Use of Safety Guarantees of Train Protection in the Safety of Autonomous Train Driving

Lukas Kacar

Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Transport Telematics, Konviktská 20, 110 00 Prague 1, Czech Republic, kacarluk@cvut.cz; ORCID 0009-0008-9513-4680

https://doi.org/10.29227/IM-2025-02-02-110

Submission date: *2025-04-03* | Review date: *2025-04-24*

Abstract

Autonomous train operation (defined by the on-board part of the ATO - Automatic Train Operation) is a key innovation in rail transport, bringing increased efficiency and safety. Ensuring ATO safety is a key challenge that can be addressed by integration with the European Train Control System (ETCS). This paper focuses on using ETCS safety mechanisms to ensure the safety of autonomous train control. The following paper analyses the possibility of taking over the ETCS safety guarantees into the ATO. It focuses on the different types of data provided by the ETCS, including static train data, dynamic data (movement authority, speed profile, gradient, localization, ETCS modes and traction) and information about the braking capabilities of the train. The key question is whether this information can be relied upon to implement autonomous control without additional redundant mechanisms. According to the RAMS (Reliability, Availability, Maintainability, and Safety) analysis, existing safety features can be adopted if the risks corresponding to the subsystem are sufficiently reduced and there is a secure link between the ATO and the ETCS systems. The specific physical interconnection via Ethernet plays an important role here. This link is described directly in the European Railway Agency specifications. Twelve packets of information are transmitted through this link. The aim is to verify whether it is possible to take over the safety guarantees of the ETCS for the ATO and to find the interface requirements between these systems. The main requirements of the ATO functions that process the ETCS information are to stop safely at a defined location, to keep to the schedule within the conditions specified by the ETCS, to optimize the speed for efficient traction energy consumption and to start the station check-in sequence only after all safety conditions have been met. The methodology includes the analysis of the common interface between the ATO and the ETCS and applying RAMS procedures to identify and mitigate risks. The following paper describes that the ETCS provides robust safety barriers during standard train operation at GoA 1 (Grade of Automation), allowing the ATO system to rely on its safety features and focus on the additional risks associated with autonomous control at higher GoA levels. However, the key factor is to ensure a secure connection between the ATO and the ETCS in accordance with the applicable standards. This paper should contribute to a better understanding of the links between the ATO and the ETCS. It also provides important information for the further development of autonomous railway systems.

Keywords: *Automatic Train Operation, Automatic Train Protection, Autonomous Train, Grade of Automation, Rail Transport, Railway Safety, RAMS*

1. Introduction

The automation of rail transportation stands for a major technological shift aimed at increasing the efficiency, reliability, and safety of rail operations. The concept of Automatic Train Operation (ATO), especially at higher levels of automation (GoA 3 and GoA 4), has the potential to fundamentally change rail transport by enabling driverless operation while supporting or even improving current safety standards. However, the implementation of autonomous driving poses significant challenges in terms of safety assurance, system integration and risk management. This transition is not only a technical challenge but also a legislative and safety challenge, especially when moving from urban rail systems, where autonomous driving is already implemented, to conventional lines, which have more complex infrastructure and conditions.

In recent years, autonomous train control has become a key element in the modernization of rail transport, promising to improve the efficiency, safety, and reliability of rail operations. While autonomous systems have already found successful applications in urban railway systems defined by the Urban Guided Transport Management System (UGTMS) standard [1], their transition to conventional railways with heterogeneous conditions poses a major challenge. While urban systems are characterized by stable conditions, conventional lines are affected by factors such as level crossings, diverse infrastructure, or mixed traffic, which place high demands on adapting safety and control systems.

The integration of advanced technologies such as Automatic Train Operation (ATO) and the European Train Control System (ETCS) is a key element for implementing autonomous train control while supporting the necessary interoperability and safety. Although these technologies cover major areas of control, conducting a thorough safety assessment of the level of autonomous operation on conventional lines is necessary, where operations are often more complex and involve higher risks.

Current regulatory requirements require that any autonomous driving technology has clearly defined safety aims that must be proved by both quantitative and qualitative methods. In the context of autonomous operation on conventional lines with automation levels GoA 3 and GoA 4, it is crucial to adapt proven safety management principles from urban systems to open rail infrastructure. This adaptation includes not only the correct definition of safety requirements but also the definition of processes and criteria that allow independent verification and validation of these requirements.

