

Safety Analysis and Design Improvement for Semi-Automatic Train Operation (STO) in High-Speed Rail Using STPA

by
Wataru Suzuki

Bachelor of Agriculture in Applied Life Sciences, The University of Tokyo, 2013
Master of Engineering in Civil Engineering, The University of Tokyo, 2015

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2025

© 2025 Wataru Suzuki. All rights reserved.

The author hereby grants to MIT a nonexclusive, worldwide, irrevocable, royalty-free license to exercise any and all rights under copyright, including to reproduce, preserve, distribute and publicly display copies of the thesis, or release the thesis under an open-access license.

Authored by: Wataru Suzuki
System Design and Management Program
May 9, 2025

Certified by: John P. Thomas
Research Engineer, Department of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: Joan Rubin
Executive Director, System Design and Management Program

Safety Analysis and Design Improvement for Semi-Automatic Train Operation (STO) in High-Speed Rail Using STPA

by
Wataru Suzuki

Submitted to the System Design and Management Program on May 9, 2025
in Partial Fulfilment of the Requirements for the Degree of
MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT

ABSTRACT

In Japan, the Tokaido Shinkansen, a major high-speed rail corridor, plans to introduce Grade of Automation 2 (GoA2) through Semi-Automatic Train Operation (STO). While partial automation promises advantages such as reduced driver's workload and enhanced efficiency, it also creates new risks due to increasingly complex interactions among automated control systems, human operators, and physical infrastructure.

This thesis aims to systematically identify and address potential hazards arising from STO in high-speed rail. By using the Tokaido Shinkansen's announced plan as a model case, the research seeks to uncover scenarios in which normal, non-failed system behaviors can still lead to unsafe outcomes, and to propose design solutions that mitigate those risks early in development. To achieve this, the study applies Systems-Theoretic Process Analysis (STPA). Rather than isolating hardware and function failures, STPA models the entire system as a hierarchical control structure, examining each controller's possible unsafe actions and their feedback pathways.

The analysis reveals hazard scenarios that traditional failure-based methods might overlook. Examples include cases where a passenger is not detected between the train and platform doors at departure, or where verbal and signal instructions conflict and delay the driver's response. These scenarios can happen even without any component failure. Drawing on these insights, the thesis recommends a variety of design improvements, such as new monitoring functions for subsystems, modifying instruction interfaces, and strengthening the software logic of automation systems.

These findings demonstrate the value of conducting a holistic safety analysis using STPA at the conceptual design stage, before late-stage changes become more expensive. Moreover, this research provides a comprehensive, system-level railway hazard analysis, and the proposed measures can be broadly applicable to high-speed rail systems with automation.

Thesis Supervisor: John P. Thomas

Title: Research Engineer, Department of Aeronautics and Astronautics

DISCLAIMER

The views expressed in this thesis are those of the author and do not reflect official policy of the Central Japan Railway Company.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my thesis adviser, Dr. John P. Thomas, for his valuable guidance and support throughout my thesis projects. I am also grateful to all the professors, staff, and classmates who have always inspired me during my time in the System Design and Management Program at the Massachusetts Institute of Technology. I would also like to thank Central Japan Railway Company for providing the time and financial support required to complete the program. Finally, I owe the warmest thanks to my family, whose steady encouragement before and during my time abroad made this journey possible.

Table of Contents

Table of Figures	9
Table of Tables	10
1 Introduction	11
1.1 Motivation	11
1.2 Research Objectives.....	12
1.3 Thesis Structure	13
2 State of Automatic Operation and Safety Standards in High-Speed Rail	14
2.1 Current Status of Automated High-Speed Rail Operations	14
2.2 Review of Safety Standards for GoA2 in High-Speed Rail.....	15
2.2.1 Positioning of GoA2 in International Standards	16
2.2.2 Safety Requirements and Hazard Analysis in IEC 62267	17
2.2.3 Limitations of Current Safety Standards	18
2.3 Traditional Hazard Analysis in Railways	19
3 Current and Future Operations of the Tokaido Shinkansen	21
3.1 Overview of the Tokaido Shinkansen	21
3.2 Introduction of Semi-Automatic Train Operation (STO)	21
3.2.1 Core System Functions of STO.....	21
3.2.2 Crew Role Adjustments and Renovation of Platform Facilities and.....	28
3.3 Safety Challenges in STO Implementation	29
4 System Theoretic Safety Analysis	31
4.1 Rationale for Applying STPA to Hazard Analysis in High-Speed Rail Automation	31

