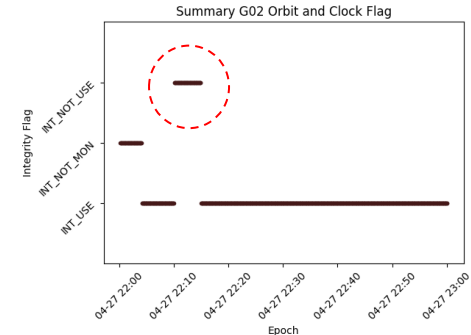
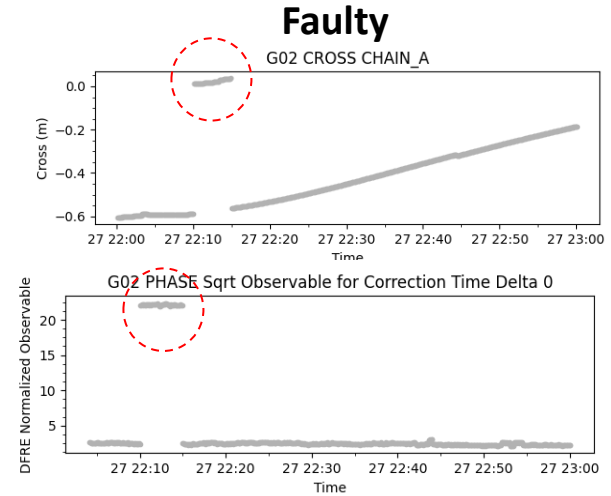
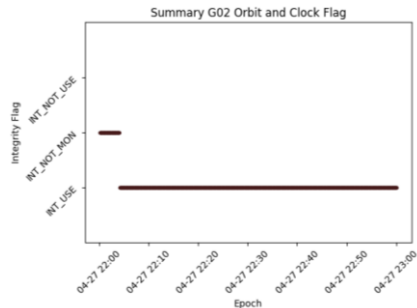
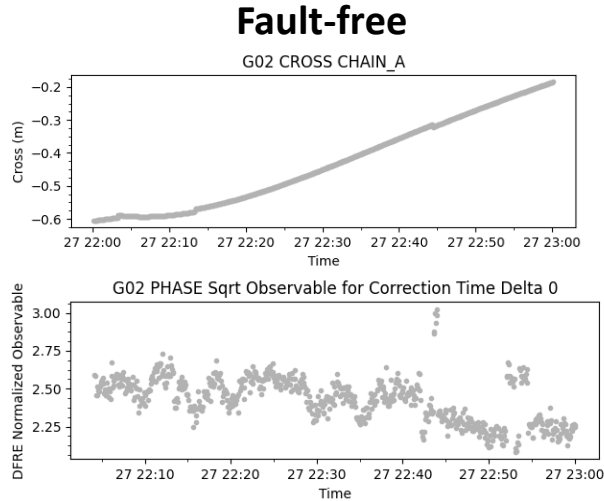


- Integrity bounds computed for radial+clock, along-track and cross-track corrections:
 - Bound projected to user range <10 cm.



Orbit & Clock Monitor

- Example of detection in faulty corrections: cross-track correction component offset for 5 minutes.

