GNSS / GALILEO certification for rail safety applications Railway requirements and the strategic position of UIC

Presenting: George BARBU
International Railway Union – UIC – Paris, France

Abstract

All railway safety related standards completed with the regulations of the national safety authorities explicitly require the certification of each intended application with safety relevance. The certification includes the proof of evidence that all safety related aspects are controlled and dependability is assured over the whole application’s life cycle. The certification of safety when train’s position, speed and timing (PVT) are determined by the global satellite system needs to include the global satellite system like an application constituent. There is an obvious difficulty – even not impossible – to exercise the certification of the satellite system each time when an intended application is certified. The European satellite systems EGNOS and GALILEO are in the phase of certification, starting with the Signal in Space (SIS) and applying step by step the whole ground and space subsystems that together realise the systems’ performances and services. The GNSS Supervisory Authority (GSA) of the European Commission has the mission to assure the verification and the certification of the satellite systems. In collaboration with the GSA, European Space Agency (ESA) and with the stakeholders of the other major users communities (Aviation, Water Transport and Road Transport), the UIC has elaborated the common strategy to certify the satellite system within “ONE STOP” process, valid for all users and applicable within the common procedures of intended applications’ certification, according to the currently existing standards. The EGNOS / GALILEO certification process includes for the rail a range of research and technical actions:

- Assessment of the key system’s performances relevant to safety which shall be verified and certified in link with the safety relevant services to applications (Safety Of Life and Public Regulated Services), definition of the corresponding "generic safety case"
- Research and assessment of the equivalence of railway relevant standards and the standards applied for the realisation, deployment and exploitation of the satellite systems (mainly derived from the aviation and aero-space sectors)
- Elaboration of the methodology and of specific tools for verification of the PVT performance within railway environment, in the minimum conditions of reception, defined within the GALILEO mission requirements as "rural and urban land vehicle environment"
- Participation within the GALILEO certification process (GALCERT GSA activity)
- Elaboration of conclusions with regard to certification by a specialised notified body
- Elaboration of the framework of legal relations between the railway operators and the GNSS Operating Company (GOC) capable of including the guarantee of the service and the liability for non-performance.

The paper presents the UIC strategy elaborated by the GALILEO for Rail Expert Group, approved by the UIC railways, and for which execution the Expert Group is mandated by the UIC Executive Committee. The paper shows the justification of the strategy and action lines of the Expert Group, including the currently available results of participation to the GALCERT. The presented actions and results are the decisive steps towards the full openness of the railway safety applications to the GNSS / GALILEO technology and are characteristic not only for Europe, but have the world relevance within a common understanding of safety based on global systems’ services.
Introduction

Although the GNSS signal in space is not available everywhere on a railway route, the GNSS is a powerful tool to build new transport services alone or in combination with other technologies, to increase the efficiency, competition and strengths of the railway system. The UIC “GALILEO for rail Expert group” has analysed the potential applications of the GNSS in the rail domain and has concluded that the safety related applications are among the most impacting and promising. The GNSS rail safety applications refer to:

- Primary safety systems, where the GNSS is involved in the direct safety chain of rail operations, i.e. is directly responsible of providing safe data (such as position, speed, time) to the vital systems and devices. As non-exhaustive examples, these can encompass the train control, train integrity and train spacing (traffic control) systems of the railways.

- Overlaid safety systems, where the GNSS provides information to "advisory" or safety back-up systems. Non-exhaustive examples are the driving (intelligent assistance), diagnosis and location of defaults in track and simplified signalling (back-up) systems capable of providing safety superior to human in simplified – low intensity - operation conditions or enhancing the human safety performance in case of failure of the primary safety systems.

The standards and regulations relevant to safety of railways explicitly require that each intended application of the categories listed above shall be validated and certified.

The UIC roadmap for GNSS applications to rail has also established a workable strategy in order to mitigate the threats and weaknesses of the new technology and to synchronise the readiness of GALILEO with the readiness of the railways to accept implementing operational applications into the railway system. The validation and certification of GALILEO as a global system should enable its use as a constituent of rail intended applications and hence, the full enforcement of the existing standards and regulations applicable for the validation and certification of every railway intended application. Because GALILEO was not designed and realised under prescriptions of the railway standards, the certification of the global system should be based on the GALILEO specifications and standards. The provision of the evidence that the system complies with the specifications should be followed by the full understanding and endorsement of the GALILEO intrinsic safety principles and synergic cooperation of its large scale components to build the prescribed performance and enabling the safety operation. The railways should be also aware of the residual risks, of the system’s safety operation and of the applicable measures to manage these risks.