4.2 Overview of STPA Methodology	31
5 Application of STPA to the Tokaido Shinkansen with STO	34
5.1 Concept of Operation.....	34
5.1.1 Departure Phase	34
5.1.2 Running Phase	36
5.1.3 Stopping Phase.....	36
5.2 System Losses and Hazards.....	37
5.3 Control Structure.....	38
5.3.1 High-level Control Structure	38
5.3.2 Control Structure for Departure Phase.....	40
5.3.3 Control Structure for Running and Stopping Phases	41
5.3.4 Defined Control Actions	41
5.4 Unsafe Control Actions	44
5.5 High-level Scenarios.....	46
5.6 Refined Scenarios	55
6 Evaluation of STPA Applied to New High Speed Rail System	65
6.1 Discussion on Identified Scenarios and Recommendations.....	65
6.2 Technical and Academic Contributions, and Evaluation of STPA.....	69
7 Conclusions	72
Appendix	74
Appendix A.1: Enlarged High-level Control Structure	74
Appendix A.2: Enlarged Control Structure for Departure Phase.....	75
Appendix A.3: Enlarged Control Structure for Running and Stopping Phases.....	76
Appendix B: UCAs	77

Appendix C: Safety Requirements 87

References 91

Table of Figures

Figure 1: Basic Mechanism of ATC (Automatic Train Control) [13].....	22
Figure 2: Speed Profile Generation and Real-time Adjustment by ATO [14]	25
Figure 3: An Operation Monitor during a Demonstration Test [15]	26
Figure 4: TASC braking profile for precise station stopping [14].....	27
Figure 5: Four Steps of STPA [12].....	32
Figure 6: Generic Control Loop [12].....	33
Figure 7: High-level Control Structure.....	39
Figure 8: Control Structure for Departure Phase.....	40
Figure 9: Control Structure for Running and Stopping Phases.....	41
Figure 10: Four Classes of Formal Scenarios[19].....	47
Figure 11: Scenario Classes in the Train Driver’s Control Loop	50
Figure 12: High-level Scenario Generation for UCA Type 1	51
Figure 13: High-level Scenario Generation for UCA Type 2.....	53
Figure 14: High-level Scenario Generation for UCA Type 3.....	54
Figure 15: High-level Scenario Generation for UCA Type 4.....	55
Figure 16: Enlarged High-level Control Structure	74
Figure 17: Enlarged Control Structure for Departure Phase.....	75
Figure 18: Enlarged Control Structure for Running and Stopping Phases.....	76

Table of Tables

Table 1: Grades of Automation [2].....	16
Table 2: Summary of Goal, Control Actions, Feedback/Input of ATC and ATO	27
Table 3: Example of Identified UCAs	44
Table 4: Example of Safety Requirements	45
Table 5: A Template to High-level Scenarios for Each Type of UCA.....	47
Table 6: High-level Scenario Generation for UCA Type 1	52
Table 7: Identified UCAs	77
Table 8: Identified safety requirements	87

1 Introduction

1.1 Motivation

High-speed rail is a fast, efficient, and environmentally friendly mode of transportation. As it is becoming increasingly important to improve safety, reduce the workload of human operators, and enhance energy efficiency, there is growing demand for the introduction of automated operation technology in high-speed rail.

However, unlike systems such as subways and monorails, where the introduction of automated operation is already well advanced, the automation of high-speed rail presents unique challenges. These include complex operating conditions due to long-distance high-speed operation and long station intervals, as well as human intervention in emergency situations. Future high-speed rail automation is expected to adopt Grade of Automation 2 (GoA2), with a driver remaining in the cab. In this operational model, unlike full automation, automation systems and human operators must work in tandem, making "coordination between humans and automated systems" a key factor in ensuring safe operations.