ETCS is a standardized European system of automatic train protection aimed at improving the safety and interoperability of rail transport. ETCS is gradually replacing older national signaling systems and provides automatic control of speed limits, Movement Authority, and activation of emergency braking in case of safety hazards. [2]

ETCS consists of two main parts:

- ETCS Trackside - holds trackside sensors, signaling equipment and train communication systems.
- ETCS On-Board Unit (OBU) - an on-board unit on the train that evaluates received signals and controls the train's response in real time.

ETCS is divided into two application levels (L1 and L2) that decide how the train and track communicate with the higher levels, allowing the elimination of traditional track-side signals and fully digital control.

ATO (Automatic Train Operation) is a train control automation system that allows diverse levels of autonomy, from partial driving support to fully autonomous operation. ATO works in conjunction with ETCS, with ETCS providing basic safety functions and ATO optimizing operational aspects such as speed profiles, energy efficiency and timetable compliance. [3]

Train automation is classified into four main levels (GoA 0-4) according to UGTMS [1]:

- GoA 0 - Manual control by driver, no automation.
- GoA 1 - Automatic control of main functions (speed control, End of Authority), but the driver is still fully responsible for driving.
- GoA 2 - ATO automates starting, braking, and stopping, but the driver is still on board to supervise driving and respond to emergencies.
- GoA 3 - Fully automated operation without a driver but with on-board staff to deal with emergency situations.
- GoA 4 - Fully autonomous operation without any human presence on board.

GoA 3 and GoA 4 represent a major challenge for safety and reliability as all activities normally performed by the driver must be completely replaced by technology.

A key aspect of safe autonomous operation is the integration of the ATO with ETCS, an essential safety feature of modern rail networks. ETCS, as a standardized train protection system, provides key safety functions such as granting movement authority, speed supervision and activation of emergency braking. Its role in the safety of conventional and high-speed rail is essential, and therefore, there is an opportunity to use its safety mechanisms for autonomous train operation.

In the context of railway automation, it seems helpful to use the safety guarantees of the ETCS system for ATO operation. As ETCS already ensures the safe operation of driver-controlled trains (GoA 1), the question arises whether its safety principles and data structures can be extended to higher levels of automation without the need for added redundant safety layers. To answer this question, it is necessary to analyze the specific safety functions of ETCS and their applicability to ATO. ETCS offers a structured data exchange mechanism that includes:

- Static train data (train length, braking characteristics, traction capability),
- Dynamic data (Movement Authority, speed profiles, track gradients, localization, ETCS modes, traction status),
- Train braking capability information to ensure compliance with safety requirements.

The integration of ETCS with ATO relies on a secure communication interface whose specifications have been standardized by the European Railway Agency (ERA). This interface allows the exchange of twelve key data packets that enable the ATO to make real-time decisions based on validated and secure train operation data. Although ETCS provides a robust safety basis, it does not cover all aspects of autonomous driving, such as obstacle detection, precision platform stopping or energy optimization.

Tab. 1. List of packets [4]

Packet Number	Packet Name	Source	Sink	Transmitting cycle [ms]	Data Class	Timeout [ms]
0	ATO_ETCS_Status	ATO	ETCS	100	Process	1000
1	ATO_ETCS_DMI	ATO	ETCS	100	Process	1000
2	ATO_ETCS_Data_Entry_Need	ATO	ETCS	NA	Message	-
3	ATO_ETCS_Data_Entry_Request	ATO	ETCS	NA	Message	-
4	ATO_ETCS_Data_View_Values	ATO	ETCS	NA	Message	-
5	ETCS_ATO_Static	ETCS	ATO	1000	Process	3000
6	ETCS_ATO_Dynamic	ETCS	ATO	200	Process	1000
7	ETCS_ATO_Driver_Inputs	ETCS	ATO	100..200	Process	1000
8	ETCS_ATO_Data_Entry_Values	ETCS	ATO	NA	Message	-
9	ETCS_ATO_Data_Entry_Flag	ETCS	ATO	NA	Message	-
10	ETCS_ATO_Data_View_Values_Request	ETCS	ATO	NA	Message	-
11	ETCS_ATO_BRAKE_DECELERATIONS	ETCS	ATO	200	Process	1000