The system certification should be common with the aviation and maritime transports, because GALILEO is an infrastructure common for all. This “one-stop” process would realise important savings of time and resources and would be the (only) realistic opportunity to include the operational and risk mitigation requirements in the final system’s use. The strategy envisages the proof of evidence of the capacity of GALILEO to comply with the specified level of performance (especially the case of the Safety Of Life service) when the railway user has access to the output interface of the standard GALILEO (SOL) receiver in the “rural and urban mobile vehicle environment”.

In the GALILEO specification documents, the SOL receiver applicable and capable of integration in the rail applications is the “rural and urban vehicle receiver” that performs within the minimum conditions of reception, in the railway environment and could additionally include specific requirements for optimally managing transitions between the visibility and non-visibility zones of the sky.

The set up of a workable and efficient certification for rail of the GNSS (GALILEO) signal in space is the first step to open the way to promising and efficient use of a new, global technology in safety related applications. Irrespective of continents and regions, the essential rules for railway safety are similar, because they have the origin in the rail system essence, in the rail-guided movement of vehicles. Therefore we consider that the application of this strategy is of major importance for the whole railway world.
The most impacting GNSS applications are the railway safety related applications. Certification of GALILEO for rail is a must

The research carried out by the railway experts in the UIC work group for GALILEO applications to rail, who acted as an expert panel, has assessed the operational impact, the costs, the benefits and profitability of applications. Safety overlaid systems and the primary safety applications are the highest ranked from a benefit and profitability point of view. The perception of the experts' panel that justifies such a high ranking relies on the opportunities of the GNSS technology to provide highly functional, modular and adaptive tools capable of satisfying a range of requirements for which other technologies can not offer solutions or can satisfy them in more restrictive conditions. Especially targeted are simplified operational systems for local lines, signalling of level crossings, systems for driving assistance that make drivers' training easier and less expensive and improve the human performance, back-up systems for operation when primary safety systems are in failure. There is also a positive highly ranked perception of experts for applications capable of satisfying the absolute positioning and odometry for train control with enhanced interoperability, cost reduction and simplification of the track-side equipment.

Figure 1: Benefits and profitability scores for application classes of GNSS / GALILEO

The role of GALILEO Signal in Space and the receiver integration in safety schemes for rail

In Europe, the major role of the continuous railway service with controlled RAMS, imposes the existence and use of GALILEO Safety of Life service (the Public Regulated Service is also preferred) to build safety related applications. Even if the EGNOS Ground Integrity Channel applied to GPS could be a start point for building applications demanding more safety integrity (eventually compatible with high Safety Integrity Level 4 in a railway application), the non guaranteed service continuity of GPS remains a major concern. The safety related applications could use GPS+EGNOS as an overlay location system, but not as a primary safety system. Obviously, the role of GALILEO is essential for building safety related applications for the European railways.
The reinforcement of flexible use of the GALILEO as a constituent in applications shall dissociate the receiver from the “aiding sensors” (such as the inertial sensors or other elements that are complementing for coverage, more integrity, more functionality). These belong to the application and they are determined by and are tailored to the application requirements.

The following figure illustrates this conception:

In response to these considerations the UIC has initiated a series of actions aiming at reducing the costs of design and manufacturing of specific equipment resulting from adaptive and flexible integration within rail applications of receivers designed on a core common basis for aviation, rail and maritime transports. The application that uses the information provided by the receiver shall evaluate the information within the constraints dictated by the application intended functionality and environment.

The basic condition to transform this conception in an actually working process is the capability of demonstrating:

1. The ability of the GALILEO SOL receiver to be integrated in scalable and versatile architectures corresponding to specific functional conditions of the intended applications. The rail SOL receiver should be defined for the SOL performance in the generic functional environment

2. The capability of application architectures that use the SOL receiver to reach the application’s required SIL. In some applications, the safety integrity requirements for train positioning and speed calculation exceed the integrity

Figure 2: role of GALILEO in the GNSS constellation

Figure 3: Strategy of GNSS certification for rail
risk of the SOL service (currently assessed at $3.5 \times 10^{-7}/150$ s, at alarm limit of $10\sigma$ and time to alarm of 6 seconds).

