Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
©2025 ESREL SRA-E 2025 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P2345-cd

Towards applying STPA to autonomous railway systems – a hierarchical safety control structure for GoA2 train operations

Abhimanyu Tonk[a], Abderraouf Boussif[a,b], El-Miloudi El-Koursi[a,b]

[a] *IRT Railenium, 180 rue Joseph-Louis Lagrange, Valenciennes, F-59300, France*
[b] *Univ. Gustave Eiffel, COSYS-ESTAS, 20 rue Élisée Reclus, Villeneuve d'Ascq, F-59650, France*
E-mail: abhimanyu.tonk@railenium.eu, {abderraouf.boussif, el-miloudi.el-koursi}@univ-eiffel.fr

A key element of Systems-Theoretic Process Analysis (STPA) method is its hierarchical safety control structure (HSCS), which defines how safety constraints have to be enforced within the system. In fact, any hazard analysis conducted using the STPA approach is only as effective as the quality of its underlying control structure. To pave the way for the application of STPA in autonomous railway systems, this paper proposes a HSCS for semi-automated train operations in European railways. The design is based on input data derived from European railway system requirements, functional and technical architectures of subsystems, and a comprehensive review of existing research works in the domain. This structure clarifies the control relationships (controllers and controlled processes) between diverse technical and operational actors, and defines the associated information flows. Starting from this HSCS, it is then possible to effectively perform the remain steps of STPA process (i.e., identifying unsafe control actions and determining loss scenarios).

Keywords: Autonomous railway systems, Railway safety, Systems-Theoretic Process Analysis (STPA), Hierarchical safety control structure, Railway automation

1. Introduction

Early adoption of automation technologies significantly influenced the evolution of railway systems (Clark, 2012). Incremental technological enhancements, such as advanced signaling and protection systems, maximized the exploitation of rail-based transportation. Particularly, the automation of driving tasks within urban rail transit demonstrably augmented network capacity, improved energy efficiency, and reduced operational costs (Cohen et al., 2015). These advantages pushed the railway industry to extend such advanced technologies to mainline and high-speed operations.

In Europe, driverless train operations aim to substantially transform mainline railways. However, beyond regulatory and technical challenges, full automation introduces safety concerns at each hierarchical level (regulatory, organizational, operational and technical) of the railway system (Singh et al., 2021). The railway domain has an immutable principle: *it is forbidden to degrade its safety level*. To this principle is added a second imposed by Europe: *it is forbidden to curb the interoperability of networks* (Cebulski, 2020). To meet these principles, the introduction of new products, services, procedures, and / or technologies into the railway system must be supported by a body of evidence (through safety/risk studies) that demonstrates that the overall level of safety (for users, operating staff, and third parties) is globally at least equivalent to the current level (Boussif et al., 2023).

Traditional hazard and safety analysis methods such as FMECA and FTA focus on hazards arising from component failures or simple combinations thereof (Barnatt and Jack, 2018). These methods are inadequate for addressing the complex nonlinear interactions and dependencies typical of automated sociotechnical systems (Hollnagel, 2004). Thus, more sophisticated and systemic approaches capable of analyzing such dynamic systems are required.

Systems-Theoretic Process Analysis (STPA) has emerged as a holistic approach for analyzing hazard and safety. Unlike traditional methods, STPA focuses on systemic interactions and potential control deficiencies (Ejaz and Chikonde, 2022). STPA examines how inadequate control actions, feedback loops, and safety constraints operate and potentially fail across an entire system's hierarchy. Demonstrated to be highly effective in various safety-critical industries, STPA is increasingly recognized as an efficient tool for addressing the complex safety challenges presented by autonomous systems (Dghaym et al., 2021; Abdulkhaleq et al., 2017).

According to the STPA handbook (Leveson and Thomas, 2018), a *Hierarchical Safety Control Structure (HSCS)* is essential, as the approach relies on identifying inadequate control scenarios that could lead to the hazards. Consequently, the effectiveness of any STPA analysis is directly dependent on the quality and completeness of its safety control structure. As highlighted in (Chaal et al., 2020; Glomsrud and Xie, 2019), the absence of detailed information about the control structure remains a significant challenge in applying STPA to autonomous systems.

