Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Function Analysis Of Safe Train Driving

Yang Sun[a,b], Anne Barros[a], Marc Sango[b], Guy André Boy[a,c]

[a]*Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, France.*
[b]*SNCF SA, France*
[c]*ESTIA Institute of Technology, Bidart, France*

Keywords: railway system, automated trains, safety, function analysis, reliability analysis

Automated trains promise a railway system with better precision and capacity for the future urban transportation system. Compared to the automated metro, for high-speed train driving, as the tracks are less protected and circulating speed is higher, train drivers can meet more complex and critical situations. Facing the automation transition from classical driving trains on Grade of Automation 1 (GoA1) to semi-automated trains on Grade of Automation 2 (GoA2), the French railway company (SNCF) aims to analyze the potential risks and threats of this next generation railway system.

The key change of this automation transition to GoA2 is the introduction of Automated Train Operation (ATO) (ERA, 2022). ATO works under the signalization provided by the European Train Control System (ETCS). From the journey profile and the signalization information, once activated, ATO can control the train according to the optimal speed from its calculation. On GoA2, ATO is a driving assistance available for the train drivers. Once the working conditions are met, ATO changes in ready status and the train driver can decide to engage the ATO and relief from the train speed control mission.

However, the grade of automation for trains can negatively impact the train drivers' vigilance and potentially conduct to railway accidents trains (Brandenburger et al., 2021; Hunter and McDermid, 2022). Once ATO is activated, the driving mission is shared between the human (train driver) and machine (ATO). In this situation, from current specifications, humans are always responsible for driving security. His/her mission of observing the environment cannot yet be replaced by a machine on GoA2.

Let us consider a quick functional analysis of the main function: "Driving Safely". The essential function at the top of the hierarchical function tree (Rausand et al., 2020) is driving safely. We then breakdown this function with the corresponding subfunctions on lower levels of indenture:

- Safe Speed Control;
- Compliance with the Signals;
- Stop the Train in an Emergency.

For each sub-function, we identify the item that commands an action and the item that does the action. The item can be either a component of the technical subsystem or a human individual in the railway system.

Safe Speed Control: in the driving cabin, the train driver controls the train speed according to the information provided by signalization system (ETCS). In case of overspeed, the train is protected by the automatic train protection system (ATP).

Compliance with the Signals: the signals passed at danger (SPAD) is the most frequent type of incident in SNCF network for the past years (Sun et al., 2023). Passing a closed signal without authorization can lead to catastrophic accidents as collisions. During the train journey, the train driver is the only item who can perceive the signalizations all the time and controls the train accordingly.

Stop the Train in an Emergency: due to the relatively open working environment of trains, train drivers need to observe consecutively the rail condition and stop the train in case of emergency. In case of emergency, the train driver needs to initiate an emergency stop by the brake system.

From this function analysis, we can develop the reliability block diagram in Figure 1 to clarify the reliability barriers and redundancies of the train system.

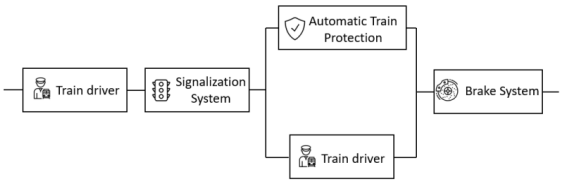

Fig. 1. Reliability block diagram for driving safely.

We see the importance of train drivers' contributions for safe driving from this diagram. To assure a safe journey, the basic items are the signalization system, the brake system and train drivers. Train drivers is also a redundancy barrier of safety for ATP. ATP protect the train from overspeed, but in case of ATP dysfunctional, the train driver can also act as a barrier to initiate the emergency stop to assure the safety of journey.

This reliability block diagram can be used on both GoA1 and GoA2. On GoA2, once the train driver decides to engage ATO, ATO takes the mission of speed control. But in case of ATO dysfunctions, the train driver still needs to take the relays and regulate the train speed in the safe interval. The safety barrier on GoA2 is independent on ATO. In practice, the introduction of ATO can impact the workload and situational awareness of the train drivers. This analysis emphasis the critical role of train driver in system reliability.

This preliminary analysis shows that further research has to focus on i) the reliability of ATO and ii) the influence of ATO introduction to the train driver's capacity to fulfill his/her functions. Point ii) is studied with a human centered approach and Safety-Critical Scenarios are planned to be implemented at SNCF on a simulator. What we propose in this work is a more quantitative approach, by studying the ATO reliability. We also propose to study the reliability of the Signalization System, the ATP system and the Brake system, so that we can lead a sensitivity analysis of the main function "Driving safely" to the item Train driver.

Acknowledgements

This work is funded by the ANRT under the contract number CIFRE 2021/1350.

References

Brandenburger, N., Naumann, A., Jipp, M. 2021. Task-induced fatigue when implementing high grades of railway automation. Cognition, Technology & Work 23(2), 273–283.

ERA. (2022). ERTMS/ATO. System Requirements Specification.

Hunter, J., McDermid, J. 2022. Investigating Human Error Within GoA-2 Metro Lines. In: Collart-Dutilleul, S., Haxthausen, A. E., Lecomte, T. (Ed.), Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification, 179–191. Springer International Publishing.

Rausand, M., Barros, A., Hoyland, A. 2020. System Reliability Theory: Models, Statistical Methods, and Applications (1st ed.). Wiley.

Sun, Y., Sango, M., Barros, A., Boy, G. A. 2023. Preliminary Safety-Critical Scenario Analysis of Semi-Automated Train Operation.

Security, vulnerability and resilience of systems