Proceedings of the Seventh International Conference on
Railway Technology: Research, Development and Maintenance
Edited by: J. Pombo
Civil-Comp Conferences, Volume 15, Paper 24.4
Civil-Comp Press, Edinburgh, United Kingdom, 2026
ISSN: 2753-3239, doi: 10.4203/ccc.15.24.4

Safe Processing for Light Rolling Stocks

M. E. A. Abdullah[1], S. Collart-Dutilleul[2] and O. Ait Mohamed[1]

[1]University Concordia, Montreal, Canada
[2]University Gustave Eiffel, France

Abstract

Light rolling stocks are considered for allowing a frugal exploitation of European secondary regional lines. The Ferromobile proposition is based on a 8 seated road minibus adapted for rail operated in driverless mode. The use of an automatic protection (ATP) inspired by the functional specification available concerning European Railway management system (ERTMS), is proposed to insure the respect of signalling. The present paper focus on the potential impact on a bit flip of the ATP dedicated processor. An error was analysed using a statistical model checking tool on an open architecture processor. The results achieve a correct level of reliability, but enlarging the restrictive assumption of the study deserve further investigations.

Keywords: regional european lines, railway safety, ATP, bit flip, processor design, light rolling stocks.

1 Introduction

Regional railway lines have to handle lower demand in terms of traffic capacity. This impacts their business model in a form that leads to a new challenge: providing tailored services, because the business model does not allow wasting by overweighting, oversizing, and overcapacity.

Several studies related to regional railway lines converge towards a seating capacity range between 10 and 70 [1]. The lowest value was computed studying reactivating potentialities, mainly considering G2 Lines in Germany.

The addressed regional lines were divided into two main categories:
– Group 1 Regional Lines (G1 Lines) connected with the mainline railway system. They shared regular exchanges of passengers with mainlines.
– Group 2 Regional Lines (G2 Lines) which are lines not functionally/operationally connected with the mainline network. As a consequence, their passenger or freight rolling stocks never enter a mainline infrastructure.
This leads to considering two types of rolling stock:
1. Type A: for longer distances (G1 lines),
maximum speed: 120 km/h.
passenger capacity: 56-80 seats
offering comfort commodities, like toilets.
Crashworthiness: category is G1/C1.
2. Type B: for short routes and frequent stops,
Maximum speed :100 km/h.
passenger capacity: less than 42 seats,
Length: less than 20 meters, (potential use of smaller platforms)
For this second class of rolling stocks, it is proposed to use a less restrictive Crashworthiness category, when it can be demonstrated that they never collide with a main line rolling stock, but only with smaller ones.

Examples include the Mireo Plus B from Siemens (117 seats) 2, ÖBB 5047 (67 seats), or Alstom Lint 41[1] (120 seats and 8 tons of service weight). According to European recommendations and fulfilling the CENELEC 15380 norm [5], most of them have multifunctional spaces for wheelchairs, prams, and bicycles, as well as universal toilets.

The smallest vehicles currently available on the market are 2-car, around 42-45 m long multiple units with Jacobs bogies and around 100 seats. It is clearly 10 times bigger then the lower bound provided by the previously mentioned studies in terms of passenger capacity [1].

[1] *https assets.new.siemens.comsiemensassetsapiuuid* : 1*cdbf*355 – *fa*91 – 4*fca* –8917 – 5*e*04*e*9419*e*17*mors* – *b*10022 – 00*dbmireoplusortenau* – 72*oriqinal.pdf*