In a previous paper (Tonk and Boussif, 2024), we reviewed the application of STPA in the railway domain, and analyzed various comparisons between STPA and existing approaches. This review highlighted the key aspects of STPA and the importance of a well-defined HSCS for hazard and safety analysis. These elements are essential for safety assurance activities at the overall system level for autonomous train operations (Tonk et al., 2023). Recognizing this necessity and inspired by similar research efforts (Allison et al., 2017; Chaal et al., 2020) in other transportation domains, our objective to address this gap by advancing the development of a railway-specific HSCS serving as a foundation for the future application of STPA for automated railway systems. In this paper, we propose a hierarchical safety control structure for semi-automated (GoA2) train operations in European railways. This structure clarifies the control relationships (controllers and controlled processes) among various technical and operational actors while defining the corresponding information flows. The design is based on insights derived from European railway system requirements, functional and technical architectures of subsystems, and a comprehensive review of existing peer-reviewed research in this domain.

The remainder of this paper is organized as follows: Section 2 discusses the foundations of STPA and HSCS. Section 3 introduces the technicalities of the interoperable European railway system and automation. Then, Section 4 presents the methodology and main contribution of the paper, that is, the HSCS for GoA2 autonomous trains. Finally, Section 5 provides a brief discussion with concluding remarks and perspectives.

2. STPA & Hierarchical safety control structure

STPA is a proactive hazard analysis method based on *Systems Theoretic Accident Model and Processes (STAMP)* accident model rooted in systems and control theories. Based on systems' theory, safety is considered as an emergent property that evolves as the result of a dynamic outcome of complex interactions within systems. STPA considers the management of this property as a control problem within a sociotechnical framework, where a dedicated control structure enforces safety constraints to control system behavior (Leveson, 2004, 2012) .

The STPA Handbook (Leveson and Thomas, 2018) presented four main steps to be carried out during the hazard analysis process:

(1) define the analysis purpose by identifying potential losses, the system's environment, and hazards at the system level, along with constraints;
(2) establish a HSCS to detail functional relationships and interactions, including feedback control loops;
(3) examine control actions to pinpoint potential unsafe actions that could cause losses under specific environmental conditions;
(4) identify causal factors and scenarios that could lead to these unsafe actions and subsequent hazards.

Clearly, the STPA process requires a HSCS of the system which captures the functional relationships through feedback control loops. A typical HSCS is organized across five hierarchical levels: (1) *Congress & Legislatures* (2) *Regulatory*, (3) *Company Management*, (4) *Operations Management*, and (5) *Operating Process* (Leveson, 2018).

At the operating process level, the HSCS is a representation of operational and technical components, including both human and automated systems, interacting with actuators and sensors to control a physical process, see Fig. 1.

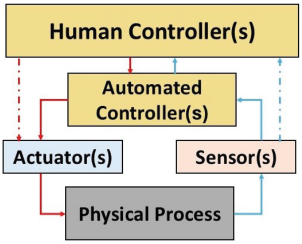


Fig. 1. General control structure – operating process.

3. European railway and automation

All railway systems around the globe are designed to operate two physical components: the infrastructure (tracks, switches, signals, etc.) and the rolling stock. The infrastructure is a static and fixed component, while the rolling stock is the mobile component which is designed to move along the rails, providing mobility for passengers and freight. Within the *Single European Railway Area (SERA)*, rolling stock can operate over infrastructure established by different European Union (EU) states, a principle referred under the Interoperability Directive[a].

The considered directive establishes conditions for achieving interoperability within the Union rail system, specifying essential requirements for subsystems including components, interfaces, procedures, and system compatibility. Established for regulating accessibility and safety of cross-border railway operations within EU, this directive organizes the technical operations of the railway system into eight subsystems, categorized into structural (Infrastructure, Energy, Trackside Control Command and Signaling (CCS), On-board CCS, and rolling stock) and functional (operation and traffic management, maintenance, and telematics applications for passenger and freight services) groups. These subsystems are designed and operated with respect to Technical specifications for interoperability[b] (TSIs), which aim to harmonize technical standards across the European rail network. The automation of train driving functions is mainly realized using both trackside and on-board components of the railway CCS subsystem, as discussed in section 3.1.