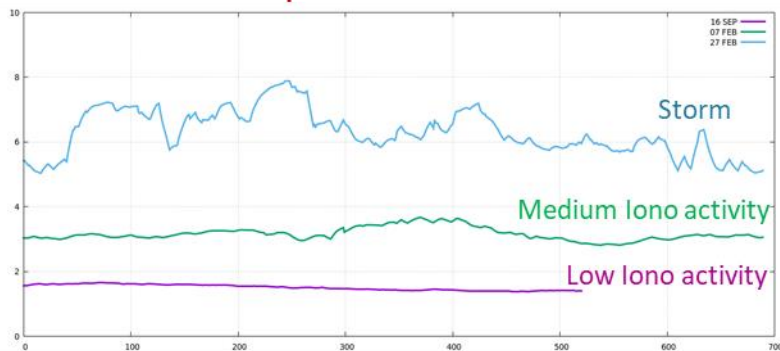


Ionospheric Storms Detection

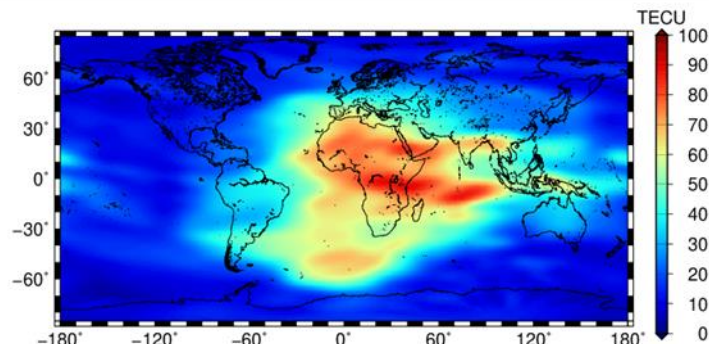
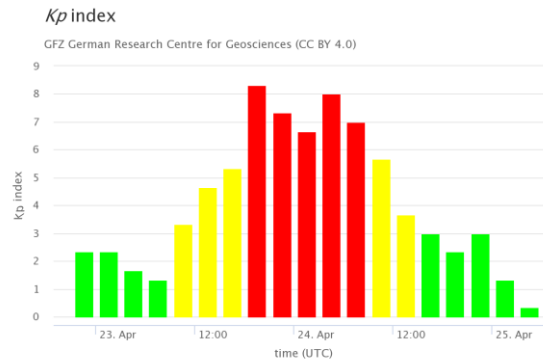
The activity of the ionosphere is very high in certain days (ionospheric storms):

- The ionospheric corrections performance may degrade and be a risk for the positioning solution integrity.
- Safety Processor computes a storm indicator to detect these degraded conditions.
- The storm indicator successfully signals the occurrence of high ionospheric activity, as checked with real data scenarios.

Ionospheric storm indicator



Kp index calculated by GFZ



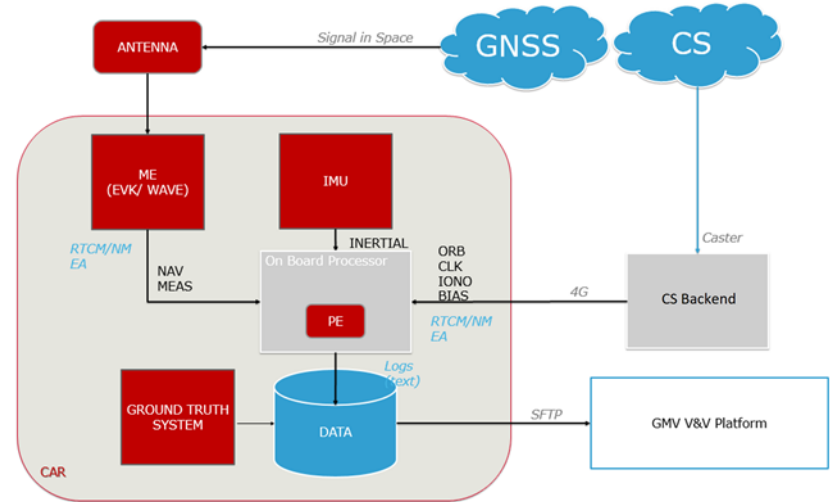
User Test Case

An end-to-end test case has been performed during the final stage of the project.

Two different scenario have been run:

- Highway.
- Semi-urban.

The accuracy and availability of the solution are not significantly affected using the integrity data.