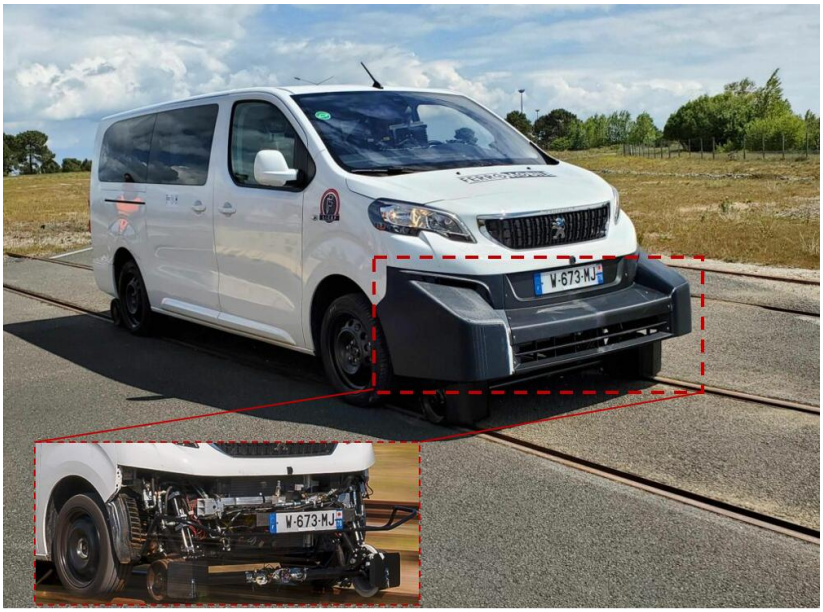

Figure 1: A Ferromobile on a railway track.

Focusing on a first target of revival of French secondary railway lines, the Ferromobile project identified a need of a 8 seated vehicle. Considering the business model, the salary cost of a driver cannot be handled and the vehicle should be autonomous. A second consequence is the presence of a prominent protection on the front of the Ferromobile which functionally plays the role of a stone guard (see figure 1).

The Ferromobile is built from a Peugeot E-Express Electric car. Using the guiding wheels that are visible on the figure 1, in front of and behind the car, the car can roll on a railway track. The massive metallic protection that visible on the excerpt of the head of the car are necessary mostly because of a railway specific danger: derailment. If a stone, a wild boar [3], or another a beast go under the car during a collision, a derailment may occur. This kind of protection is not needed on a road car.

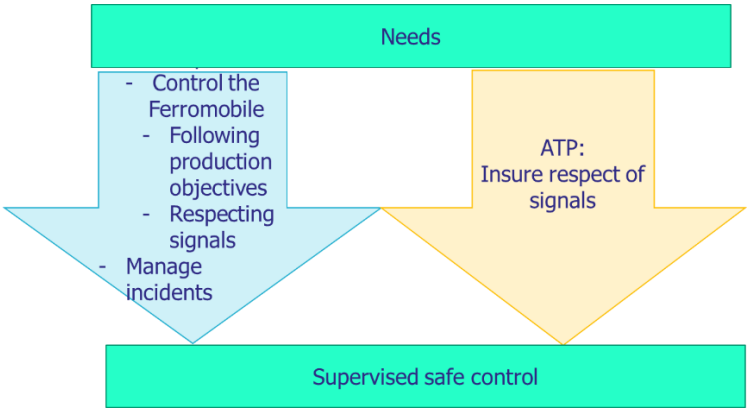

Figure 2: proposition of an ATP

When the train is driverless, then another business model can be applied. Using Automatic train Operation (ATO) on secondary line is an innovation, as driverless metro lines belong to the class of massive urban transports. Moreover, driverless metro infrastructure is designed so that, no pedestrian, vehicle or animals can access to the track. Specifying a safe ATO for low traffic regional lines is a difficult new subject for safety studies.
A first proposition, is to use an ATP controlling that signalling (i.e. stops point and speed limits) is insured with a reliability compatible with the severity of danger that it prevents. Considering the software railway norms, a framework using ERTMS as a functional reference model has been proposed [4,14] to specify an ATP component.
The main idea is not to use the ERTMS norms which is based on costly components, but rather to provide similar functions using cost effective services allowed by smaller vehicles and much lower commercial speeds. Assuming that image processing from cameras and lidar signal analysis is based on complex calculation that would be difficult prove, the ATP considers the vital rolling stocks information to check that basic safety properties are fulfilled: it must be as simple as possible and cost effective.
Assuming that the software specification is perfectly compliant with railway norms concerning software entities [2], the present paper proposes to answer the question of the potentiality of a processor execution that is compliant with the safety needs, but to the low cost pragmatic need too. The next section presents a methodology, identifying safety objective focusing on a single hazard: bit shift producing the non-respect of an EOA (End Of Authority). The study is based on an open source design on which STPA analysis (System-Theoretic Process Analysis) is applied. In the last section, hazards rate is produced with regards to the Device Vulnerability Factor (DVF) evolutions.