In recent years, several high-speed rail operators, mainly in Japan, have announced plans to introduce automation at GoA2 or higher. For example, Japan's Tokaido Shinkansen, one of the world's most frequent and high-capacity high-speed rail systems, plans to introduce Semi-Automatic Train Operation (STO), equivalent to GoA2, from 2028 onward [1]. The implementation of STO will require upgrades to ground infrastructure, as well as modifications to crew roles and operational procedures. These transformations will significantly reshape the interactions among components within the overall system.

In the new system following STO implementation, automated control systems, human operators, and physical infrastructure on stations and platforms will intricately interact. These interactions may give rise to unforeseen hazards. Therefore, at this early stage of system design and development, it is essential to thoroughly understand potential hazards at the overall system level and implement necessary design improvements.

Systems-Theoretic Process Analysis (STPA) is an advanced hazard analysis method that goes beyond traditional failure-based approaches. One of its strengths is its ability to analyze human factors, automation control, and infrastructure as interconnected elements within a

unified system, rather than as isolated components. This study aims to apply STPA to analyze safety challenges associated with the introduction of STO in high-speed rail, contributing to the broader knowledge of safety evaluation in high-speed rail automation.

1.2 Research Objectives

Building upon the motivation discussed in the previous section, this study aims to achieve the following two objectives.

The first objective is to identify hazard scenarios in the new high-speed rail system with STO (GoA2) and derive design recommendations. To achieve this, using the Tokaido Shinkansen in Japan as an example, a conceptual system design for STO implementation in the Tokaido Shinkansen will be constructed based on existing operations and publicly available STO implementation plans. By applying STPA, this study will systematically identify hazardous scenarios that may arise from interactions between human operators, automation systems, and physical infrastructure. Particular attention will be given to complex interactions between human operations and automation, which are particularly relevant to train departure or stopping procedures at stations and emergency interventions during operations. Based on the findings, design recommendations that can be incorporated at the conceptual design stage will be derived to mitigate potential risks and enhance safety.

The second objective is to demonstrate the effectiveness of STPA in identifying system-level hazards that may not be apparent through conventional methods in the railway industry. In railway systems, fail-safe mechanisms are widely implemented, where physical component failures generally result in a “stop” response. This approach differs from aviation, where failures must be managed while maintaining continued operation. While railway safety analysis has historically focused on identifying hazards associated with physical component failures and implementing appropriate countermeasures, hazards may still emerge at the system level even in non-failure scenarios where all components operate as specified. Moreover, traditional system engineering and hazard analysis have often been applied separately to subsystems such as signaling and rolling stock. However, comprehensive hazard analysis at the total railway system level, including human operations, has been relatively limited. This research will demonstrate that STPA is useful for identifying such system-level hazard scenarios, which traditional safety methods may overlook.

By achieving these objectives, it aims to provide practical insights for the safe introduction of STO in high-speed rail while also contributing to the broader application of STPA in railway automation safety analysis.

1.3 Thesis Structure

Chapter 1 introduces the purpose and objectives of this research. Chapter 2 provides background on the current status of automated high-speed rail, with a focus on GoA2. It also reviews the relevant safety standards and safety analysis practices used in the railway industry. Chapter 3 offers an overview of the Tokaido Shinkansen and its STO introduction plan as background for the analysis. Chapter 4 introduces the STPA framework and explains why it is suitable for analyzing high-speed rail systems that feature multiple interacting components and human operators. Chapter 5 applies STPA to the Tokaido Shinkansen with STO and shows the results of analysis that include losses and hazards, control structures, a sample of UCAs, and a sample of hazard scenarios and design recommendations. (Full tables of UCAs can be found in the Appendices). Chapter 6 assesses the findings of the STPA analysis and evaluates how the suggested solutions differ from traditional failure-based approaches. Finally, Chapter 7 presents conclusions that summarize the key insights from this work.