3.1. *Automation in railway*

The automation of train driving functions started in the urban rail transit domain. The IEC622901 (2014) describes *Grade of Automation (GoA)* as the *"automation level of train operation, in which a train can be operated, resulting from sharing responsibility for given basic functions of train operation between operations staff and electronic/electrical system"*. The GoA allocates the responsibility for several basic functions to either on-board staff or technical systems, such as train operation, train speed control, train stopping, train door control and disruption management.

In urban rail transit domain, the automation is implemented through the concept of *automatic train control* (ATC). The ATC comprises three subsystems, *Automatic Train Protection* (ATP), *Automatic Train Operation* (ATO), and *Automatic Train Supervision* (ATS), which reflect the progressive automation of the safety functions, driving operations, and traffic management, respectively. One of the successful implementations and integration of ATC system, in urban railways, is the Communication-based Train Control (CBTC) system.

In European mainline and high-speed railways, the automation is mainly implemented within the the European Rail Traffic Management System (ERTMS), as part of CCS. ERTMS is a signaling and speed control system which is composed of three subsystems: European Train Control System (ETCS), Railway Mobile Radio (RMR)[c] and Automated Train Operation (ATO). Similarly to the urban rail systems, the functions of ATS are performed by a so-called Traffic Management System

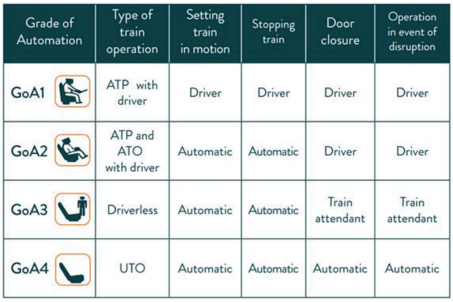
[a] Directive (EU) 2016/797 on the interoperability of the rail system within the EU

[b] Introduction to Technical specifications for interoperability

[c] Notice that RMR consists of both Global System for Mobile Communications-Railway (GSM-R) and Future Railway Mobile Communication System (FRMCS), implemented simultaneously or independently.

(TMS). The ETCS is a safety-critical ATP system, while ATO is optional and enhances functionality across GoAs. Concurrently, RMR provides voice communication for train drivers and signalers, and data transmission for ETCS.

In mainline railways, the concept of GoA serves as a taxonomy for categorizing the transfer of train driving authority from human operators to technical systems. This taxonomy is essential for understanding and standardizing the varying levels of technical automation within the railway sector (Brandenburger and Naumann, 2019). The ERTMS/ATO Operational Principles' specification (ERA UNISIG, 2023) distributes the different responsibilities of train driving functions between human and technical systems across all GoA's (see Fig. 2).



Grade of Automation	Type of train operation	Setting train in motion	Stopping train	Door closure	Operation in event of disruption
GoA1	ATP with driver	Driver	Driver	Driver	Driver
GoA2	ATP and ATO with driver	Automatic	Automatic	Driver	Driver
GoA3	Driverless	Automatic	Automatic	Train attendant	Train attendant
GoA4	UTO	Automatic	Automatic	Automatic	Automatic

Fig. 2. Grade of Automation levels (UITP, 2018).

In GoA1, the driver plays a central role, guided by ATP (ETCS or national systems) and supported by TMS and Train Management (TM). Optional Driver Advisory Systems (DAS) can augment this setup by providing optimal speed and timing advice to enhance efficiency.

GoA2 introduces the ATO (both on-board and trackside) system that automatically handles driving tasks such as traction and braking, closely interacting with TMS to synchronize train movements with the operational timetable and manage traffic effectively. The ATO system may also compute DAS trajectories, which can be displayed as guidance for the driver in GoA1 scenarios.

In GoA3 and GoA4, complexity increases as the ATO system begins to interact not only with TMS, but also with train management to automate daily railway operations, such as train configurations and staff management. GoA4 represents the pinnacle of automation, where all driving and on-board tasks are fully automated, eliminating the need for any on-board staff, contrasting with GoA3 where some staff roles are retained.