2 Methodology:

2.1 Safety objective

SO1. The onboard controller shall ensure that the vehicle stops at the intended position associated with the valid EoA / stop condition.

This objective follows from the ATO-over-ETCS functional reference model adopted for Ferromobile [4, 7], where the onboard controller must respect the Movement Authority (MA) and stop at or before the End of Authority (EoA) [8, §3.2].

2.2 Hazards

H1 — gross overrun. The vehicle stops past the EoA by a distance that exceeds the authorized protective distance. H1 is the higher-severity positive-direction violation.

H2 — bounded positive stop-position violation. The vehicle stops beyond the intended EoA-related stopping target, but the excess distance remains below the gross-overrun threshold used for H1. H2 is therefore a lower-severity positive-

direction violation: it does not create the downstream-conflict condition associated with H1, but it still violates the intended EoA stopping objective.

Grounding. Hamidi et al. [8] §3.2 introduce the protective-distance model and partition braking errors into a positive-direction error (vehicle past target) and a negative-direction error (vehicle short of target). Both H1 and H2 fall in the positive-direction regime; the partition between H1 and H2 is by magnitude, where H1 violates the protective envelope and H2 does not.

2.3. STPA control structure

Figure 3 shows the control structure used as the basis for our STPA analysis (System-Theoretic Process Analysis). As we used The Leveson–Thomas STPA Approach [9], it requires the control structure to be made explicit before deriving UCAs. The diagram identifies the in-scope component (the onboard controller running the EoA-handling firmware on a NEORV32 instantiation on Zynq-7020) and the out-of-scope components held nominal (trackside controller, brake plant, and vehicle dynamics).

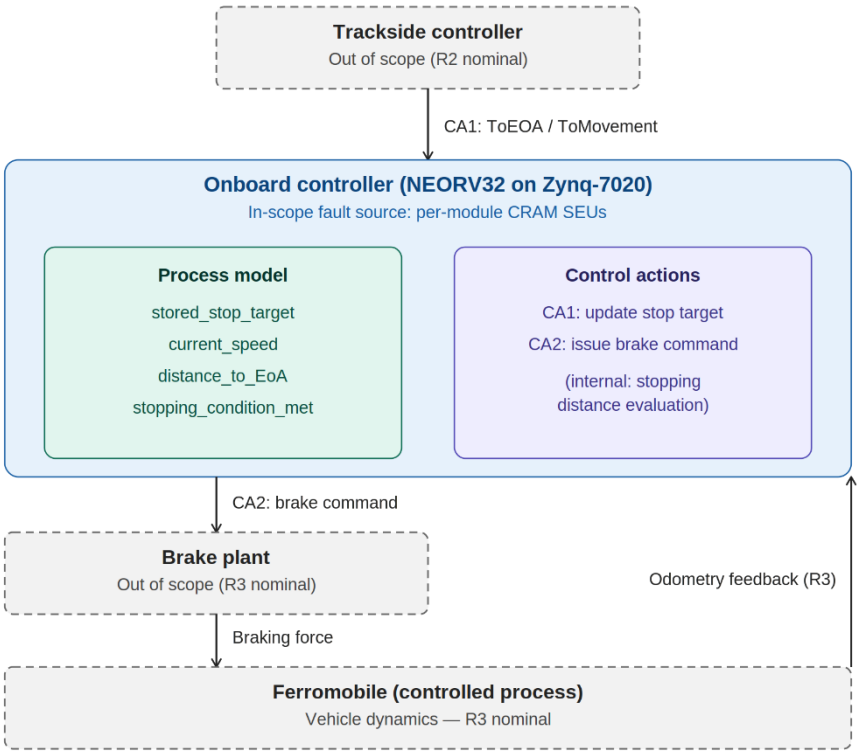

Figure 3. STPA control structure for the Ferromobile EoA-handling scenario.