Table 1 presents the twelve packets transmitted between ATO and ETCS, each of which is specified in detail in the relevant documentation. Each packet has several variables carrying relevant data that allow the ATO system to retrieve key information from ETCS or to provide feedback on the data transfer towards ETCS. Packets can be divided into two categories: Process data and Message data. While message data is transmitted via TCP, process data uses the UDP protocol. Message data is primarily used for data retrieval or acknowledgement requests, while process data transmits the actual information necessary for the ATO to function in relation to the ETCS (or vice versa). The transmission of process data is strictly defined compared to messages. Each packet has not only the time of sending but also a timeout, which ensures the security of the transmitted information due to the limited time validity of the delivery. Similarly, the values of individual variables in packets can be limited by time validity. These measures allow the use of UDP instead of TCP for the transmission of process data without compromising the integrity and security of communication.

For ETCS, the ATO defines the Automatic Driving (AD) mode of operation for autonomous train control. This mode is only available provided that the ATO is fully operational at a given time and location and that the transition is from Full Supervision (FS) mode. FS mode stands for the highest level of protection within ETCS, ensuring that the most stringent safety criteria that an ETCS

train protection system can guarantee are met during autonomous driving. Switching to AD mode requires confirmation by the driver, who can also take back control at any time. [1]

This paper is crucial because it focuses on one of the most critical aspects of implementing autonomous train control on conventional lines. Namely, it is the interconnection between the train protection and the autonomous control system. The efficient and safe integration of these two systems is essential to ensure the smooth and safe operation of trains in the high-risk and high-variability conditions that exist on conventional lines. This paper provides a detailed assessment of the technological, safety and regulatory challenges associated with the integration of these systems, which is key to achieving the desired level of safety and efficiency in autonomous driving. The aim is thus to contribute to the development of methodologies and standards that will enable the smooth integration of autonomous systems into real rail operations.

2. Objectives

The aim of this article is to analyze the possibilities of using the level of security provided by Automatic Train Protection (ATP) as a basis for autonomous train control via Automatic Train Operation (ATO). The key question is whether the safety mechanisms of the European Train Control System (ETCS) can be reliably used for autonomous operation and, if so, under what conditions.

This research investigates the requirements of the ATO system for functions that make use of the data and safety measures provided by ETCS. The main requirements include:

- Ensuring safe stopping at a specifically defined location according to operational requirements.
- Compliance with the timetable within the travel options set by the train protection system.
- Optimization of the running speed with respect to efficient traction consumption, the maximum speed being limited to the values defined by ETCS.
- Safe execution of the clearance sequence, for example door opening, only after all safety conditions defined by ETCS have been met. [5]

The following figure provides better clarity on the link to be analyzed within the ETCS/ATO logical structure.

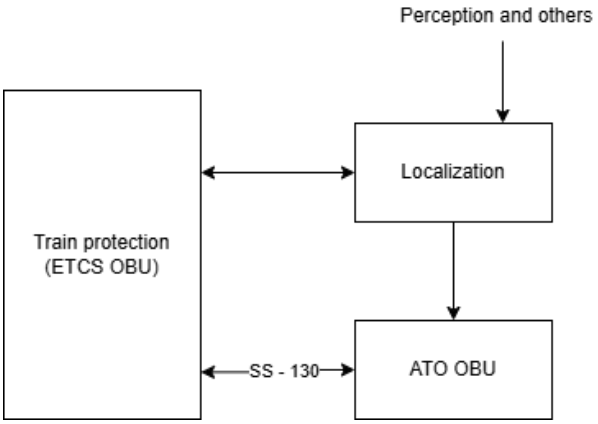

Fig. 1. Cutout from the logical structure of ETCS/ATO OBU (Adapted from [6])

'Fig. 1' shows, among other things, our two essential elements for examining the given bond. These are Train Protection and ATO OBU. These elements are embedded in the cutout from the logical architecture in this image. Their connecting link is essential for this post. It is labelled SS-130, which refers to the specification that describes the link. [4]

From the point of view of interoperability between ATO and ETCS, it is necessary to analyze the specific data transmitted and used between these systems. The ETCS-OB (ETCS On-Board Unit) transmits the following information to the ATO-OB (ATO On-Board Unit):

ETCS Train Data:

- Train Category
- Train Length
- Traction and Braking Parameters (Brake Percentages, Brake Positions)
- Maximum Train Speed
- Axle Load Category

ETCS Additional Data:

- Driver ID
- Train Number [3]

These data are critical inputs to the ATO control and affect its ability to control the train safely and efficiently in autonomous mode. Therefore, this paper focuses on the following questions:

- Can the data provided by ETCS be relied upon in an ATO system?
- Is the information transmitted from ETCS sufficiently verified and validated?
- What mechanisms ensure their correctness and timeliness?
- How is the transfer and validation of this data between the ETCS and the ATO conducted?