Train operations in both GoA3/4 modes require advanced technologies (integrated with ATO) to ensure safe operations; this includes, but is not limited to, perception system, obstacle detection, digital mapping, localization, and emergency management. Thus, ensuring that the system can operate safely and efficiently without human intervention. Finally, we recall that our focus in this paper is on the railway components involved in the GoA2 train operating process and their systemic interactions.

4. Railway HSCS for GoA2

An HSCS consists of controlling units (controllers), the controlled process, and the flow of control actions and feedback between them (Rejzek et al., 2018). In railways, HSCS components include human operators and technical systems, working in collaboration or assistance to perform a set of functions relevant to train operations. In this section, we establish an initial HSCS for GoA2 train operations within the European railway system.

The HSCS established in this work focuses on systemic interactions related to train driving operations, along with their underlying system hierarchy and interactions. Notice that both the human operator (i.e., train driver) and the technical system (i.e., ATO) are jointly involved in driving operations.

4.1. *Methodology*

From the literature, Chaal et al. (2019) have established a method for developing a hierarchical system structure for the (future) autonomous maritime systems, starting from functional specifications. Inspired by this work and recognizing the particularities of the European railway system, we present our two-step methodology used to establish the HSCS of the railway, illustrated in Fig. 3, as follows.

Step 1 involves gathering information from three primary sources:

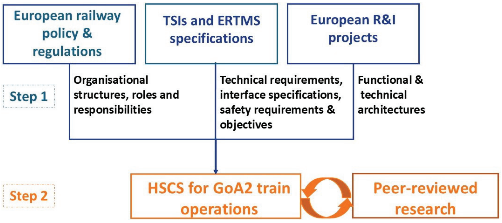

European railway policy & regulations
TSIs and ERTMS specifications
European R&I projects
Step 1
Organisational structures, roles and responsibilities
Technical requirements, interface specifications, safety requirements & objectives
Functional & technical architectures
Step 2
HSCS for GoA2 train operations
Peer-reviewed research

Fig. 3. Methodological approach used to develop the HSCS.

(1) ***European railway policies and regulations***, which provide information on the organizational structure of the system, including administrative bodies, regulatory authorities, and railway companies. They define the roles, responsibilities, and interactions of these entities, which are crucial for governance and decision-making within the HSCS.

(2) ***TSIs and ERTMS specifications***, which define the technical and operational standards required to meet essential requirements (mainly safety) and ensure interoperability. Most importantly for our work, they outline the interfaces and interactions between these subsystems and their underlying components (see Fig. 4). This information is fundamental to defining the control actions and feedback loops within the operational and technical layers of the HSCS.

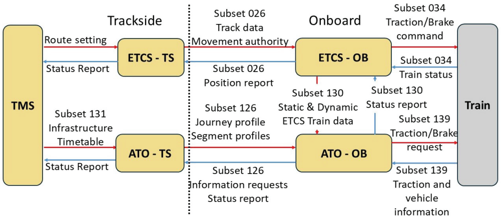


Fig. 4. ATO over ETCS reference architecture (Wang et al., 2022).

(3) ***European R&I projects***, which propose specifications for future standardization, focusing on defining the functional and technical architectures of automated railway systems. For example, the "X2Rail-1" project detailed the essential functionalities, interfaces, and system specifications of an interoperable GoA2 train control system. Ongoing reviews of ATO over ETCS GoA3/4 specifications in the "X2Rail-4" project will lead to updated ERTMS / ATO specifications. Other projects, such as "OCORA," "TAURO," "MOTIONAL," "EULYNX," and "R2DATO," standardize technical aspects of various subsystems for safe GoA4 train operations. These architectures are transformed into control structures that represent the operational and technical layers of the system.

At the end of Step 1, a preliminary version of railway HSCS was developed based on a review of the aforementioned sources. In Step 2, this version was iteratively refined using insights from peer-reviewed studies, particularly on automatic train operations, STPA control structures, and safety of automated systems. We specifically acknowledge (Wang et al., 2022; Yin et al., 2017) for their contributions regarding ATO technology.