The two Control Actions in scope are CA1 (ToEOA / ToMovement, trackside-to-onboard) and CA2 (MakeTrainStop / Brake, onboard-to-brake-plant). The internal stopping-distance evaluation described in [8] §4.1 is part of the onboard controller's process model and is not modelled as an exchanged Control Action.

2.4. Control actions and unsafe control actions

2.4.1 Control actions

CA1. Update / commit the local EoA-related stopping target after valid MA / EoA information is available (ToEOA / ToMovement).

CA2. Issue the braking / stop command (MakeTrainStop / Brake).

Grounding. CA1 corresponds to the Autopilot ToEOA / ToMovement messages in the SysML model of [4] §4.2 and is verified verbatim in [10] (the goal model: ProgressTrain is satisfied by ToEOA + ToMovement; StopTrain is satisfied by MakeTrainStop + MoveTrain). CA2 corresponds to the MakeTrainStop / Brake message in the same sequence diagram. Because communication is held nominal in our scope, CA1 captures the local commit of the received target rather than the trackside-to-onboard transmission itself.

2.4.2 Unsafe control actions

UCAs are derived by applying the four guide-word categories of the STPA Handbook [9] to each Control Action: (a) action not provided when required; (b) action provided when not required, with a wrong value, or to the wrong target; (c) action provided too early, too late, or in the wrong order; (d) action stopped too soon or applied too long. Applying these to CA1 and CA2 gives eight candidate UCAs; we retain five as in-scope.

Table 1. Unsafe control actions.

ID	Control action and unsafe mode	Context	Hazard
SU1	CA1 not provided when required	A new MA has been received, and the onboard target must be synchronized, but no update reaches stored_stop_target. The controller continues braking against the previously stored EoA-related target. If that stale target lies modestly past the current EoA, the resulting stop falls within the protective envelope (H2); if it lies grossly past, the protective envelope is exceeded (H1).	H1, H2
SU2	CA1 provided with wrong value	Vehicle within braking distance of the EoA; stored target is corrupted during update. The implicit target is wrong by an unknown sign and magnitude.	H1, H2
SU3	CA1 provided too late / out of order	Vehicle has passed the point at which a safe stop based on the previous EoA is still achievable; the update arrives but is too late to be acted on.	H1, H2
SU4	CA2 not provided when required	Current speed and distance-to-EoA satisfy the braking-initiation condition, but no brake command is issued.	H1
SU5	CA2 provided too late	Braking-initiation condition true at time t; command emitted at $t + \delta$ with δ exceeding the available margin for a stop within the protective envelope.	H1, H2

Three candidate UCAs from the systematic STPA enumeration are excluded with the following rationale:

- **Spurious provision of CA2** (brake provided when not required) results in the vehicle stopping short of the EoA. This falls in the negative-direction regime of [8] §3.2 and is out of scope per §3.2.
- **CA2 provided too early** also results in a stop short of the EoA, again in the negative-direction regime of [8] §3.2 and out of scope per §3.2.
- **CA2 released too soon** (brake released before the vehicle stops) requires modelling sustained brake-control behavior rather than the discrete brake-issuance modelled by CA2.

2.5. Controller responsibilities

R1. The onboard controller preserves correct local handling of valid EoA / stopping information and issues braking-related control so that the vehicle stops at the intended position. Derived from [4, 7].

R2. Communication faults are excluded from this study, which means that the received EoA information is assumed valid.