These questions are essential to figure out whether the safety measures in place for ATP can be considered credible for autonomous operation or whether modifications or additions to the safety mechanisms are necessary. The results of this analysis can contribute to the further development of autonomous train control and its effective integration with existing safety systems on the railway.

3. Methods

3.1 Demonstration of Reliability, Availability, and Maintainability

The RAMS (Reliability, Availability, Maintainability, Safety) methodology is a structured approach to safety assessment for the integration of ETCS (European Train Control System) with ATO (Automatic Train Operation). With risk analysis and interoperability assurance, it can be assessed whether ETCS provides sufficient safety guarantees for autonomous railway operation. [7]

The actual analysis of ETCS compliance with RAMS requirements according to EN 50126 and related standards is not part of this paper. However, ETCS can already be considered as a safe system that meets these standards. Several risk and safety analyses have been conducted in the past following the RAMS methodology, and the results have confirmed that ETCS meets the high safety requirements for rail transport. Today, ETCS is a commonly used signaling system on a significant part of the European rail network, and there are extensive studies confirming its safety. [8]

Individual ETCS elements should meet the requirements of SIL4 (Safety Integrity Level 4), the highest level of safety integrity in the railway sector. Below is how ETCS fulfils the different components of the RAM methodology:

Reliability - ETCS is designed to be an exceptionally reliable train protection system that aims to minimize the probability of critical functions failing. Redundant safety mechanisms, such as multi-level data authentication and continuous communication between the train and the track infrastructure, ensure that the train receives exact and up-to-date instructions. ETCS hardware and software components are subject to stringent certification processes and meet SIL4, which guarantees an extremely low probability of failure leading to an accident.

Availability - ETCS is designed to maximize the availability of railway operations, i.e., minimizing unplanned outages caused by faults. Thanks to the modular architecture and the implementation of hot-standby redundancy in key elements (e.g., GSM-R radio communication, packet sensors), the system can continue to work even if some components fail. In addition, the dynamic allocation of Movement Authority enables more efficient use of line ability, thus contributing to the smoothness of rail traffic.

Maintainability - ETCS is designed as an easy-to-maintain system, which reduces operating costs and intervention times. Remote diagnostics and monitoring allow early detection of potential faults, thus avoiding serious operational complications. The standardized architecture of ETCS enables rapid replacement of faulty modules, helping maintenance and upgrades without the need for extensive infrastructure modifications.

Based on the available studies, it can be concluded that ETCS meets the highest safety standards, as confirmed by the expert analysis conducted so far. However, the RAMS methodology must also be applied to the interface between ETCS and ATO systems.

The standards allow the adoption of existing safety features, provided that the risks corresponding to the subsystem are sufficiently reduced and there is a safe interconnection between ETCS and ATO. This interconnection is detailed in Subset 130, which defines the communication standards between the ETCS On-board Unit and the ATO On-board Unit.

A closer examination of the physical layer of the ETCS/ATO interface shows that the system uses standardized IEEE 802.3 (Ethernet) [9]. According to expert studies, the Ethernet link can be considered as SIL3, which is a reduction in security level compared to SIL4. Still, this reduction is compensated by added security measures at the network layer. [10]

Each data packet transmitted between the ETCS and the ATO requires feedback acknowledgement and acceptance of new data. This mechanism ensures that mistaken or incorrect data cannot be processed. If the data transmission were to be disrupted, the packet would not be acknowledged by the terminal equipment, which would automatically trigger the retransmission request algorithm. This principle ensures a prominent level of communication integrity between ETCS and the ATO.

ETCS meets the requirements of the RAMS methodology and is a highly dependable, available, easy to keep and safe system for rail transport. Its integration with ATO does not require further security analysis at the level of the communication interface while ensuring a proper level of security integrity in the data transfer between the systems.

