Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria

doi: 10.3850/ESREL2026061419_esrel26-p27869-cd

Towards the safe deployment of GNSS-based localization for autonomous trains: A Preliminary Hazard Analysis

Evan Samzun
Université de Technologie de Compiègne, CNRS, Heudiasyc, France Syntony GNSS.
E-mail: evan.samzun@hds.utc.fr

Joelle Al Hage
Université de Technologie de Compiègne, CNRS, Heudiasyc, France.
E-mail: *joelle.al-hage@hds.utc.fr*

Mohamed Sallak
Université de Technologie de Compiègne, CNRS, Heudiasyc, France.
E-mail: *mohamed.sallak@hds.utc.fr*

Anis Ziadi
Syntony GNSS, France
E-mail: *anis.ziadi@syntony.fr*

Several European projects have investigated Global Navigation Satellite System (GNSS)-based approaches to simplify signalling architectures and reduce the railway infrastructure costs by migrating more functions on board and relying on virtual blocks instead of traditional fixed-block operation.
However, introducing GNSS into safety-critical functions creates new failure modes and threat scenarios that challenge existing safety certification practices. This paper presents a first step towards the certification of a GNSS-based localization function through a Preliminary Hazard Analysis (PHA) carried out for autonomous shuttle systems.
This PHA identifies GNSS-related events that may lead to hazardous train movements, and provides an initial risk ranking that can guide future design decisions. The analysis combines a functional description of the localization chain and a review of safety-related events from affiliated rail systems (tramways and conventional trains) to compensate the lack of operational data from autonomous shuttles. The PHA highlights a small number of dominant scenarios, including derailment due to erroneous or unavailable GNSS position information. For these scenarios, the paper derives sets of initiating GNSS failures for later quantitative analysis.
The scientific contribution of this work is two-fold. First, it proposes a hazard identification approach adapted to the context of autonomous shuttle safety events. Second, it establishes links between GNSS failure modes and system-level hazards within an EN 50129-compliant signalling safety case.

Keywords: Satellite positioning system, Railway signalling, Autonomous train, Preliminary Hazard Analysis, Dependability

1. Introduction

Today, European railway signalling relies on trackside installations, whose deployment and maintenance contribute significantly to life-cycle costs. One promising direction of future signalling is the transfer of parts of the signalling functionality (like train detection) from trackside to onboard systems. GNSS-based localization is therefore investigated as a potential solution. GNSS is already used in the rail sector for passenger information. However, it is not yet deployed in safety-related functions such as train detection and separation. Bridging this gap would permit the deployment of autonomous shuttles on low-traffic lines, where trackside equipment deployment costs can be a major barrier.

Introducing GNSS brings new kinds of hazards that are atypical of conventional railway signalling. While many studies focus on adapting and improving GNSS localization performance and architectures Spinsante and Stallo (2020); Cai et al. (2020), significant work remains in the certification process, which needs a comprehensive analysis of the link between GNSS risks and train accidents. PHA is typically the first step in the certification process, as recommended by railway standards such as CENELEC (2017). It identifies system risks and links them to hazardous situations likely to cause accidents. These risks are then ranked according to severity and frequency classes, to prioritize safety requirements and guide subsequent analysis.

In this work, we conduct a PHA with reference to a preliminary design of the GNSS-based localization system for the ECOTRAIN[a] project's shuttle. In this paper, we propose:

- An identification and a risk ranking of railway accident scenarios affected by localization system failures for a representative autonomous shuttle use case.
- A practical bridging framework between train accidents and GNSS localization events, providing traceability from GNSS phenomena to train-level hazards in order to support requirements definition, and to validate and provide certification evidence.

This paper is organized as follows. Section 2 presents the case study and system modelling. Section 3 aims to identify and rank the top-level events: the accidents. Section 4 studies the causality chain down to GNSS-induced localization failure modes.

2. Case study and system modelling

2.1. *System under study: autonomous shuttle localization subsystem*

The onboard localization subsystem combines a multi-constellation, dual-frequency GNSS receiver and an inertial measurement unit (IMU). While GNSS provides absolute positioning, IMU improves short-term performance and offers bridging during GNSS outages. Several projects consider this type of architecture for future rail shuttles, such as CLUG2 (2025); Shift2Rail (2021) and TRENI Puccitelli et al. (2022). This subsystem is often augmented by other sources of information, such as digital maps Kassas et al. (2020). The outputs are position, speed and time, provided at a specific frequency. This information is used for traffic management among shuttles and for interaction with basic infrastructure, such as station arrivals and level crossings. In this paper, we focus on the GNSS component, without considering additional sensors.