4.2. *The control structure*

Fig. 5 illustrates the high-level hierarchical safety control structure for GoA2 train operations. In the diagram, each yellow box represents a system component or human actor within the railway system. On the other hand, gray boxes represent the physical processes. Red lines indicate control actions or information transmissions, while blue ones represent feedback mechanisms. The controllers at the top of this diagram are part of the operation and traffic management (OTM). Notice that the trackside components are located on the left, and the on-board components are located towards the right of this diagram.

Starting from *Planning System*, long-term and advance timetables are shared with Infrastructure Manager's traffic dispatchers, such as *Operations Manager*, and *Railway Undertaking (RU) Supervisor*. *Operations manager* interact with *RU supervisor* who interact with *Train driver* via *Train management*. Together, the Operations Manager and the RU supervisor also provide status reports to the planning system when modifications are necessary.

During real-time operations, trains often deviate from their scheduled targets. Such disturbances and disruptions are managed by the *TMS* while optimizing the utilization of rail *infrastructure*. Previously, human *signalers* (as part of TMS) commanded *Interlocking* for route setting and trackside signaling, but this function has been successfully automated and is now managed by *Automatic Route Setting* commanded by a traffic dispatcher remotely.

The on-board and trackside components of the *CCS* (including ETCS and ATO) enable train drivers to command the train (that is, *rolling stock*) under the constraints of the railway schedule while maintaining safe distances from the preceding and following trains. Transmission between trackside and onboard components is facilitated through the ERTMS RMR system, except for trackside signaling observations, which, according to the ETCS application level, are performed visually by the train driver or communicated to the ETCS driver machine interface (refer ERA UNISIG (2016)).

Notice that Fig. 5 provides a high-level HSCS. In Fig. 6, we further detail the safety control structure described above by illustrating the systemic interactions involved between different components of the railway.

5. Discussion and Conclusion

This paper presents an HSCS specifically designed for semi-automated (GoA2) train operations within the context of European railways. The HSCS enables the tracing of distinct systemic interactions between human and automated controllers to facilitate GoA2 train driving-related functions. It also clarifies the system hierarchy, interfaces, control actions, and feedback mechanisms between these components.

The HSCS is established as a foundation for the effective application of the Systems-Theoretic Process Analysis (STPA) method in hazard and safety analysis of automated railway systems. It facilitates the final two steps of the STPA process: identifying unsafe control actions and loss scenarios. This enables the identification of potential unsafe control actions during GoA2 operations, such as mode confusion leading to human error on the part of the train driver.

In the future, this HSCS will be further enhanced by including railway components involved at non-technical hierarchical levels, as discussed in section 2. Additionally, our aim is to adapt the HSCS to support higher levels of automation, specifically GoA3 and GoA4. Once these extensions are completed, the enhanced HSCS will enable a more effective application of STPA, facilitating systematic identification of unsafe control actions and failure scenarios. This will be particularly important during GoA mode transitions in autonomous trains with dynamic autonomy. This, in turn, will support the derivation of appropriate safety constraints and requirements, contributing to the safety assurance of fully autonomous/ unattended (GoA4) train operations.

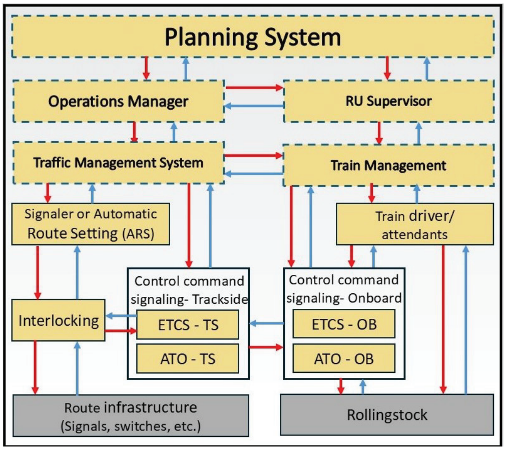

Planning System
Operations Manager
RU Supervisor
Traffic Management System
Train Management
Signaler or Automatic Route Setting (ARS)
Train driver/ attendants
Control command signaling- Trackside
Control command signaling- Onboard
Interlocking
ETCS - TS
ATO - TS
ETCS - OB
ATO - OB
Route infrastructure (Signals, switches, etc.)
Rollingstock

Fig. 5. Railway HSCS for GoA2 (semi-automated) train operations.