2 State of Automatic Operation and Safety Standards in High-Speed Rail

This chapter provides an overview of recent developments toward the automation of high-speed rail and reviews the relevant safety standards and safety analysis practices used in the railway industry.

2.1 Current Status of Automated High-Speed Rail Operations

Compared to urban rail systems, high-speed rail automation is still in early stages, and actual operational experience remains limited. In subways and other urban rail systems, Automatic Train Operation (ATO) has been adopted early on, with many lines already achieving fully unattended operation. Urban rail typically follows a relatively simple operating pattern of controlled acceleration, cruising, braking, and precise stopping, which makes automation easier to implement.

High-speed rail involves long-distance, high-speed operation, resulting in more complex and varied operating patterns. Operating patterns and speed limits often differ depending on the type of train and time of day, requiring coordination of trains traveling at different speeds on the same tracks. These factors together make the technical barriers to high-speed rail automation higher than in urban rail.

Many high-speed rail automation projects are currently in either the testing phase or early deployment stage, with most targeting Grade of Automation 2 (GoA2), which allows for partial automation. Under GoA2, operations such as train departure, acceleration, deceleration, and stopping are automated, while the driver or an onboard crew member remains present and can intervene when needed [2]. This “semi-automatic” approach is used to first verify safety and reliability, with the aim of transitioning step-by-step to higher levels of automation (GoA3 or GoA4) in the future. However, even GoA2-level systems are not yet fully deployed in service, and new safety issues may arise as operational experience grows.

The following provides an overview of regional developments.

Japan

Plans are underway to introduce automation into the Shinkansen network, which has long led

global high-speed rail technology. East Japan Railway Company (JR East) plans to implement GoA2-level automatic operation (with a driver onboard) for both commercial and non-revenue (deadhead) trains between Nagaoka Station and Niigata Depot (60.8 km) on the Joetsu Shinkansen [3]. Starting in FY2029, GoA4-level driverless operation is planned for deadhead trains between Niigata Station and Niigata Depot (5.1 km). By the mid-2030s, JR East plans to expand GoA2 automatic operation to the section between Tokyo and Nagaoka, followed by GoA3 driverless operation for commercial trains between Tokyo and Niigata, and GoA4 driverless operation for deadhead trains on the same corridor. In addition, Central Japan Railway Company (JR Central) has announced plans to introduce Semi-Automatic Train Operation (STO), equivalent to GoA2, on the Tokaido Shinkansen between Tokyo and Osaka, one of the world's most heavily used and highest-frequency rail corridors, by around 2028 [4], [5]. The Tokaido Shinkansen is considered a critical test case for large-scale high-speed rail automation due to its extreme operational intensity.

China

In late 2019, China opened the Beijing–Zhangjiakou high-speed railway, where ATO was introduced to achieve autonomous operation at speeds of up to 350 km/h [6]. This system fully automates departure, speed control, station stopping, and door operations. However, at the time of opening, only six of the approximately 30 daily trains operating between Beijing and Zhangjiakou were using the new system, meaning large-scale deployment was still limited.

Europe & North America

In Europe and North America, high-speed rail automation remains in the research and testing phase. No concrete plans for full commercial deployment are expected within the next few years (at least five years). In France, SNCF (the French national railway) announced plans to develop a prototype of an automated TGV and conduct test runs by 2023 [7]. However, as of now, the system has not been introduced, and there has been no public update on further development or deployment schedules. In North America, the limited presence of operational high-speed rail means that no specific automation projects currently exist. Even for future high-speed rail plans, such as the California High-Speed Rail, there have been no mentions of automation features in planning documents.

2.2 Review of Safety Standards for GoA2 in High-Speed Rail.

After reviewing the overall status of automated high-speed rail in Section 2.1, it becomes clear

that many of the planned or early-stage implementations aim for Grade of Automation 2 (GoA2), in which a driver or operator remains present in the cab. With this in mind, the following discuss the major international safety standards and guidelines commonly referenced in railway automation.