2.2. *Operational context used for the PHA*

The operational context considers a reference line, the Axat-Rivesaltes corridor, currently used by a tourist train[b], which is representative of a mountainous rural to peri-urban environment. The line is approximately 45km long. The infrastructure mainly consists of single track with passing loops and 47 level crossings, equivalent to 1 level crossings per km. For comparison, the national rate is approximately 0.5. The railway line is shown in figure 1 with its main infrastructure assets.

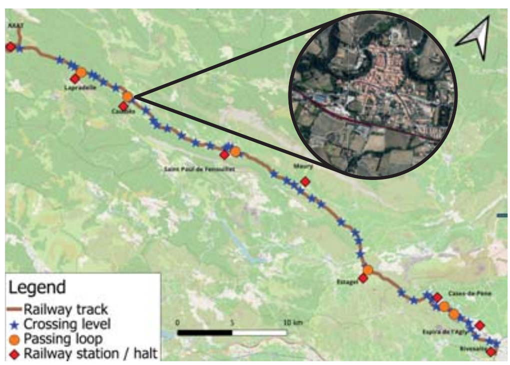

Fig. 1. Axat-Rivesaltes line in under study. Data provided by open access with IGN and SNCF: `https://geoservices.ign.fr/documentation/donnees` ; `https://data.sncf.com/pages/accueil/`

The operating parameters of the shuttle are re-

[a] `https://ecotrain.eu/`

[b] The *Train Rouge*: `https://www.letrainrouge.fr/`

ported in table 1.

Table 1. Autonomous shuttle's system operating parameters

Parameter	Value
Nominal speed	70 km/h
vehicle mass	12 t
maximum passengers	30
service period	17h/day
shuttle interval (minutes)	30

2.3. *PHA causality terminology*

Following the PHA and railway terminology IEC (2019); CENELEC (2017), we define:

- A railway accident as an undesirable safety event with harmful consequences (e.g., fatalities, injuries, damage).
- A hazardous situation as a condition that could lead to an accident. In this study, it is a shuttle-level operational event.
- A dangerous event as a system failure or condition that may result in the hazardous situation. In this study, it is a safety-related localization function failure that can bring to the hazardous situation.

3. Identification of scenarios and risk ranking

This section aims to identify and prioritize railway accidents. The resulting hierarchy is based on an assessment of accident frequency and severity. This task presents a particular challenge in the context of emerging systems, such as autonomous shuttles. We present a methodology for making an *a priori* estimate.

3.1. *Risk ranking framework: standard's recommendation*

Risk ranking follows the railway standard EN-50126-1 CENELEC (2017). A risk is categorized by an estimated probability of occurrence (its frequency), and an estimation of the damages (its severity). Frequency classes range from 1 (*Unbelievable*: one occurrence per 10,000 years) to 6 (*Frequent*: 100 times per year). Severity classes range from 1 (*Operational*: minor injuries, if any) to 5 (*Catastrophic*: more than 10 deaths).

The risk matrix combines frequency and severity of each railway accident, and assigns a tolerance level: *Intolerable*, *Undesirable*, *Tolerable*, *Negligible*, as shown in figure 2. The level of tolerance provides a hierarchy of accidents that drives the allocation of safety measures and subsequent analyses.

Risk qualification		Severity qualification				
		1 Operational	2 Minor	3 Marginal	4 Critical	5 Catastrophic
Frequency qualification	1 Unbelievable	Negligible	Negligible	Negligible	Negligible	Tolerable
	2 Improbable	Negligible	Negligible	Negligible	Tolerable	Undesirable
	3 Rare	Negligible	Negligible	Tolerable	Undesirable	Undesirable
	4 Occasional	Negligible	Tolerable	Undesirable	Undesirable	Intolerable
	5 Probable	Tolerable	Tolerable	Undesirable	Intolerable	Intolerable
	6 Frequent	Undesirable	Undesirable	Intolerable	Intolerable	Intolerable

Fig. 2. Suggestion of the risk tolerance level, derived from the EN 50126 standard

3.2. *Risk ranking framework: adapted methodology*

Autonomous shuttle risk ranking addresses a methodological challenge: anticipate unwanted events from an emerging system when no historical accident data are available. The closest information can be obtained from existing French rail systems, such as the interoperable national rail network (RFN), the secondary branch railway (SBR), and the tramway systems.