Certification principles and strategy resulting from integration requirements in applications

The validation and certification based on demonstration of conformity should consider that safety applications can be realized, integrating the GALILEO SOL receiver which receives the SIS from visible satellites and delivers the information on position, speed and integrity risk defined by the SOL service. The receiver can deliver this information only in the minimum condition of reception. With other words, it should be demonstrated that affordable and workable architectures are feasible, to serve the application’s conditions starting from the certifiable performance of the satellite system and its constituents in application, i.e. the signal in space, the receiver and the provision of the navigation service to the users.

More UIC, national and European Commission sponsored projects have demonstrated until now, when using the combination of GPS and EGNOS as a pre-requisite scenario approaching the new GALILEO system, that the satellite receiver:

- Can satisfy the accuracy requirements of the most demanding applications of railway safety (in train control functions) when it has the visibility of minimum 4 satellites and a favourable geometric configuration of them;
- Can be integrated in complex architectures, in combination with inertial sensors to assure the coverage on zones with difficult reception of the satellite signals. The quality of the sensors and the “policy” of integration (the KALMAN filter algorithms) should be concretely adapted to the application requirements;
- The application dedicated architectures can also implement techniques capable of decreasing the integrity risk of the position information at values acceptable by the application Safety Integrity Level.

Even this last feature of the integrating architectures needs more clarification with regards to the capability of applying the safety principles of the railway to build structures with controllable safety integrity, starting from components with worse integrity risk. This should also show the clear capability of such integrating structures to demonstrate the safety dependability using the railway standards. It would then be clearly demonstrated that systems and components validated by means of other safety principles are capable of integration in railway applications and can demonstrate dependability when applying the railway safety principles.

This clarification is also necessary to demonstrate that the core requirements of the SOL receiver usable for rail can be similar with those of aviation or maritime applications. This should consolidate the common share of the basic technology, the components and software basis, in the interest of cost, quality, migration, market size and technologic excellence.

This would also consolidate the opportunity to implement the “one stop” validation of the GALILEO SOL service, common for aviation, rail and maritime and to validate a “core” SOL receiver common for them.

The satisfaction of accuracy requirements of $2\sigma = 4-6$ meters at 95% confidence when the receiver has at least 4 satellites in direct view is in general a non-contested performance of the GNSS receiver and it is expected that the SOL receiver will have even better performance.

Therefore the driving requirements to determine the architectures of integrating the SOL receiver are: **The capacity of integration schemes to decrease the integrity risk**, especially there, where the application’s integrity risk requirements are more exigent than the integrity risk of the SOL service; Two cases should be identified:

1. The application’s integrity risk is not less than the SOL integrity risk. In this case the SOL receiver can alone satisfy the integrity risk requirements of the application
2. Integrity risk of the application is less than the integrity risk of the SOL. In this case the SOL receiver can not satisfy alone the integrity risk requirements of the application. Techniques for improving the safety integrity of the position information should be applied in the application’s integrating architecture
The satisfaction of coverage requirements

Two cases have to be considered:

1. The application is tolerant to partial coverage, i.e. the position could be requested only on zones where the open sky visibility is available. In this case the SOL receiver alone can deliver the position information and, depending on the integrity risk accepted for the information, safety qualifier can be added if the application’s IR is less than SOLIR.

2. The application requires coverage for zones with difficult reception of the satellite signals. In this case the SOL receiver should be integrated in architectures that complement the navigation with inertial sensors or with other techniques to enable positioning in such “grey” or “dark” zones. Depending on the application’s integrity requirements, the integration architectures should apply for improving the application’s SIL.

The figure illustrates the results of this analysis. The GNSS / GALILEO signal in space and the GNSS / GALILEO receiver capable of delivering to application the position and speed information with the guaranteed GALILEO safety integrity level can be integrated in schemes that are tailored to the individual application requirements such as to satisfy the intended requirements for coverage and safety integrity.