R3. The vehicle dynamics and braking plant are not fault sources in this model; they are used only to interpret if a delayed or missing command would lead to a hazardous stop.

2.6 Safe and hazardous outcomes

SS. Intended safe stop at the EoA-related position.

SH1 (gross overrun). The vehicle stops past the EoA by a distance that exceeds the authorized protective distance. Either no braking was applied, or braking was applied too late to arrest motion before exceeding the protective envelope. Realization of H1.

SH2 (bounded positive stop-position violation). The vehicle stops past the intended EoA-related stopping target at a wrong final position, but the excess distance remains below the gross-overrun threshold. The protective-envelope violation of SH1 is not reached; the deviation is still a violation of the intended stopping objective. Realization of H2.

3 Results: Processor fault classes and module-to-UCA routing

3.1 Processor scope

We assume that the onboard controller runs on a NEORV32 soft processor [11, 12] implemented on a Xilinx / AMD Zynq-7020 FPGA (PYNQ-Z2 board), following the platform studied by Cora et al. [11]. NEORV32 is documented [12] as a two-stage in-order pipeline with an instruction-fetch front-end and an execution back-end coupled by a multi-cycle processing engine. We retain the five modules CU, ALU, BUS, MEM, and RF and use their CRAM essential-bit counts directly from [11, Table 2]. The Device Vulnerability Factor (DVF), defined in AMD's Device Reliability Report UG116 [13] as the fraction of configuration-memory upsets that produce a functional error, is the principal parameter of our analysis; UG116 reports typical design-level values around 5%. We sweep DVF over [0.05,1.0] – from this typical value to the conservative bounding case DVF = 1 – and report the processor induced hazard rate as a function of it.

3.2 Operational rates

Per-vehicle EoA-event rate λ_EoA. The Ferromobile business model in [10] targets secondary lines with low traffic density. Assuming each vehicle performs two station-

to-station missions per operating day and approximately three MA-update / EoA-reach events per mission, the per-vehicle rate is 2 × 3 / 24 h ≈ 0.25 /h. This value is used as a nominal operational assumption rather than as a measured service rate.

Brake resolution time τ_brake. Paper [4] §2 states that Ferromobiles brake in only 100 metres at their commercial speed, as an order of magnitude. Paper [10] §II describes the on-rail demonstrator operating at 70 km/h. Modelling uniform deceleration from 19.44 m/s over 100 m gives t = 2 × 100 / 19.44 ≈ 10.3 s. We adopt τ_brake = 10 s, giving 1/τ_brake = 360 /h. The 100 m figure in [4] is itself an order of magnitude and the Subset-26 braking profile is non-linear (a polynomial of degree five [14]).

3.3 PRISM model checker properties

We follow the system-level probabilistic model checking approach of Ammar et al. [6]. The PRISM model encoding Q is queried for the following properties:

- Mean first-passage time E[T] from S0 to {SH1 ∪ SH2}, the lumped MTTF.
- Processor-induced hazard rate h = 1/MTTF.
- Sensitivity sweeps over DVF ∈ [0.05, 1.0] and λ_EoA ∈ [0.10, 0.50].