We propose an assessment methodology based on the extrapolation of past events from these systems, based on specific operational parameters that influence the frequency and severity of accidents. It is divided into three steps:

(1) Identify key operational parameters contributing to an accident,
(2) Quantify their contribution into an exposure score for each system,
(3) Compare the autonomous exposure score result with the other system to support the assignment of severity/frequency classes.

This framework provides a preliminary severity and frequency assessment. The following subsections illustrate its application through the frequency estimation of a derailment scenario.

Key operational parameters identification

The key operational parameters can be identified from accident reports e.g. SNCF (2023); STRMTG (2023); STRMTG (2023). For derailment, we identify:

- Traffic density
- Train speed
- Curvature density
- Switches density

Exposure score quantification and integration

For each parameter, we rate its relative exposure level on an ordinal scale from 1 to 3 (low - medium - high), derived from measurable indicators (e.g., operating speed, curves per km) based on institutional operational data [c] and operational reports. Exposure scores for the autonomous shuttle system are estimated based on operating parameters listed in table 1. For example, with a speed limit of 70km/h, the exposure score for "train speed" can be estimated as 2 (medium). For "curvature density", an exposure score of 3 can be assigned given the Axat line shown in figure 1.

The total sum provides a ranking of derailment exposure ranging from N to $3N$, where N is the number of parameters. Table 2 illustrates derailment exposure results for different systems. The total exposure scores have a limited range (7-10), indicating that the studied systems are broadly comparable in terms of derailment exposure. The autonomous shuttle ranks second, driven by medium traffic density and speed exposure, but with high curvature exposure.

Comparison of score results and derailment frequency ranking

In this step, we compare the total exposure score, quantified by Σ (theoretical), with the annual accident rates of the systems, as reported in official accident records. This step provides the *Frequency classification* row in the table 3 for the RFN, SBR and tramway systems. The table shows that the hierarchy of the total exposure score is consistent with that of the accident frequency, thus demonstrating the coherence between our theoretical assessment and the observed accident frequencies. This allows us to extend the results to the autonomous shuttles and classify their accident frequency.

We assess the accident frequency of the autonomous shuttle by comparing its exposure score to that of other systems. Since the autonomous shuttle's derailment exposure score is 9, between RFN (8 corresponding to an *Occasional* frequency) and Tramway (10 corresponding to a *Probable* frequency), we conservatively assign a risk level of 5 (*Probable*).

Table 2. Exposure score resume of each systems studied for the derailment.

	Traffic density	Train speed	Curv. density	Switch density	Σ (sum)
RFN	3	3	1	1	8
SBR	1	1	3	2	7
Tram	3	1	3	3	10
AS*	2	2	3	2	9

Note: With the scale 1 to 3, the total exposure range from 4 to 12 (*AS for Autonomous shuttle)

Table 3. Link between total exposure score and frequency qualification. (4: Occasional, 5: Probable)

	RFN	SBR	Tram	AS
Σ	8	7	10	9
Frequency	4	4	5	5

The same strategy is also applied for severity classification, considering different key operational parameters, such as the number of victims, or speed.

[c]information accessible in open data from the IGN and the SNCF websites : https://geoservices.ign.fr/documentation/donnees ;https://data.sncf.com/pages/accueil/

3.3. *Risk-significant accidents for autonomous shuttles (results of the PHA ranking)*

The proposed procedure is applied to each accident to assess frequency and severity. It enables us to propose the accident prioritization, as illustrated in table 4.

Table 4. The dominant risk contributors of the analysis according to their severity (Si) and frequency (Fi) indexes

Accident	Si	Fi	$Si \times Fi$
Side collision	5	5	25
Head-on collision	5	5	25
Train-person collision	4	6	24
Level crossing collision	4	5	20
Derailment	4	5	20
Rear-end collision	3	4	12

The results indicate that the dominant risk contributors are head-on/side collision, train-person collision, level-crossing collision and derailment. Based on figure 2, they are classified as *Intolerable*. The rear-end collision is assessed as *Undesirable* in the considered operational setting.