References

Abdulkhaleq, A., S. Wagner, D. Lammering, H. Boehmert, and P. Blueher (2017). Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. *Lecture Notes in Informatics (LNI) P-269*, 149–162.

Allison, C. K., K. M. Revell, R. Sears, and N. A. Stanton (2017). Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Safety Science 98*, 159–166.

Barnatt, N. and A. Jack (2018). Safety analysis in a modern railway setting. *Safety Science 110*, 177–182. Railway safety.

Boussif, A., A. Tonk, J. Beugin, and S. Collart Dutilleul (2023). Operational risk assessment of railway remote driving system. *Safety and Reliability 42*(2-3).

Brandenburger, N. and A. Naumann (2019). On Track: A Series of Research about the Effects of Increasing Railway Automation on the Train Driver. *14th IFAC Symposium on Analysis, Design, and Evaluation of HMS*.

Cebulski, L. (2020). Digital transformation of the rail sector: what impact on the regulator? *The International Railway Safety Council*, 01–06.

Chaal, M., O. Valdez Banda, S. Basnet, S. Hirdaris, and P. Kujala (2019). An initial hierarchical systems structure for systemic hazard analysis of autonomous ships. In *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC)*.

Chaal, M., O. A. Valdez Banda, J. A. Glomsrud, S. Basnet, S. Hirdaris, and P. Kujala (2020). A framework to model the STPA hierarchical control structure of an autonomous ship. *Safety Science 132*.

Clark, S. (2012). A history of railway signalling (from the Bobby to the Balise). In *IET Professional Development Course on Railway Signalling and Control Systems*, pp. 6–25.

Cohen, J. M., A. S. Barron, R. J. Anderson, and D. J. Graham (2015). Impacts of Unattended Train Operations on Productivity and Efficiency in Metropolitan Railways. *Transportation Research Record 2534*(1), 75–83.

Dghaym, D., T. S. Hoang, S. R. Turnock, M. Butler, J. Downes, and B. Pritchard (2021). An STPA-based formal composition framework for trustworthy autonomous maritime systems. *Safety Science 136*, 105139.

Ejaz, M. R. and M. Chikonde (2022). STPA for Autonomous Vehicle Safety in Traffic Systems.

ERA UNISIG (2016). ERTMS/ ETCS System Requirements Specification. REF: SUBSET-26, Issue: 4.0.0.

ERA UNISIG (2023). ERTMS/ATO Operational Principles. REF: 12E108, Version: 2b.

Glomsrud, J. and J. Xie (2019). A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships. In *29th European Safety and Reliability Conference*.

Hollnagel, E. (2004). Barriers and accident prevention.

IEC622901 (2014). IEC 62290 Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts . Standard.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science 42*(4), 237–270.

Leveson, N. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

Leveson, N. (2018). STPA Handbook. *MIT Partnership for Systems Approaches to Safety and Security (PSASS)*.

Leveson, N. G. and J. P. Thomas (2018). STPA Handbook. *Cambridge, MA, USA*.

Rejzek, M., S. H. Björnsdóttir, and S. S. Krauss (2018). Modelling multiple levels of abstraction in hierarchical control structures. *International Journal of Safety Science 2*(01), 94–103.

Singh, P., M. A. Dulebenets, J. Pasha, E. D. S. Gonzalez, Y.-y. Lau, and R. Kampmann (2021). Deployment of Autonomous Trains in Rail Transportation: Current Trends and Existing Challenges. *IEEE Access*.

Tonk, A. and A. Boussif (2024). Application of systems theoretic accident model and processes in railway systems: A review. *IEEE Access 12*.

Tonk, A., M. Chelouati, A. Boussif, J. Beugin, and M. E. Koursi (2023). A safety assurance methodology for autonomous trains. *Transportation Research Procedia 72*, 3016–3023.

UITP (2018). World Report On Metro Automation. Technical report, Union Internationale des Transports Publics.

Wang, Z., E. Quaglietta, M. G. Bartholomeus, and R. M. Goverde (2022). Assessment of architectures for Automatic Train Operation driving functions. *Journal of Rail Transport Planning & Management 24*, 100352.