Figure 4: Integration of GNSS receiver in applications

Based on the results of the research carried out, the UIC strategy for certification of GNSS / GALILEO consists of the following three consecutive layers:

1. The certification of the signal in space (SIS) – certification of the GALILEO system involved in broadcasting the Signal In Space with the performance and at the technical characteristics defined in the Mission Requirements Documentation.

2. The certification of the GALILEO reference receiver (software receiver) - applicable in the rural and urban vehicle environment to obtain, at the application level, the tangible information of position, speed and timing, with the performance defined in the MRD and with the safety integrity defined for the Safety of Life (eventually Public Regulated Service). The integrity risk computed by the receiver shall correspond to the integrity conception of GALILEO and shall implement the corresponding reference algorithms.

3. The definition of the legally applicable conditions which should be established between the GALILEO Operating Company (GOC) or GNSS Navigation Service and the railway operators - eventually represented by the UIC - in order to fix the conditions of guarantees and liabilities for the GALILEO Safety of Life performance.

Enforcement of the GNSS / GALILEO certification for rail

The UIC executive committee has mandated the UIC GALILEO Expert Group to identify and carry out the actions aiming at enforcing the established strategy. The GALCERT initiative of the EU GNSS Supervisory Authority provided to be the first step where the railways and the other users’ communities could collaborate in order to elaborate and set up a workable system for validation and certification of the GNSS / GALILEO. The following figure illustrates the GALCERT proposed process:
The certification of the Signal in Space in a "one stop" process common for aviation, railway, maritime and other users of safety of life service fully corresponds to the railway strategy. The certification is based on the proof of evidence and conformity demonstration of the GALILEO performance specified by the Mission Requirements Documents.

The GALCERT certification process enforces also the legal framework applicable for each major user community, i.e. the existing relevant standards and regulations, in comparison with the standards and regulations used for design, deployment and verification of the GALILEO system.

In case of the GALILEO certification for rail, the base has been provided by the railway safety standards in Europe (CENELEC) + the EC Safety Directive for rail. They are representative for all safety related applications. The requirements eventually derived from individual applications shall not be relevant in this phase. They may limit the application areas. The railway users shall have the freedom of using the GALILEO system with its best performances in fields which have not yet been explored. This is also a conclusion to extend the certification validity outside of Europe.

For the railway domain only few requirements remain uncovered by the European Space Agency In Orbit Validation (IOV) development standards and the ECSS documents. The comparison of the standards showed that the structure of the documents is very different. The structure of the CENELEC standards follows the system life-cycle, while the ECSS documents allocate each chapter to a certain topic within the life-cycle of space projects.

As a consequence, the position of the UIC, expressed by the GALILEO Expert Group concludes that:

- No representative safety case encompassing all rail applications will be defined for the SIS certification for rail. The analysis of safety integrity requirements of railway applications show that the GALILEO SoL integrity is not sufficient for all high safety demanding applications. The achievement of safety targets in such cases applies the GNSS SoL integrity at its performance.
defined by the MRD within fail-safe architectures which shall be built according to the railway standards. Some other application classes can be directly covered by the GALILEO SoL safety integrity. It is impossible to describe a limited number of representative safety cases to cover all situations within their large diversity of sky visibility conditions from a train route when the running train encounters random successions of zones with full, poor or no sky visibility. Therefore the SIS certification for rail shall focus on the MRD specified performance of the SoL service (eventually PRS) in those situations when the minimum conditions of reception are fulfilled. This is a common base for all applications.

- The applicability of the European rail standard for certification of safety critical software is not fitting into the GALILEO standards for software approach (derived from the aviation standards). Nevertheless the aim of rail and GALILEO standards coincide, i.e. the certification procedure shall prove that systematic errors of the safety critical software are controlled and maintained under the specified limit. The rail community may accept the end result of the GALILEO software assurance procedures, subject these will demonstrate the achievement of dependability and controllability of software systematic errors. Other differences between the rail and aviation standards can be explained by the different safety conception and safety design philosophy. The rail system accepts an immediate safe state (the immediate stop of the train) to be reached once a first wrong side failure is detected. In the situation of a failure, the aircraft shall be able to continue flying and land on the nearest airport (safe state of the aircraft). Therefore the structure of the safety standards is different. But the scope is the same: the achievement of the safe state. The railways understand to encompass the formal differences of the standards such a way as to reach the final purpose. i.e. the demonstration of the dependability with the applicable verification and validation GALILEO standard specific procedures.