2.2.1 Positioning of GoA2 in International Standards

At present, there are no international safety standards specifically dedicated to GoA2 in high-speed railways. In practice, general automation standards intended for urban railway systems can be referenced. Two representative examples are the IEC 62290 series and IEC 62267. IEC 62290 specifies the design and operation of Urban Guided Transport Management and Command/Control Systems (UGTMS) and defines the classification of Grades of Automation (GoA0 to GoA4)[2]. Table 1 summarizes the mandatory basic functions of train operation for each grade.

Table 1: Grades of Automation [2]

Basic functions of train operation		On-sight train operation	Non-automated train operation	Semi-automated train operation	Driverless train operation	Unattended train operation
		GOA0	GOA1	GOA2	GOA3	GOA4
Ensure safe movement of trains	Ensure safe route	x (points command/control in system)	system	system	system	system
	Ensure safe separation of trains	x	system	system	system	system
	Ensure safe speed	x	x (partly supervised by system)	system	system	system
Drive train	Control acceleration and braking	x	x	system	system	system
Supervise guideway	Prevent collision with obstacles	x	x	x	system	system
	Prevent collision with persons on tracks	x	x	x	system	system
Supervise passenger transfer	Control passengers doors	x	x	x	x	system
	Prevent injuries to persons between cars or between platform and train	x	x	x	x	system
	Ensure safe starting conditions	x	x	x	x	system
Operate a train	Put in or take out of operation	x	x	x	x	system
	Supervise the status of the train	x	x	x	x	system
Ensure detection and management of emergency situations	Detect fire/smoke and detect derailment, detect loss of train integrity, manage passenger requests (call/evacuation, supervision)	x	x	x	x	system and/or staff in OCC
NOTE		x = responsibility of operations staff (may be realised by UGTMS system)		system = shall be realised by UGTMS system		

IEC 62290 includes a detailed description of GoA2 (semi-automatic operation), which is the focus of this study. GoA2 is defined as follows:

Grade of automation 2 (GoA2): Semi-automated train operation

In this grade of automation, the driver is in the front cabin of the train observing the guideway and stops the train in the case of a hazardous situation. Acceleration and

braking is automated and the speed is supervised continuously by the system. Safe departure of the train from the station is the responsibility of the operations staff (door opening and closing may be done automatically).

Although IEC 62290 presents minimum functional requirements for each automation level, safety aspects are addressed mainly at a high level, and there is no in-depth discussion of specific safety measures.

2.2.2 Safety Requirements and Hazard Analysis in IEC 62267

IEC 62267 serves as a general guideline that specifies the safety requirements for Automated Urban Guided Transport (AUGT) systems[8]. While it primarily focuses on fully automated operations (GoA3 and GoA4), it also provides a system-level hazard analysis for railway operations under automation. This analysis is based on operational experience gained during the drafting of IEC 62267 itself and covers various risk factors to be addressed in any automated operation. In total, the standard identifies 67 top-level hazardous situations and outlines possible safeguards for each.

Although not a standard tailored specifically to high-speed railway at GoA2, several of the safety measures outlined are potentially useful references for semi-automated operations. For example, in an automated system equipped with platform doors, the risk of passengers being trapped between the platform screen door and the train is recognized as a critical accident scenario. IEC 62267 recommends multiple layers of safety measures for such a scenario, including:

- Emergency stop demand on board
- Emergency stop switch on the platform
- Ensure that platform doors cannot be closed when a passenger is between the train and platform screen
- Detection of obstacles during door closure
- Design measures to minimize the gap between the train and the platform screen
- Devices on board or on the platform to monitor the lateral space between the train and platform screen

Following the presentation of potential safeguards, the guideline defines corresponding

general safety requirements. These measures are primarily presented as a means of ensuring safety in unattended (GoA4) systems, where neither a driver nor station staff are present, but many of them can also be effectively applied to semi-automated operation (GoA2) under human supervision. Consequently, these guidelines can serve as a valuable reference when introducing partial automation in high-speed rail.

However, the standard does not prescribe which specific safeguards must be adopted, nor does it define a universally acceptable level of residual risk. Instead, it assigns this responsibility to the relevant Safety Regulatory Authority (SRA), which must determine safety policies, targets, and tolerable risk thresholds based on the operational context and local safety culture. As a result, the final safety solutions and their associated risk levels may vary from one application to another.

