STEMS Final Presentation

ESA-NAVISP-EL1-003 System Suitability Study for Train Positioning using GNSS in the European Rail Traffic Management System
Agenda

1. STEMS Project Overview

2. WP1000 Review and Consolidation of Requirements and Assumptions for Virtual Balise Detection in ERTMS using GNSS

3. WP2000 SBAS Suitability Analysis for use in ERTMS

4. WP3000 Analysis of the Suitability of SBAS for Cross-Acceptance by Railway Safety Authorities

5. Conclusions and Future Work

6. Audience Questions
STEAMS Project Overview

Project Team

- GMV NSL, TVUK, GMV-RO: GNSS expertise
- UPA: railway safety concepts
- TUV: accredited safety independent safety assessor
Objectives

- Objective 1: Review and consolidate requirements and assumptions on virtual balise detection in ERTMS using GNSS;
- Objective 2: Study the suitability of the current generation of SBAS for use in the evolution of the European Traffic Management System (ERTMS) with virtual balise detection using GNSS, confirming the feasibility of current SBAS system allocations;
- Objective 3: Assess the suitability of SBAS for cross-acceptance by railway safety authorities, to be performed by an accredited railway independent safety assessor;
- Objective 4: Propose a methodology for building a suitable safety case for SBAS for use by the railway community in the ERTMS virtual balise application.

STEMS Project Overview
STEMS Project Overview

Work Logic

WP0000
Management

WP1000
Review and Consolidation of Requirements and Assumptions for Virtual Balise Detection in ERTMS using GNSS

WP2000
SBAS Suitability Analysis for use in ERTMS

WP3000
Analysis of the Suitability of SBAS for Cross-Acceptance by Railway Safety Authorities

KOM
ISW
RR
T2-IKP
T2-KPR
FR
STEMS Project Overview

Deliverables

<table>
<thead>
<tr>
<th>WP</th>
<th>ID</th>
<th>Title</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP1000</td>
<td>D101</td>
<td>Technical Note on Requirements and Assumptions for Virtual Balise Detection in ERTMS using GNSS</td>
<td>V1.0</td>
</tr>
<tr>
<td>WP2000</td>
<td>D201</td>
<td>SBAS for ERTMS Suitability Analysis File</td>
<td>V1.0</td>
</tr>
<tr>
<td></td>
<td>D202</td>
<td>Version of D201 suitable for public release</td>
<td>V1.0</td>
</tr>
<tr>
<td>WP3000</td>
<td>D301</td>
<td>Suitability Assessment of SBAS for Cross-Acceptance in Rail</td>
<td>V1.0</td>
</tr>
<tr>
<td></td>
<td>D302</td>
<td>Version of D301 suitable for public release</td>
<td>V1.0</td>
</tr>
</tbody>
</table>
Baseline Assumptions

- Use of SBAS ‘as-is’:
  - Currently operational SBAS which provides augmentation of GPS L1 only
  - Includes EGNOS V2 and V3.1
  - No SBAS system-level modifications
- Consideration of SBAS provision of integrity in range-domain
- GADF (GNSS Augmentation Distribution Function):
  - System function which retrieves SBAS messages from SIS at the Trackside and distributes them to the Onboard
  - No fixed assumptions on data processing, communications system from Trackside to Onboard or latency constraints.
Baseline Assumptions

- Requirements reviewed for Virtual Balise Detection using GNSS for ERTMS (WP1000)
  - Studies involving use of GNSS in ERTMS with alternative approaches have been initiated (inputs not available at the time that WP1000 was executed).
  - The approach studied is not exclusive to VBD.
- Local effects and local feared events are assumed to be handled by the Onboard and are outside of the scope of the study.
- Track discrimination is not possible with GNSS alone in ERTMS, additional trackside support is needed.
Inputs

- ESA and GSA working paper: “Preliminary Study on the Use and Certification of EGNOS in Interoperable Railway Control-Command and Signalling Subsystems”.
- University of Pardubice technical notes and papers.
- NGTC project D7.7 Results of the Safety Analysis.
- ESA RAILSAFE project outputs.
- Industry Stakeholder Workshop
  _Held between STEMS consortium and X2RAIL-2 Work Package 3: Fail Safe Train Positioning (including Satellite Technology).
Overview of ERTMS

- EU initiative, with objective of improving safety and increasing interoperability of rail transport in Europe through a Europe-wide standard for train control and command systems, replacing existing national systems.