3.4 Processor-induced hazard rate as a function of DVF

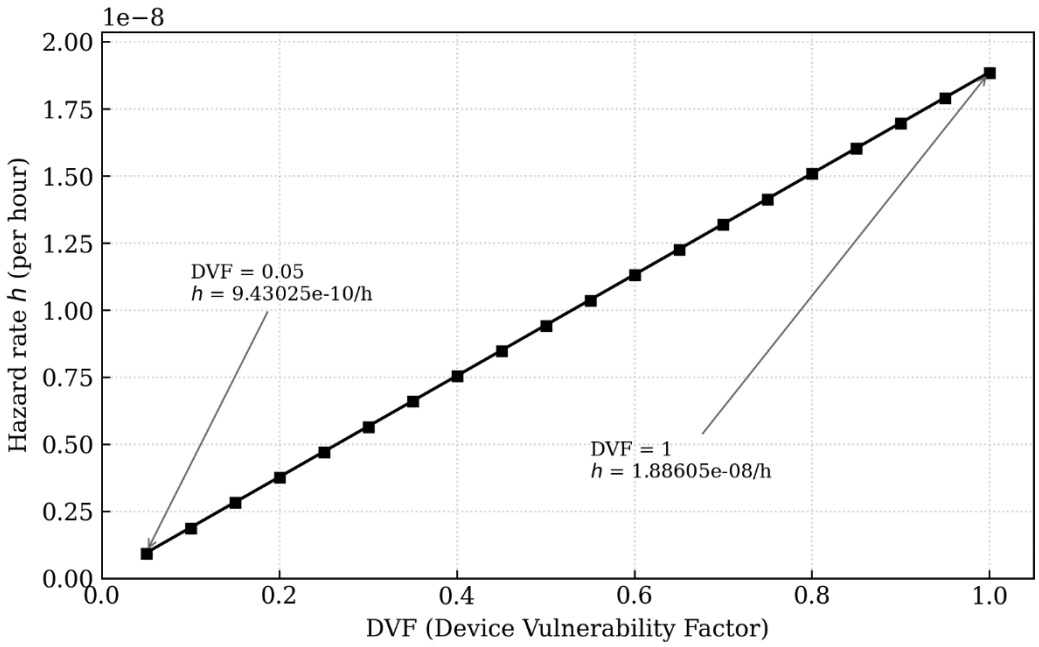

Figure 4. PRISM-computed processor-induced hazard rate h (per hour) as a function of DVF.

Figure 4 shows the corresponding hazard rate. The relationship is linear in DVF to within ~10^{-7} relative. For railway applications interested in tolerable-hazard-rate (THR) comparisons, a measured workload-specific DVF can be used directly to scale the upper-bound figure reported here.

3.5 Discussion regarding safety

Concerning EOA and the corresponding safety interpretation, hazard rates does not really meet the specification, unless the DVF is limited to 0.5
Assuming that corruption of an EOA end of section value may produce a collision with another rolling stocks which is stopped ahead in a station for letting passenger going in and out,this scenario is clearly considered as a catastrophic event that should be highly improbable to reach a tolerable state (see figure 5). As a consequence, the safety conditions looks clearly achievable. The documentation of AMD claims "The DVF for a typical design is 5% (one in 20 upsets, on average, cause a functional soft error). In the worst case, the DVF is never larger than one in ten, or never more than 10% of the upsets cause a soft functional error."

However, several scenarios may be considered and the present paper only focus on the processor execution level. The hypothesis of two travels per day is really low and higher values of traffic should be studied.

Finally, the proposed preliminary study, rather reaches initial objectives: the targetted safety level is reached, not easily and not by far. However specific technological measures may increase the obtained results.

			Severity Classes			
			S1	S2	S3	S4
			Insignificant Minor injury	Marginal Major injury	Critical Single fatality	Catastrophic Multiple fatalities
Frequency Classes	F1	Frequent $F > 10^{-3}$	Undesirable	Intolerable	Intolerable	Intolerable
	F2	Probable $10^{-3} \leq F < 10^{-4}$	Tolerable	Undesirable	Intolerable	Intolerable
	F3	Occasional $10^{-4} \leq F < 10^{-5}$	Tolerable	Undesirable	Undesirable	Intolerable
	F4	Rare $10^{-5} \leq F < 10^{-7}$	Acceptable	Tolerable	Undesirable	Intolerable
	F5	Improbable $10^{-7} \leq F < 10^{-9}$	Acceptable	Acceptable	Tolerable	Intolerable
	F6	Highly improbable $F \leq 10^{-9}$	Acceptable	Acceptable	Acceptable	Tolerable

Figure 5. Risk acceptability Matrix from [15].