Yin, J., T. Tang, L. Yang, J. Xun, Y. Huang, and Z. Gao (2017). Research and development of automatic train operation for railway transportation systems: A survey. *Transportation Research Part C: Emerging Technologies 85*, 548–572.

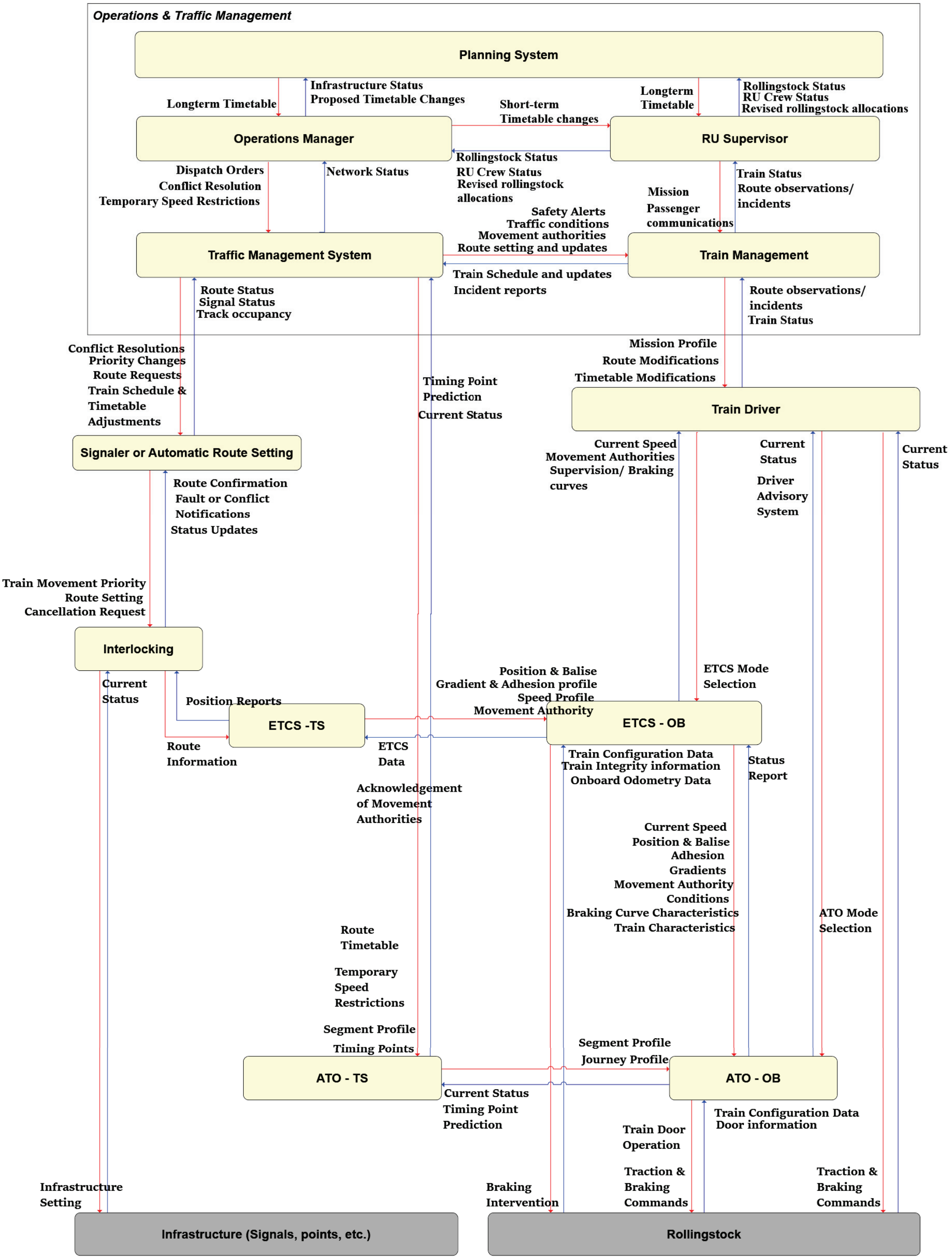


Fig. 6. Railway HSCS for GoA2 (semi-automated) train operations.