- Consists of two parts:
  1. European Train Control System (ETCS), an automatic train protection system providing in cab train control;
  2. GSM-R, a radio system based on GSM for voice and data communications between the train and trackside.
Overview of Virtual Balise Detection (VBD)

- ERTMS uses odometry for positioning.
- Balises are transponders mounted on the track that communicate with trains passing over them.
- Train position is defined by estimated distance from last relevant balise group to the front end of the train.
- Train position confidence interval bounds this estimated distance and is reset when a train passes over a physical balise.
- Physical balises may be replaced by virtual balises in suitable locations.
- A Virtual Balise Reader would be introduced to the Onboard, interfacing with the ETCS Kernel.
- Virtualising the balise transmission system based on GNSS will enable a reduction in trackside infrastructure CAPEX and OPEX, removing the need for almost all physical balises on suitable lines e.g. low-speed, low-density railways.
Consolidation of Virtual Balise Requirements

- Integrity targets derived using top-down approach from balise subsystem hazards.
- GNSS receiver and VBR assumed to be fault-free (processing errors considered within an integrity target allocated to Onboard)
- Integrity targets only specified for longitudinal errors (along-track)
  _Correct track guaranteed through linking information for modes with a movement authority
- SBAS integrity concept is not directly applicable:
  _Position domain.
  _Alert Limit concept not applicable (confidence interval does not have maximum tolerable magnitude).
  _ATPE > ATPL is hazardous (may lead to train confidence interval not bounding the front end of the train).
- An independent non-GNSS diagnostics function would be required to meet the top level integrity target.
# STEMS WP1000: Requirements for VBD in ERTMS

## Consolidation of Virtual Balise Requirements

<table>
<thead>
<tr>
<th>Virtual Balise Detection</th>
<th>GNSS</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity target (THR) for erroneous localisation of a Balise Group, with reception of valid telegrams</td>
<td>Integrity target (THR) for GNSS Misleading Information (ATPE &gt; ATPL and TTA &gt; x seconds)</td>
<td>0.5 $\times 10^{-9}$ / hour</td>
</tr>
<tr>
<td></td>
<td>Along-Track Protection Level (ATPL) (99.7%)</td>
<td>~ $7.5 \times 10^{-6}$ / hour</td>
</tr>
<tr>
<td></td>
<td>Along-track Alarm Limit</td>
<td>&lt; 20 meters</td>
</tr>
<tr>
<td></td>
<td>Time to alert (TTA)</td>
<td>6-10 seconds</td>
</tr>
</tbody>
</table>
Assumed SBAS Usage Concept inc. Integrity Concept for Railway

- The SBAS integrity concept for railway will be based on the provision of integrity in the range-domain, rather than the position domain. In this case there would be no commitments from SBAS in the position domain.

- $\sigma_{flt}$ and $\sigma_{UIRE}$ values (associated to UDRE and GIVE respectively) would be applied as input to railway-specific protection levels.

- The user will be able to assume that pseudoranges for satellites monitored by SBAS are fault-free from system-level feared events (i.e. those originating from the GNSS space segment and ground segment) and ionosphere feared events, up to the target level of integrity.

- The fast corrections, slow corrections and ionospheric model will be used in order to improve accuracy.
Analysis of SBAS Performance, Safety Assurance and Risk Assessment with Respect to ERTMS Application

- SBAS performance
  - Requirements currently defined in position domain in ICAO Standards and Recommended Practises (SARPS).
  - EGNOS Safety of Life (SoL) service is certified for achieving minimum levels of performance, defined in Service Definition Document (SDD)
Analysis of SBAS Performance, Safety Assurance and Risk Assessment with Respect to ERTMS Application

Risk Assessment

- Review of work carried out in NGTC, STARS and ERSAT-GGC projects.
- SUBSET-091: Max. allowable rate of ETCS Core Hazard = 2.0e-09/h
- Uniform apportionment of 0.67e-09 to Onboard functions (trusted), Trackside functions (trusted), Transmission functions (untrusted).

- Transmission functions include subsystem hazards:
  - TRANS-BALISE-1 – Incorrect balise group message received by onboard Kernel functions as consistent (Corruption)
  - TRANS-BALISE-2 – Balise group not detected by onboard Kernel functions (Deletion)
  - TRANS-BALISE-3 – Inserted balise group message received by onboard Kernel functions as consistent (Insertion / Cross talk)

- TRANS-BALISE-3: an independent GNSS diagnostic function has been proposed in previous projects to cover the gap between the target THR and the integrity risk sources not related to the train, which includes GNSS.
Analysis of SBAS Performance, Safety Assurance and Risk Assessment with Respect to ERTMS Application

• Safety Assurance
  _Six Common Safety Methods exist in the railway domain._
  
  Common Safety Method for Risk Evaluation and Assessment (CSM-RA) is relevant to the Virtual Balise concept.
  _CSM-RA covers the following activities:
  1) Risk assessment process and demonstration of compliance with the safety requirements
  2) Hazard Management
  3) Independent Assessment by CSM Assessment Body
SBAS Assumptions on the GNSS receiver

- Review of ICAO SARPS and RTCA Minimum Operational Performance Standards (MOPS) i.e. DO-229E.
- Receiver requirements that apply to the SBAS integrity concept for the railway were identified along with any issues/gaps.
  