Although our hierarchy differentiates certain accidents, some events remain of equal criticality (side/head-on collisions, level crossings/derailments). To obtain a clearer hierarchy, a detectability criterion could be integrated into our assessment, as is commonly employed in Failure Mode, Effects, and Criticality Analysis (FMEA) procedures Dissel (2023).

In the next section, these prioritised train accidents are used as reference top events to structure the link between localization-related failure modes and hazardous train situations.

4. Bridging train events and GNSS/localization events

This section addresses a practical certification problem: linking GNSS localization performance to hazardous situations at the shuttle level. We present two examples that highlight the links between GNSS failures and railway accidents.

4.1. *PHA causality levels*

The causality chain is shown in figure 3, starting from accident scenarios and ending with the GNSS failure modes, which occur at the localization outputs (position, speed, time, heading).

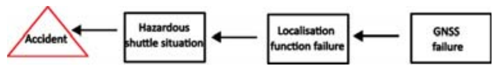

Fig. 3. Causality chain followed by the PHA

The methodology proceeds by following the causality chain to establish the corresponding causal links. Before doing so, we present GNSS criteria that can lead to failure modes. These criteria are generic, well-defined, and documented in standards and in the literature such as CENELEC (2020) and ETSI (2020).

4.2. *GNSS performance criteria and failure modes*

GNSS performance can be described in terms of four criteria: accuracy, integrity, availability and continuity Jing et al. (2022); Zhu et al. (2018). In this paper, we focus on the first two criteria that are used in the remainder of this paper.

Accuracy refers to the difference (error) between a measured or estimated value and its real one.

Integrity is a measure of the trust in the accuracy of the localization-related data provided by the localization system and the ability to provide timely and valid warning to users when the localization system does not fulfil the condition for intended operation.

Protection Level (PL) is an integrity parameter representing a statistical error bound computed to ensure that the probability of the absolute position error exceeding the PL is smaller than or equal to the target integrity risk (TIR):

$$P(error > PL) < TIR \qquad (1)$$

This parameter is used to assess the performance of a localization system.

These criteria are generally characterized by threshold values specific to each case study, which form the basis for certification. We propose to define a GNSS failure as an exceed of defined thresholds. In the following, we illustrate different use cases to demonstrate the link between these criteria and accident related events.

4.3. *Causality chain study applied to operational scenarios*

In this section we will focus on constructing a causal chain, starting from an identified accident and tracing back to one or more GNSS failures. This approach will be illustrated using two types of indicative accidents: Head-on collisions and derailments.

4.3.1. *Head-on collision*

The line under consideration is a single-track, and shuttles can pass one another only at crossing loops. During a normal planned crossing, the waiting shuttle is routed into the siding and waits while the main shuttle remains on the main track to pass. A hazardous situation occurs if the system incorrectly believes that the main shuttle has left the track, while it is still occupying the track section planned for the waiting shuttle. This creates a conflicting train movement which can lead to a head-on collision.

Returning to localization function causality, this situation can occur if the localization function misjudges shuttle block occupancy. Accuracy and integrity are critical to this operational case as shown in figure 4. Indeed, the main shuttle estimated position is situated in block 2, and the protection level indicates that it is confident about its localization. However, the main shuttle is actually located in block 1. The waiting shuttle, aware only of the estimated position, perceives block 1 as free and decides to move. This misjudgement of track occupancy may cause both shuttles to enter the shared area, creating a risk of collision.

4.3.2. *Derailment*

We assume a simplified speed supervision function, where the shuttle follows a permitted speed profile derived from the track layout (curves, elevation). A hazardous situation arises if the shuttle exceeds the permitted speed, potentially leading to

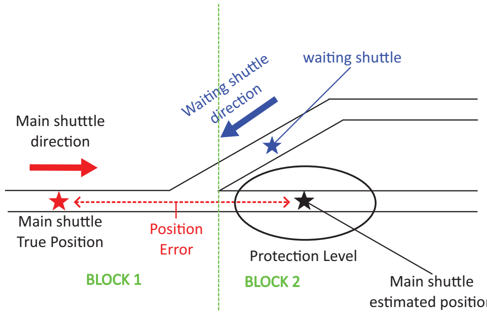

Fig. 4. A GNSS failure that could lead to a hazardous situation

a loss of guidance and derailment.