3.2 Common Interface Task from Systems Engineering Theory

To verify the correctness of the link between the ETCS on-board part and the ATO on-board part, the system engineering method ‘Common Interface Task’ was used. [11] This two-way link ‘Fig. 1’ between ETCS as Train Protection and ATO as ATO OBU can be seen as a feedback link between ATO and ETCS in the interface analysis. We have pairs of message data, which usually trigger some data requests, and then I have pairs of process data, which send those variables to us.

In this interface, the ETCS can be described as a superior system to the ATO, which means that the ETCS primarily figures out the correct behavior of the ATO. When analyzing the data transmission between these systems in detail, the packets transmitted can be sequenced: pairs of message data packets to start the transmission of pairs of process data. These (table 2) pairs of packets can be seen as an ETCS action with an ATO response for this analysis.

Tab. 2. Pairs of packets

OUT	IN
ETCS_ATO_Static	ATO_ETCS_Status
ETCS_ATO_Dynamic	ATO_ETCS_Status
ETCS_ATO_BRAKE_DECELERATIONS	ATO_ETCS_Status
ETCS_ATO_Driver_Inputs	ATO_ETCS_DMI
ETCS_ATO_Data_Entry_Values	ATO_ETCS_Data_View_Values
ETCS_ATO_Data_Entry_Flag	ATO_ETCS_Data_Entry_Need
ETCS_ATO_Data_View_Values_Request	ATO_ETCS_Data_Entry_Request

Each transmission packet is characterized by three basic parameters (table 1):

- Transmitting cycle
- Data Class
- Timeout

Thus, the system output is figured out by these three parameters for packets from the ETCS. The input values for ATO packets are processed according to the same set of parameters. This sets up the first level of the common interface task.

Second level - Integrity conditions define the rules that the transmission link between the ETCS and the ATO must satisfy to achieve secure and consistent communication. The regularity conditions can be described verbally as follows:

- The ATO response packet to an ETCS message must have the same Data Class.
- Transmitting cycle and the largest timeout shall be greater than or equal to the response.
- Each packet holds specific data and information, which is then checked for compliance with these rules.

$$Out\ (Data\ Class) = In\ (Data\ Class)$$
$$Out\ (Transmitting\ cycle) \geq In\ (Transmitting\ cycle)$$
$$Out\ (Timeout) \geq In\ (Timeout)$$

Level Three - Removal of Partial Irregularities. Level Three addresses the removal of any irregularities in data transmission. The current system, as designed, does not have any identified irregularities. However, as part of the development and testing of the autonomous driving system, conversion elements have been defined to allow the adaptation of the information transmitted between the different subsystems.

For example, the ATO takes over the train location information, which is primarily derived from the balise data (ETCS task). However, the train location is also compared with the Perception data, which ensures higher accuracy and redundancy. Therefore, a conversion element is created in the ERTMS/ATO super-system architecture in the form of a separate Localization element – 'Fig. 1'.

Level four - Integrated Interface. The last step of the analysis is to assess whether the binding can be classified as an integrated interface. This status is achieved if all regularity conditions have been met, and any irregularities have been found and removed.

If these conditions are met, it can be concluded that the link between ETCS and ATO meets the integrity requirements from a system engineering perspective.

4. Results of putting the ETCS/ATO link into the context of autonomous rail transport

Communication between ETCS and ATO is implemented through a defined interface, with ETCS serving as the overarching system that sets safety limits and provides key data relating to infrastructure and track conditions. The ATO receives this data and uses it to refine train operation, always respecting the constraints set by ETCS. From a technical point of view, communication between the two systems is ensured by the protocols specified in Subset 130 [4], the physical layer being standard Ethernet. Although Ethernet may have a lower level of security than some other technologies, the bi-directional data transmission verification mechanisms in ETCS and ATO ensure the integrity of the data transmitted and a sufficient level of security.