4 Conclusions and Contributions

The paper presented the context of the Ferromobiles that takes place in global vision of European secondary line revival. As Ferromobile should be driverless for economic reasons, a dedicated ATP component is proposed in order to respect signalling with a high level of reliability. Taking into account the low coast constraints, the paper presented a study of a publicly available design and considers that potential bit flip of the end section of an EOA. Using an ASTP methodology, A simulation is performed using a statistical model checking tool. A first analysis shows that the results are compatible with the class of severity of the potentially induced scenario.
The study is based on very low traffic assumption. In order to allow a wider range of application, less restrictive assumptions producing higher failure rate should be integrated. Nevertheless, the current study does not investigate all potential defence strategies.
Further works may use selective hardening for providing better results.
Moreover, the detailing the technical implementation used in the current study will allow concurrent propositions and improve scientific transparency.

Acknowledgements

This work was carried out as part of the Ferromobile project, funded by Agency for Ecological Transition (ADEME) through the 'France 2030' program (grant number 2282D0215-F).

References

[1] Pauline Guicheney and Working group,: D5.1 state-of-the-art report for regional lines rolling stock. Tech. rep., Europe'sRail (2024)
[2] Cenelec: 15380-5:2014,railway applications - classification system for railway vehicles - part 5: System breakdown structure (sbs). Tech. rep. (2014)
[3] Jägerbrand, A.K., Gren, I.M.: Consequences of increases in wild boar-vehicle accidents 20032016 in sweden on personal injuries and costs. Safety 2018, 4(4), 53; https://doi.org/10.3390/safety4040053 (2018)
[4] S. Collart-Dutilleul, P. Bon, and R. Laleau, "Securing automatic small railway vehicles using Automatic Train Protection," Leveraging Applications of Formal Methods, Verification and Validation. Application Areas: 12th International Symposium, ISoLA 2024, Crete, Greece, October 27–31, 2024, Proceedings, Part V,Pages 159 – 173, https://doi.org/10.1007/978-3-031-75390-9_11
[5] En 50716:2023 railway applications. requirements for software development. Tech. rep., BSI (2023)
[6] Ammar, M., Hamad, G.B., Mohamed, O.A., Savaria, Y.: System-level analysis of the vulnerability of processors exposed to single event upsets via probabilistic model checking. IEEE Transactions on Nuclear Science 64(9), 2523–2530 (2017). https://doi.org/10.1109/tns.2017.2736061, https://publications. polymtl.ca/38595/
[7] UNISIG, "Subset-125: ATO over ETCS — System Requirements Specification," Issue 0.1.0, 2018.

[8] A. Hamidi, S. Collart-Dutilleul, and P. Bon, “Formalizing for proving the system safety of the software component for a small sized guided transport system,” LNCS, Springer, 2023.
[9] N. G. Leveson and J. P. Thomas, “STPA Handbook,” MIT, 2018. http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
[10] S. Collart-Dutilleul, P. Bon, and A. Hamidi, “A railway norms application for small traffic railway lines autonomous vehicle,” in 2023 7th International Conference on Control, Automation and Diagnosis (ICCAD), 2023, pp. 1–6.
[11] G. Cora, C. De Sio, S. Azimi, and L. Sterpone, “Selective hardening of RISC-V soft-processors for space applications,” Microelectronics Reliability, vol. 167, art. 115667, 2025. https://doi.org/10.1016/j.microrel.2025.115667.
[12] S. Nolting and the NEORV32 contributors, “The NEORV32 RISC-V Processor,” Zenodo, 2024. https://doi.org/10.5281/zenodo.10851939.
[13] AMD, Device Reliability Report (UG116), Revision 10.20, 23 July 2025. https://docs.amd.com/r/en-US/ug116.
[14] UNISIG, “Subset-26: System Requirements Specification,” Baseline 3 Release 2, 2016.
[15] CENELEC EN50126. En-50126-2. railway applications - the specification and demonstration of reliability, availability, maintainability and safety (rams) - part 1: Systems approach to safety. Technical report, BNF AFNOR-CEF/UF9, 2017.