Two localization-function failures can contribute to this hazardous situation:

(1) An underestimation of the shuttle speed,
(2) A block occupancy misjudgment, which causes the system to apply the wrong speed limit.

The first case depends on a persistent speed underestimation by the GNSS-based localization system. Speed accuracy is critical in this case. The second failure, resulting from incorrect block occupancy, is linked to localization accuracy and integrity, as discussed in section 4.3.1. Indeed, a speed limit is associated with each occupancy block, misjudging a block will result in a speed that differs from the reference value.

5. Conclusion

In this work, we conducted a preliminary risk analysis for autonomous shuttle accidents. We proposed a methodology for a risk ranking framework based on three steps. The analysis has identified the main critical accidents with a risk extrapolation method. We also proposed a causality study to link the accidents to GNSS failure modes. We detailed two examples and show that the accuracy and integrity of localization are critical to avoid accidents. Formalisation of GNSS criteria thresholds for specific operational scenarios should be done, as these were not defined in this paper.

References

Cai, B., B. Wu, and D. Lu (2020). Survey of performance evaluation standardization and research methods on gnss-based localization for railways. *Chinese Journal of Electronics 29*(1), 22–33.

CENELEC (2017). EN 50126-1 Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process. English version.

CENELEC (2020). En 16803-1:2020 — space: Use of gnss-based positioning for road intelligent transport systems (its) — part 1: Definitions and system engineering procedures for the establishment and assessment of performances.

CLUG2 (2025). Clug demonstration of readiness for rail – clug 2.0 d6.5 - architecture trade off analysis and proposed localisation on-board system. Project deliverable, European Union Agency for the Space Programme.

Dissel, R. (2023). Ertms/etcs hybrid level 3: Analysis of the overall challenges/limitations of etcs hybrid level 3. Master's thesis, Delft University of Technology, Delft, The Netherlands.

ETSI (2020). Satellite earth stations and systems (ses); gnss based location systems; part 3: Performance requirements. Technical report, European Telecommunications Standards Institue.

IEC (2019). IEC 31010:2019 — Risk Management — Risk Assessment Techniques.

Jing, H., Y. Gao, S. Shahbeigi, and M. Dianati (2022). Integrity monitoring of gnss/ins based positioning systems for autonomous vehicles: State-of-the-art and open challenges. *IEEE Transactions on Intelligent Transportation Systems 23*(9), 14166–14187.

Kassas, Z. M., M. Maaref, J. J. Morales, J. J. Khalife, and K. Shamei (2020). Robust vehicular localization and map matching in urban environments through imu, gnss, and cellular signals. *IEEE Intelligent Transportation Systems Magazine 12*(3), 36–52.

Puccitelli, M., L. Marradi, G. Pastore, H. Al Bitar, A. Tobie, R. Guidi, G. Galgani, F. Inzirillo, F. Rodriguez, A. Martinelli, Y. Yossef, and D. Lopour (2022). The treni project: Development of a galileo-based gnss receiver and antenna for railway safety-related applications. In *2022 52nd European Microwave Conference (EuMC)*, pp. 1–4.

Shift2Rail (2021). Consolidated annnual activity report 2020. Technical report, Shift2Rail Joint Undertaking (S2R JU).

SNCF (2023). Annual safety report 2023. Technical report, SNCF Réseau Safety.

Spinsante, S. and C. Stallo (2020). Hybridized-gnss approaches to train positioning: Challenges and open issues on uncertainty. *Sensors 20*(7).

STRMTG (2023). Annual report 2023: Fleet, traffic and operational events — tramways. Technical report, Technical Service for Cableways and Guided Transport.

STRMTG (2023). Parc, trafic et événements dexploitation — chemins de fer secondaires : Rapport annuel 2023. Technical report, Service Technique des Remontées Mécanique et des Transports Guidés.

Zhu, N., J. Marais, D. Bétaille, and M. Berbineau (2018). Gnss position integrity in urban environments: A review of literature. *IEEE Transactions on Intelligent Transportation Systems 19*(9), 2762–2778.