A single train protection system, ETCS, is already in place within the European rail infrastructure, providing safety supervision of train movements and enabling interoperability between countries. Any introduction of autonomous driving on this infrastructure must be designed to be compatible with ETCS and follow the safety rules laid down. In this context, ATO Autonomous Control acts as a superstructure over ETCS, emphasizing integration to ensure both compatibility and safety of the entire system. [12]

In contrast, urban rail systems such as metro and trams use different train control systems that are not uniformly standardized. These systems, known collectively as CBTC (Communication-Based Train Control), allow a high degree of flexibility and adaptation to the specific needs of individual urban networks. In Europe, these systems are categorized by UGTMS (Urban Guided Transport Management and Command/Control Systems) [1], which include not only ATP (Automatic Train Protection) signaling but also ATO and ATS (Automatic Train Supervision) timetable planning. This integrated ATC (Automatic Train Control) system enables fully automated operation, which, in effect, cuts the need for an external ATP system such as ETCS. With this flexibility, urban systems can achieve higher levels of automation, including fully unattended operation at GoA Level 4.

Compared to urban rail systems, where autonomous control can be explicitly implemented in an integrated control system [13], in conventional rail transport, the autonomous functions must be adapted to the existing ETCS signaling system. This difference is due to the requirements for interoperability and safety, which are of prime importance in rail transport due to the international nature of the railway infrastructure and its long service life. The development of autonomous trains on conventional railways therefore presents a complex challenge not only in terms of technology but also in terms of certification and regulatory framework. Unlike urban systems, new autonomous technologies must be precisely aligned with already set up and strictly regulated safety standards.

The combination of ETCS and ATO fits into the Railway 4.0 concept [14], which is an approach to digitization and automation of rail transport that uses advanced technologies to improve efficiency, safety, and interoperability. This approach includes upgrading infrastructure, deploying fiber optic and power lines, digitizing control and security and centralizing operations through control centers. A key part of Railway 4.0 is the integration of autonomous ATO control into rail operations. Combined with ETCS, ATO enables diverse levels of automation (GoA - Grade of Automation) to be achieved, with the potential to achieve fully autonomous operation (GoA 4) through gradual development.

In terms of safety requirements, autonomous rail transport is governed by RAMS standards, which set out requirements for reliability, availability, maintainability, and safety of systems. Each element of the interconnection between ETCS and ATO must meet the strict RAMS standards to ensure not only efficient but also safe and reliable operation. The results of this paper suggest that safety guarantees can be adopted by ETCS that already meet safety requirements following standards addressing RAMS. However, it is essential to have a clear, assured link between the autonomous control systems and the train protection system represented by ETCS in Europe. The train protection system provides us with GoA 1, and the ATO superstructure systems will increase this level from GoA 2 to GoA 4. If we can take safety guarantees from the systems already in place and transfer them to the superstructure systems, this will accelerate the progress of automation many times over on conventional rail, where autonomous driving is more of a problem than on urban rail, which is already reaching GoA 4 in some areas of the world. [15]

5. Conclusion

Autonomous train control combined with ETCS stands for a major step forward in the modernization of rail transport. This integration not only allows for increased safety and operational efficiency but also optimizes driving parameters to minimize energy consumption and improve traffic flow. The use of ETCS as a single European standard for railway safety enables seamless interoperability between different transport systems and ensures reliable train control even in autonomous mode. A key factor for the successful implementation of ATO based on ETCS is the reliability and stability of the communication interface between the two technologies. ETCS provides exact and real-time updated information on track conditions, allowing the ATO to react efficiently to

changes in traffic and ensure the safety of train drive. This constructive interaction contributes to increased line ability and allows a higher level of automation without compromising operational safety.

Security is a key aspect of this technological transformation. ETCS minimizes the risk of human error through advanced safety features such as continuous monitoring of train position, speed limits and signal aspects. This data is shared in real time with the Autonomous Train Operation (ATO), which can react reliably to any changes in operating conditions. In addition, the ATO, together with ETCS, enables the use of dynamic braking curves and predictive control, reducing the risk of emergency situations and ensuring smooth and safe operation. The link between ETCS and ATO is designed with an emphasis on safety protocols, ensuring a prominent level of reliability. In case of failure of any part of the ATO over the ETCS system, the train automatically applies emergency brakes, cutting the possibility of a crash or other safety incident. This mechanism provides a robust basis for autonomous driving. It allows rail operators to rely on fully automated systems without compromising safety. Experience from projects to date shows that introducing this combination of technologies leads to significant operational benefits. These include reduced journey times, reduced operating costs and improved timetable accuracy. In addition, the influence of the human factor on train control is reduced, reducing the risk of errors and potential incidents.