2.2.3 Limitations of Current Safety Standards

As outlined above, existing international standards (IEC 62290 and 62267) provide a basic framework for ensuring safety in automated operation. However, several challenges remain when it comes to applying them to GoA2 operations in high-speed railways.

First, the scope of current standards is limited. IEC 62267 is primarily a compilation of best practices from past urban railway automation projects, so the operational conditions and hazard scenarios considered are largely derived from subway or new transit systems. High-speed rail has many differences from urban rail, such as high-speed operation and long distances between stations. Thus, the existing standards alone may not fully cover the unique risks of high-speed operations. Additionally, while GoA2 assumes the presence of a train driver (semi-automatic operation), the standard guidelines often draw a broad distinction between “manual” and “driverless,” with insufficient discussion of intermediate forms. For example, there is no clear definition of how authority is transferred or how the system intervenes when the onboard driver manually activates the emergency brake, leaving each project to develop its own rules. In response, some discussions in Japan have described an intermediate form between GoA2 and GoA3, referred to as “GoA2.5,” where the driver is present only for emergency intervention. However, this kind of intermediate operation mode is not officially reflected in Japan's Technical Standards Ministerial Ordinance (including interpretation standards and explanations), let alone in international standards, revealing a gap in standardizing its safety requirements.

Second, the standards themselves are becoming outdated, lacking reflection of the latest technological trends. Since the first edition of IEC 62267 was issued in 2009, technology around autonomous operation has advanced significantly. In particular, AI (Artificial Intelligence) and computer vision are increasingly deployed in railway applications, enabling advanced anomaly detection and sophisticated hazard prediction modeled on human judgment. However, the existing standards (IEC 62267/62290) were established in an era dominated by conventional sensor technology and fail-safe design concepts, offering no provisions for system-specific issues related to the latest technologies. As the introduction of AI-based monitoring or image recognition systems in high-speed railway operation becomes more likely, developing updated safety guidelines or entirely new standards that incorporate these modern technologies has become imperative.

2.3 Traditional Hazard Analysis in Railways

In railways, Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) have been the main safety analysis methods for many years. These methods are recognized or referenced in standards such as IEC 62278, which defines RAMS (Reliability, Availability, Maintainability, and Safety) management for railways, and have been widely used [9].

FTA is a top-down, deductive approach that models sequences of failures using Boolean logic and symbols. It starts with a top-level failure event, and decomposes it into combinations of more detailed failure causes [10]. FMEA is a bottom-up, inductive approach to identify potential failure modes of a system or product and their effects [11]. Both methods often quantify the probability of identified failures.

However, both methods have limitations when applied at the system level. The focus of FTA and FMEA is primarily on individual failures. FTA analyzes the causes of failure by assuming that there is a one-way sequence leading to the failure, but it is difficult to apply to complex systems where multiple interactions exist beyond simple one-way sequences. Similarly, because FMEA starts at the component level, it provides good vertical traceability (failure mechanisms, modes, and effects) but tends to be weak in analyzing horizontal interactions between system elements.

Because these methods assume that a failure occurs as a starting point, they are not well suited

for handling hazards that arise even when no failures are present. Modern railway systems have evolved into large and complex systems that include interactions among humans and many other systems. In such environments, accidents can happen even when all components are functioning as designed. Since FTA and FMEA mainly focus on individual failures, they may not fully capture hazards that arise due to system-level design issues even when no individual component or function has failed.

In addition to these method-specific characteristics, there is also a structural issue in how hazard analysis is performed during railway system development. Traditionally, hazard analysis has been carried out separately for each subsystem based on development or procurement units. Railways, however, function as total systems that integrate vehicles, signaling, power supply, track infrastructure, and human operations. Although each subsystem is strictly developed and analyzed according to its own standards and processes, there are cases where a comprehensive, total-system-level safety analysis is not fully performed. As a result, interface and system-level hazards may be overlooked.