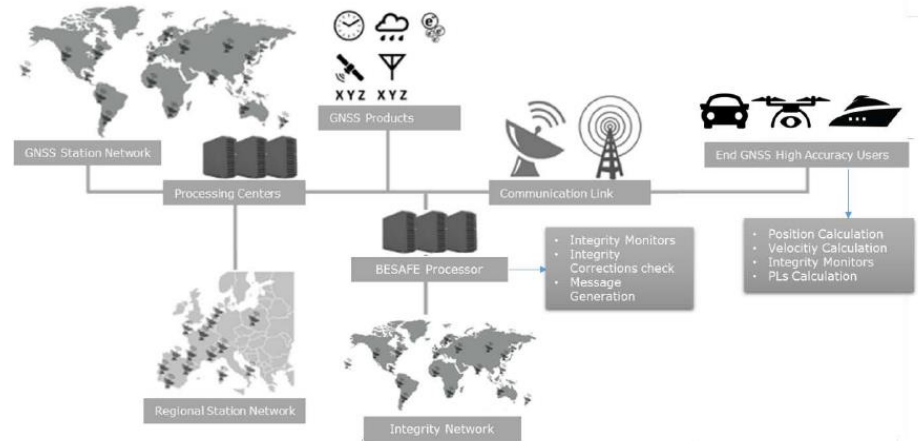


Product Competitiveness and Market Opportunities

Product Competitiveness

*The developed PPP **magicBESAFE** Safety Processor is implemented within the GMV **GSharp**® PPP Corrections Service (CS) and the output information will be usable by a Positioning Engine (PE) to ensure compliance to safety requirements of the target application.*

- The whole GMV *GSharp*® service including magicBESAFE provides a full end-to-end solution for safe high-accuracy GNSS positioning.
- magicBESAFE is a key piece to assure the integrity of the GNSS system.



Market Opportunities

- Market segments with needs for GNSS high-accuracy and high-integrity services:
 - **Autonomous Vehicles.** The automotive industry is strongly interested in Precise Point Positioning techniques providing high-accuracy performances that can be combined with other positioning technologies such as inertial sensor units (IMUs), cameras, etc. Additionally, we can deliver a certain level of integrity for applications such as assisted or autonomous driving. GMV is currently the provider of high-accuracy PPP for **BMW** automated driving vehicles.
 - **Rail.** Several studies have pointed out the convenience to implement specific GNSS integrity solutions for success in train control applications.
 - **Maritime.** Applications such as vessel navigation, fishing vessel control, docking maneuvers, inland navigation and marine engineering could benefit from the integrity technology developments.
 - **Agriculture.** Applications employed in agriculture are moving from partially automated solutions to fully automated ones. In order to apply these solutions in a safe and reliable way, a positioning integrity protection is highly desired by the stakeholders.
 - **Timing.** Segment markets of precise GNSS timing such as critical infrastructures, telecom (5G networks) and IoT could benefit from integrity services specifically adapted to fulfil the needs of these communities.
 - **Space Users.** There is an increasing demand of GNSS services by space users for different applications such as orbit determination, remote sensing and radio occultation.
 - **Others.** Many other applications such as mapping and GIS, safety and emergency, insurance, social networking, livestock tracking and geo-traceability for agriculture, cadastral surveying, mapping, etc. could also benefit from the fact of having a certain error bounds or alarms in case of potentially excessive positioning error.

Conclusions and future work

CONCLUSIONS

- The magicBESAFE Safety Processor ensures that the corrections are safe while keeping the availability in any location of the service area.
- The magicBESAFE monitors have been successfully tested over fault-free and faulty scenarios.
- The safety validation process has shown that the integrity requirements have been achieved.
- An integration test campaign has been conducted to demonstrate the performance of magicBESAFE in a user test platform, on urban and semi-urban scenarios.

FUTURE DEVELOPMENTS

- Provide support to multi-frequency users, processing more than two frequencies.
- Process additional GNSS constellations to increase the solution availability and expand service areas.
- Analyze and validate the usage of magicBESAFE for other industry sector applications.

Working with ESA

- The development of magicBESAFE was possible thanks to the support provided by ESA and the NAVISP Element 2 program.
- ESA has provided valuable technical review, guidance and expertise at all stages of the project.
- magicBESAFE gains increased visibility through the ESA NAVISP mechanisms.
- ESA showed understanding with respect to delays that appeared in the project and trusted the company's capability to complete the technical challenges that arose in the project.

GMV would like to thank ESA and the NAVISP team for the ongoing support to magicBESAFE.

Q&A Session

Thank you!

Pedro F. Navarro – pfnavarro@gmv.com

Jaume Grabulosa – jaume.grabulosa@gmv.com