**Final remarks, next actions – transparency and world wide applicability of the certification results**

Besides the Signal In Space certification, which is currently ongoing, the next important activity is the analysis and evaluation of the GALILEO conception of safety integrity and the contribution of the GALILEO components to the integrity. One of the characteristics of satellite navigation is that user positioning accuracy always depends on several factors such as the system performance, the receiver’s ranging accuracy and the individual observation conditions, including the ranging geometry. Consequently a meaningful confidence interval for the position error can only be computed by the user receiver itself, based on some data provided by the system. The system integrity function sends integrity information to the user receivers. The integrity information consists of:

- The accuracy of the Signal In Space broadcast by satellites in view (SISA)
- The accuracy of the monitoring by the Ground Segment of the SIS broadcast by the satellites (SISMA)
- The information which SIS broadcast by satellites shall not be used (integrity flag and integrity flag threshold)

From this information the user receiver can derive the integrity risk for the individual position solution. This integrity risk is always calculated for a given Alert Limit. Currently, the Alert Limits on horizontal and vertical position accuracies are dimensioned from aviation requirements. The railway user shall fully evaluate the consequences of this conception within the design of the safety related architectures and enforce the verification, validation and certification of the applicable reference algorithms and the application software in the receivers.

The world rail community represented by the UIC is now carrying out the actions aiming at the certification of GALILEO for rail. Although the certification applies mainly the European norms and standards, the transparency of the certification process shall ensure the world rail community that the
basic principles of safety and GALILEO system control and operation are verified, documented and certified.

This transparency will provide the confidence and will play an important role for the acceptance of GALILEO as a constituent of rail safety systems not only in Europe but also in the other regions of the world.

The full transparency of the verification and certification procedures shall enable the rail domain specialists to take part to the representative certification actions, especially to the evaluation procedures, with the aim to acknowledge the positive results, to understand the problems encountered and the solutions proposed.

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UIC</td>
<td>International Railway Union – Union Internationale des Chemins de Fer</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>GALILEO</td>
<td>Denomination of the European civil satellite navigation system</td>
</tr>
<tr>
<td>SOL</td>
<td>Safety of life service of GALILEO</td>
</tr>
<tr>
<td>PRS</td>
<td>Public regulated service of GALILEO</td>
</tr>
<tr>
<td>EGNOS</td>
<td>European Geo-stationary Navigation Overlaid System</td>
</tr>
<tr>
<td>GPS</td>
<td>Abbreviation of the US NAVSTAR satellite navigation system</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level – corresponding to the European safety standards</td>
</tr>
<tr>
<td>IR</td>
<td>Integrity Risk</td>
</tr>
<tr>
<td>SOLIR</td>
<td>Integrity Risk of the Safety of life service of GALILEO</td>
</tr>
<tr>
<td>MRD</td>
<td>Mission Requirements Documentation of GALILEO</td>
</tr>
<tr>
<td>GOC</td>
<td>GALILEO Operating Company</td>
</tr>
<tr>
<td>GSA</td>
<td>GNSS Supervisory Authority of the European Commission</td>
</tr>
<tr>
<td>GNS</td>
<td>GALILEO Navigation Service</td>
</tr>
<tr>
<td>SISA</td>
<td>Signal in space accuracy</td>
</tr>
<tr>
<td>SISMA</td>
<td>Signal in Space Monitoring Accuracy</td>
</tr>
<tr>
<td>IOV</td>
<td>In Orbit Validation</td>
</tr>
<tr>
<td>ESA</td>
<td>European Space Agency</td>
</tr>
<tr>
<td>FOC</td>
<td>Full Operation Capability</td>
</tr>
</tbody>
</table>

References

[1] UIC Code: GALILEO applications for rail; Roadmap for applications
[2] UIC Code: GALILEO applications for rail; Economic estimates of the GALILEO applications for rail
[3] UIC Code: GALILEO applications for rail; Fusion of technologies for maximisation of effects
[5] GALCERT support to certification of GALILEO for the European GNSS Supervisory Authority – WP4000, final version