In the new high-speed rail systems operating under GoA2, there are complex interactions not previously considered that could affect safety. Therefore, new hazard scenarios that have not been addressed by traditional methods may emerge. To address this, this study applies Systems-Theoretic Process Analysis (STPA), which allows for system-level analysis that considers the interactions among components [12]. Details and application of STPA are discussed in Chapter 4 and beyond.

3 Current and Future Operations of the Tokaido Shinkansen

In this study, the Tokaido Shinkansen, which is a proven high-speed rail in Japan, is used as the model case for the safety analysis of high-speed rail with STO. JR Central, the operator, has announced that it plans to introduce STO around fiscal year 2028, and some details of the technical development have already been made public[1] [13] [14]. This chapter gives an overview of the Tokaido Shinkansen and the STO introduction plan as background for the analysis in Chapter 4 and later.

3.1 Overview of the Tokaido Shinkansen

Since its opening in 1964, the Tokaido Shinkansen has developed as a world-leading high-speed railway, known for its safety, very high service frequency, and large transport capacity. It connects Tokyo and Osaka, the main transport artery of Japan. In fiscal year 2023, about 372 trains ran per day, and about 432,000 passengers were transported per day [13]. It is one of the world's largest high-speed mass transport services, comparable to a commuter railway. In terms of safety, no passenger has been killed or injured in a train accident while on board since opening [13]. In terms of punctuality, according to the data for fiscal year 2023, the average delay per train was only 1.6 minutes, including delays caused by natural disasters [13]. In terms of speed performance, the Tokaido Shinkansen operates at a maximum service speed of 285 km/h, and the fastest trains travel between Tokyo and Osaka in 2 hours and 21 minutes (based on the March 2023 timetable) [13].

3.2 Introduction of Semi-Automatic Train Operation (STO)

JR Central plans to start the operation of automatic driving functions around fiscal year 2028. The automation method corresponds to Grade of Automation 2 (GoA2) and is called Semi-Automatic Train Operation (STO). With this method, it is expected that the workload on train drivers will be reduced. The following two subsections give an overview of the functions of STO that have been published and the renovations of facilities and reviews of crew roles that will accompany it.

3.2.1 Core System Functions of STO

STO consists of two primary system components: ATC (Automatic Train Control) and ATO

(Automatic Train Operation). ATC serves as the foundational safety system ensuring the safe operation of the current Tokaido Shinkansen. STO is realized by incorporating ATO into the existing foundation of ATC.

ATC (Automatic Train Control)

ATC is a fundamental safety system that has been adopted on the Tokaido Shinkansen since its opening [13]. The purpose of ATC is to maintain a safe distance between trains and keep each train within the speed limit in order to prevent collisions and derailments. ATC continuously monitors the train's speed against the maximum allowable speed and automatically applies brakes if the speed exceeds the limit. The ATC signal is calculated based on the track speed limit and the distance to the preceding train and is displayed in the driver's cab as an in-cab signal indicating the allowable operating speed at that moment.

Figure 1 shows how ATC functions. The on-board ATC equipment first receives the position information of the train ahead through ground facilities. It then compares that with its own train position and creates an ATC signal (speed limit) expressed as a brake pattern (the blue curve in Figure 1). The train's speed is constantly checked against the ATC signal, and if the speed approaches the limit, ATC automatically applies the brakes.