Further improvements in autonomous train control can be expected as technology advances. The continuous improvement of algorithms for predicting driving conditions, the increasing accuracy of location systems and the development of digital communication platforms will further strengthen the reliability of this technology. The integration of ATO and ETCS is thus becoming not only a promising but inevitable direction for the future of European rail transport. In view of these advantages and the positive experience to date, it can be confidently said that the combination of autonomous control and advanced security in the form of ETCS L2 forms a solid basis for modern railway operations. This technology not only allows for increased efficiency and safety but also supports the environmental sustainability and competitiveness of rail transport within the wider transport system. Thanks to the emphasis on safety, passengers can rely on the prominent level of protection provided by this technological symbiosis, thereby strengthening confidence in public rail transport as a reliable and safe means of transport. Therefore, the introduction of this technology stands for not only the modernization of rail transport but also a strategic step towards its future development.

Acknowledgements

This work was supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS25/104/OHK2/2T/16.

References

1. IEC 62290-1:2014, “Railway Applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts,” (CENELEC, 2014).
2. European Union Agency for Railways SUBSET-026, “ERTMS/ETCS – System Requirements Specification,” (UNISIG, 2023).
3. European Union Agency for Railways SUBSET-125, “ERTMS/ATO – System Requirements Specification,” (UNISIG, 2023).
4. European Union Agency for Railways SUBSET-130, “ERTMS/ATO – ATO-OB / ETCS-OB FFFIS Application Layer,” (UNISIG, 2023).
5. Z. Wang, E. Quaglietta, M. G. P. Bartholomeus, and R. M. P. Goverde, “Assessment of architectures for Automatic Train Operation driving functions,” vol. 24, 2022, doi: 10.1016/j.jrtpm.2022.100352.
6. X2Rail-4, “Deliverable D3.2 GoA3/4 Specification:” Dec. 2021, p. 31. Accessed: Apr. 01, 2025. [Online]. Available: https://voie-libre.com/wp-content/uploads/2023/01/X2R4-WP13-D-ALS-015-02_-_D3.2_WP3_GoA34_Specification_v0.1.0ter.pdf
7. EN 50126-2:2017, “Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety,” (CENELEC, 2017).
8. M. Sallak, S. Destercke, W. Schon, F. Vanderhaegen, D. Berdjag, and C. Simon, “Uncertainty, elicitation of experts' opinion, and human failures: Challenges for RAM analysis of ERTMS SoS,” 2015 10th System of Systems Engineering Conference (SoSE), 2015, doi: 10.1109/SYSOSE.2015.7151917.
9. 802.3.2-2019, “Standard for Ethernet,” (IEEE, 2019).
10. F. Zezulka and O. Hynčica, “Průmyslový Ethernet V: Bezpečná komunikace po Ethernetu,” Automa, vol. 13, no. 12, 2007, Accessed: Apr. 01, 2025. [Online]. Available: https://automa.cz/Aton/FileRepository/pdf_articles/36338.pdf
11. J. Vlček, “Úlohy systémového inženýrství,” in Systémové Inženýrství, 2010 ed., (CTU, Prague, 1999), pp. 84-85
12. E. Jansson, N. O. E. Olsson, and O. Fröidh, “Challenges of replacing train drivers in driverless and unattended railway mainline systems—A Swedish case study on delay logs descriptions,” Transportation Research Interdisciplinary Perspectives, vol. 21, 2023, doi: 10.1016/j.trip.2023.100875.
13. M. Vaniš, M. Horák, T. Tichý, Z. Lokaj, M. Malý, and J. Brož, “Autonomous Trams and Urban Infrastructure: A Methodological Approach to Testing and Integration,” 2024 Smart City Symposium Prague (SCSP), May 2024, doi: 10.1109/SCSP61506.2024.10552728.
14. M. Leso, “The Railway 4.0 Concept – the vision of a digital railway in the Czech Republic (CR),” Acta Polytechnica CTU Proceedings, vol. 35, May 2022, doi: 10.14311/APP.2022.35.0027.
15. A. Tonk, M. Chelouati, A. Boussif, J. Beugin, and M. E. Koursi, “A safety assurance methodology for autonomous trains,” Transportation Research Procedia, vol. 72, 2023, doi: 10.1016/j.trpro.2023.11.849.