  These requirements would form the basis of an equivalent standard for the railway which may be referred to as “railway GNSS receiver guidelines”.

STEMS WP2000: SBAS Suitability Analysis
SBAS Assumptions on the GNSS receiver

- GAP-REC-001: Message Timeout Periods
  When no valid SBAS message has been received for 4 seconds due to a probable communications link issue, all UDREI data from that SBAS satellite shall timeout.

- While being directly applicable to the GADF, this requirement also needs to be considered from the point of view of the Onboard receiver with respect to the communications link between the Trackside and Onboard. Timing out of UDREI data shall result in a loss of availability of SBAS integrity.

- Recommendation:
  
  *Communications link between the Trackside and Onboard must be robust.*
SBAS Assumptions on the GNSS receiver

- GAP-REC-002: Message Timeout Periods
  - The applicable timeout interval for UDREI terms is 12 seconds and that for fast corrections can also be this low (corresponding to the highest degradation factor).
  - This represents a potential issue for the SBAS Integrity Concept for Rail in case the total TTA for rail (SBAS TTA + ‘Train TTA’) is 12s or greater since this data would timeout before it is possible to use it.
  - The implications of this depend on the approach taken by the Onboard receiver to the management of the TTA, but in any scenario, it must be ensured that the fast corrections and UDREI applied have not timed-out.
  - Recommendation:
    
    *Communications link between the Trackside and Onboard should be selected to enable ‘Train TTA’ to be < 6 seconds, taking into account contributions of GADF and VBR processing.*
SBAS Assumptions on the GNSS receiver

- GAP-REC-003: Smoothing
  
  The requirement for carrier-smoothing of code measurements represents a challenge in the railway environment due to frequent signal obstructions and cycle slips in carrier phase measurements.

  Recommendation:

  A railway receiver smoothing filter may need to use a lower time constant with respect to that recommended in MOPS or a time-variant approach in order to be effective.

  This will be subject to advancements in carrier phase tracking in the railway environment.

  For an alternative filter to be accepted it must be compatible with existing safety commitments and must meet a minimum level of performance (error less than 0.25m within 200 seconds after initialisation) conditional on a maximum level of code-carrier divergence (0.018m/s).
SBAS Assumptions on the GNSS receiver

- GAP-REC-004: Smoothing

  The potential use of a different smoothing filter may impact on the validity of the broadcast error bounds $\sigma_{GIVE}$ and $\sigma_{UDRE}$, which are computed based on the assumption of a MOPS-compliant filter being applied by the user receiver, taking into account potential maximum bias due to divergence in the presence of the worst-case ionospheric gradient for such a filter.

  Recommendation:

  In order to ensure the validity of $\sigma_{GIVE}$ and $\sigma_{UDRE}$, the selected smoothing filter must be compatible with existing safety commitments and must meet a minimum level of performance (error less than 0.25m within 200 seconds after initialisation) conditional on a maximum level of code-carrier divergence (0.018m/s).
SBAS Assumptions on the GNSS receiver

- GAP-REC-005: Smoothing

  _The definition of TTA assumes a MOPS-compliant user receiver._

  _The use of a different smoothing filter may affect the point in time at which, given the presence of a feared event on satellite X, the pseudorange of satellite X is affected by the feared event._

  _This could affect the TTA that is actually experienced by the user._

  _This may represent a safety issue in the event that the (smoothed) pseudorange of satellite X is affected by the feared event at a moment in time that is earlier than that at which the corresponding pseudorange is affected at any SBAS reference station (thus potentially meaning that the TTA that is experienced by the user is greater than the requirement)._

  _Recommendation:_

  Analysis is required into the impact of the standardised Onboard receiver smoothing filter on the point in time at which, in the presence of a feared event on satellite X, the pseudorange of satellite X is affected.
SBAS Assumptions on the GNSS receiver

- GAP-REC-006: Satellite Selection
  - Any GPS satellite that is designated GPS UNHEALTHY shall be excluded from processing unless it is overridden by an SBAS HEALTHY designation.
  - This overriding is applicable in all events unless the GPS UNHEALTHY designation is due to failure of parity on five successive words of the navigation message.
  - The way in which this is handled depends on whether a trackside navigation message distribution function is included in the system architecture.
  - Recommendation:

    Regardless of whether a trackside navigation message distribution function is included in the system architecture, it is recommended that the Onboard receiver decodes the GPS navigation data in order to check parity and enable it to process "health" designations in accordance with DO-229E.
Time To Alert (TTA) and Management Strategies

- SBAS performance commitments based on a TTA:
  - Precision approach: TTA = 6.0s (5.2s system + 0.8s user receiver).
- ERTMS:
  - End-to-End TTA = SBAS System TTA + TTA_Rail
    = 5.2s + TTA_Rail
  - TTA_Rail = Trackside TTA + Onboard TTA
Time To Alert (TTA) and Management Strategies

- TTA must be managed by one of the following approaches:
  - A-posteriori verification
  - Coasting from last verified measurements based on one of:
    - Inertial sensors
    - Odometer
    - Carrier phase with Relative RAIM

- In case of coasting:
  - FDE must be applied to sensors or carrier phase measurements applied during propagation period.
  - Nominal errors in sensors or carrier phase measurements must be modelled to enable overbounding to the required integrity level.
Approach

- Analysis of concept of cross-acceptance of EGNOS by the railway community for application in ERTMS. This involves:
  _EGNOS SoL service (and railway-specific service based on it).
  _Certification of EGNOS Service Provider (ESP) as Air Navigation Service Provider (ANSP).
- Analysis of a methodology for building a corresponding safety case.
- Provision of feedback on a number of proposal statements made in the ESA/GSA working paper “Preliminary Study on the Use and Certification of EGNOS in Interoperable Railway Control-Command and Signalling Subsystems”.
Regulatory Railway Aspects

STEMS WP3000: Cross Acceptance Analysis

- NATIONAL SAFETY AUTHORITY
  - NSA

- INFRASTRUCTURE MANAGERS IM
- RAILWAY UNDERTAKINGS RU
- SERVICE PROVIDERS
- MANUFACTURERS

- REGULATION
  - ERA - EUROPEAN RAILWAY AGENCY
  - EC - EUROPEAN COMISSION

- HARMONISED TECHNICAL STANDARDS
  - CENELEC - EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION
  - CEN - EUROPEAN COMMITTEE FOR STANDARDIZATION
  - ETSI: European Telecommunication Standards Institute
  - IEC
  - ISO

- SAFETY & INTEROPERABILITY
  - AsBo: CSM Safety Assessor
  - ISA-CENELEC Safety Assessor
  - NoBo: NOTIFIED BODY
  - DeBo: DESIGNATED BODY
Regulatory Railway Aspects

- Review of regulatory railway aspects, including consideration of stakeholders, the railway authorisation process and conformity assessment for modified ERTMS interoperability constituents (ICs).
  
  _Modifications may be required to the Onboard and RBC ICs._

  There is also the possibility of new ICs being defined in the longer term e.g. VBR or Enhanced Onboard Localisation Equipment.

  _Such modifications are dependent on updating the mandatory specifications listed in Annex A of the Control, Command and Signalling Technical Specification for Interoperability (CCS TSI) and in the definition of a possible new IC._

  _Conformity assessment of the ICs would probably be carried out by a Notified Body (NoBo), against essential requirements included in a future TSI._
Concept of Suitability for Use

One of the options considered in ESA/GSA working paper is that an EC declaration of suitability for use be required for the EGNOS constituent (GNSS receiver), considering its use within the railway environment and the functional requirements concerned.

Analysis found that this cannot be applied as it is not required by the CCS TSI. The TSI only requires compliance with the relevant basic parameters.

‘Module’ options are defined for assessing ICs which form part of the CCS subsystem.

The procedure of suitability for use is described in the application of the module CV.

This is applicable for constituents for which validation is necessary by in-service experience.
Regulatory Frameworks

- Analysis of regulatory frameworks applicable to EGNOS in aviation and railway domains.
- Aim: to define practical interface between them.
- Included consideration of process for cross-acceptance of EGNOS in the railway domain, implications for Infrastructure Managers and required amendments to the CCS TSI.
Regulatory Frameworks

Proposal:

• Not necessary to have an agreement between the individual IMs and the EGNOS Service Provider (ESP).
• Instead, an agreement would be better made between the European Railway Agency (ERA) and the ESP.
• This proposal is supported by the new process included in the CCS TSI, where the Infrastructure Manager (IM) has the responsibility to classify their network for the Register of the Infrastructure (RINF) and for the ERTMS System Compatibility and Radio System Compatibility (ESC/RSC).
• For ESC/RSC, IM has to demonstrate interoperability technical compatibility using ESC/RSC parameters.
• IM has to notify ERA of the ESC/RSC parameters.
• With the ESC/RSC parameters from the IMs, ERA could then be responsible for defining a generic GADF (GNSS Augmentation Distribution Function) based on a common trackside configuration.
• ESC/RSC parameters may also be used by the ESP for adapting their services to the needs of the individual lines where EGNOS will be used.
Process for Safety Demonstration and Acceptance

- Service concept: a dedicated EGNOS SoL railway service would be created, based on existing EGNOS SoL service and its safety case.

- Analysis made for how to cross-accept existing EGNOS SoL service based on the Common Safety Method for Risk assessment (CSM-RA) overarching process.

  The CSM-RA establishes a common approach for specifying and demonstrating compliance with safety levels and requirements of the railway system among the Member States.

  CSM-RA makes it easier for an assessment undertaken in one EU Member State to be accepted in another with the minimum of further work. This is the basis of successful cross-acceptance.

- Cross-acceptance would involve **acceptance of the EASA (European Aviation Safety Agency) certification of the ESP as an ANSP (Air Navigation Service Provider) by ERA**.

  Only applicable if the “proposer” of the change is ERA and if the risk assessment process is performed by both entities (EASA and ERA).
Process for Safety Demonstration and Acceptance

Proposal for cross-acceptance:

- Consider EGNOS as a “pre-existing item” as specified in the IEC61508 and CENELEC EN50129 standards.
- This would mean no requirement for additional development of the safety case according to EN50129 or IEC61508.
- The safety-related function performed by EGNOS according to §6.2 of EN50129 (2018) may be classed based on:
  
  a) requirements for use of complete pre-existing systems OR
  
  b) requirements for use of pre-existing equipment

- The approach adopted would require approval by an independent safety assessor.
- The concept of a Safety Manual as defined in IEC61508, but not explicitly mentioned in EN50129 (2018), is used to provide the safety evidence required for a pre-existing item by EN50129.
STEWS Conclusions

Recap

- STEMS has investigated the use of EGNOS for applications of GNSS in ERTMS, considering:
  - The legacy services (EGNOS V2, V3.1)
  - The system as-is.
  - An integrity concept for railway based on the provision of integrity in the pseudorange domain.
- This would allow the railway user to assume that pseudoranges for satellites monitored by SBAS are fault-free from system-level feared events (i.e. those originating from the GNSS space segment and ground segment) and ionosphere feared events, up to the target level of integrity.
- Mitigation of local effects and feared events would be the responsibility of the Onboard supplier.
- Focus of work on Virtual Balise Detection due to relative maturity and need for interoperability.
- STEMS has built on the working paper authored by ESA and GSA “Preliminary Study on the Use and Certification of EGNOS in Interoperable Railway Control-Command and Signalling Subsystems”.

© GMV NSL Property - All rights reserved
Outcomes

- Review and consolidation of requirements for Virtual Balise Detection in ERTMS using GNSS.
- In-depth review of aviation MOPS i.e. DO-229E, identifying applicable parts to the SBAS integrity concept for the railway, issues/gaps and recommendations to address these.
- Analysis of the concept of cross-acceptance of EGNOS for use in the railway domain, considering interoperability and safety requirements and the authorisation process.
  - Proposal made to consider EGNOS as a “pre-existing item” as specified in the IEC61508 and CENELEC EN50129 standards, developing a Safety Manual as defined in IEC61508 in order to provide the required safety evidence.
- Feedback has been provided on a number of proposal statements made in the ESA/GSA working paper.
STEMS Conclusions

Future Work

- Drafting of railway receiver guidelines (for the Onboard).
- Analysis of receiver requirements at Trackside/Wayside i.e. the receiver used in the GNSS Augmentation Distribution Function.
  
  *These two items are now being addressed through an initiative led by ERTMS Users Group, ESSP, ESA and GSA in the scope of a CCS TSI Change Request.*
- Assessment of the suitability of EGNOS for consideration as a pre-existing system or pre-existing equipment as defined in EN50129 (2018).
- Development of full safety case.
- Extension of analysis to cover the EGNOS V3.2 Dual-Frequency Multi-Constellation (DFMC) service, including receiver assumptions/requirements based on DFMC MOPS.
- Extension of analysis to cover a hypothetical safety-critical EGNOS railway dissemination channel.
- Extension of analysis to other safety-critical domains which have differences with respect to aviation in terms of operational and regulatory environments e.g. maritime, automotive.
Audience Questions
Thank you
Michael Hutchinson
michael.hutchinson@gmvnsl.com