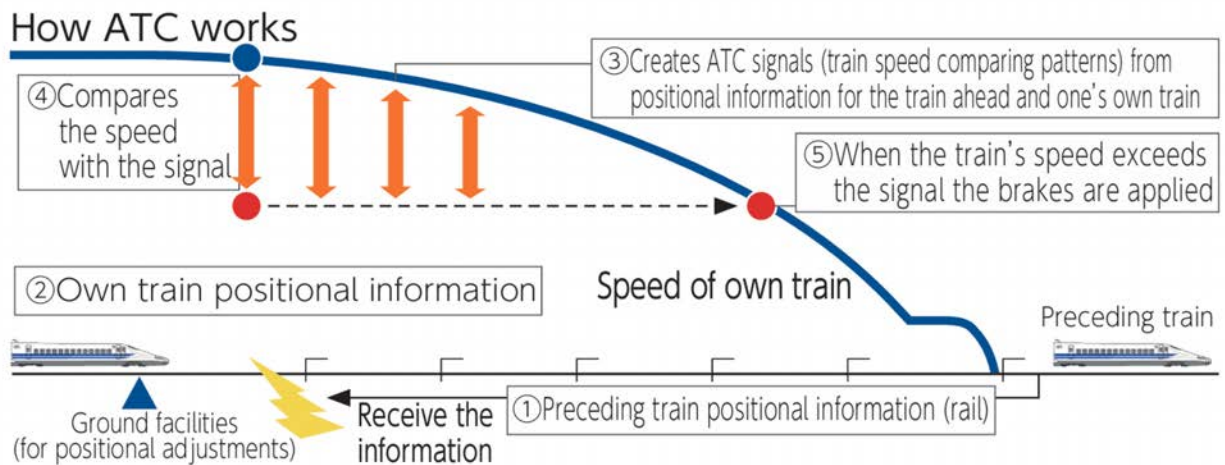


Figure 1: Basic Mechanism of ATC (Automatic Train Control) [13]

The safety of ATC has been proven through many years of operational experience. It will continue to be the foundational safety system in the new STO system. Regardless of the ATO mode or behavior described later, ATC will automatically apply brakes at any time if the train speed exceeds the ATC signal.

ATO (Automatic Train Operation)

ATO is a new feature that will be introduced to replace the control actions previously performed by the train driver [14]. Specifically, it refers to speed adjustment to meet the schedule and to control station stopping. ATO has two modes corresponding to these functions.

- Interstation running mode is responsible for departure and speed adjustment between stations. It generates a speed profile based on the schedule and adjusts acceleration, coasting, and braking accordingly.
- TASC mode is responsible for the final phase of stopping at a station. Using the Train Automatic Stop Control (TASC) function, it controls the train's braking from below 30 km/h to a complete stop at the designated platform position.

The details of each mode are as follows.

Interstation running mode

In interstation running mode, ATO generates an optimal speed profile based on the operational schedule (station stop/passing times), while always ensuring compliance with the maximum allowable speed defined by the ATC signal. The system controls the train's speed (acceleration, coasting, deceleration) according to this profile.

The major difference from ATC is the purpose. ATC is designed to ensure safety by preventing collisions, derailments, and overspeed. In contrast, the purpose of this ATO mode is to achieve automatic on-time operation. The maximum allowable speed is shown by the ATC signal, but in actual operation, trains do not always run strictly at that speed. In practice, extra buffer time is added to the minimum required travel time between stations to allow for operational flexibility. Because of this, trains usually run at speeds lower than the ATC limit during normal operation. These schedules and conditions vary depending on the route and the specific train. In the current system, the train driver has been responsible for determining the appropriate speed based on the operational situation and adjusting acceleration and braking accordingly. Under the STO system, this process of speed calculation and control will be automated by the interstation running mode of ATO. ATC can only apply brakes when the train is about to exceed the ATC limit, but ATO controls both acceleration and deceleration to adjust train speed.

In general, automated train operation systems implemented in subway systems and other urban railways rely on predetermined speed profiles. These systems operate based on simple travel patterns with short station intervals, adjusting speeds according to pre-defined operation curves and regulating schedules through station dwell times. However, the Tokaido Shinkansen features diverse and dynamic speed profiles, requiring precise responses to sudden speed restrictions. Traditional automation methods are insufficient to handle these complexities.

To address these challenges, the ATO function in the new system will dynamically generate optimized operation speed profiles. The upper part of Figure 2 shows an example where, when running from station A to station D, a speed profile (orange curve) is calculated before departure at station A. The train departs station A and runs according to this profile. While running, the system checks every 0.1 seconds whether the train can pass through and arrive at upcoming stations on time according to the current speed profile. These speed profiles are created based on factors such as ATC signal (including slow-down instructions), track conditions (such as gradients and tunnels), vehicle performance, and real-time scheduling data (such as current time and planned passing and arrival times).

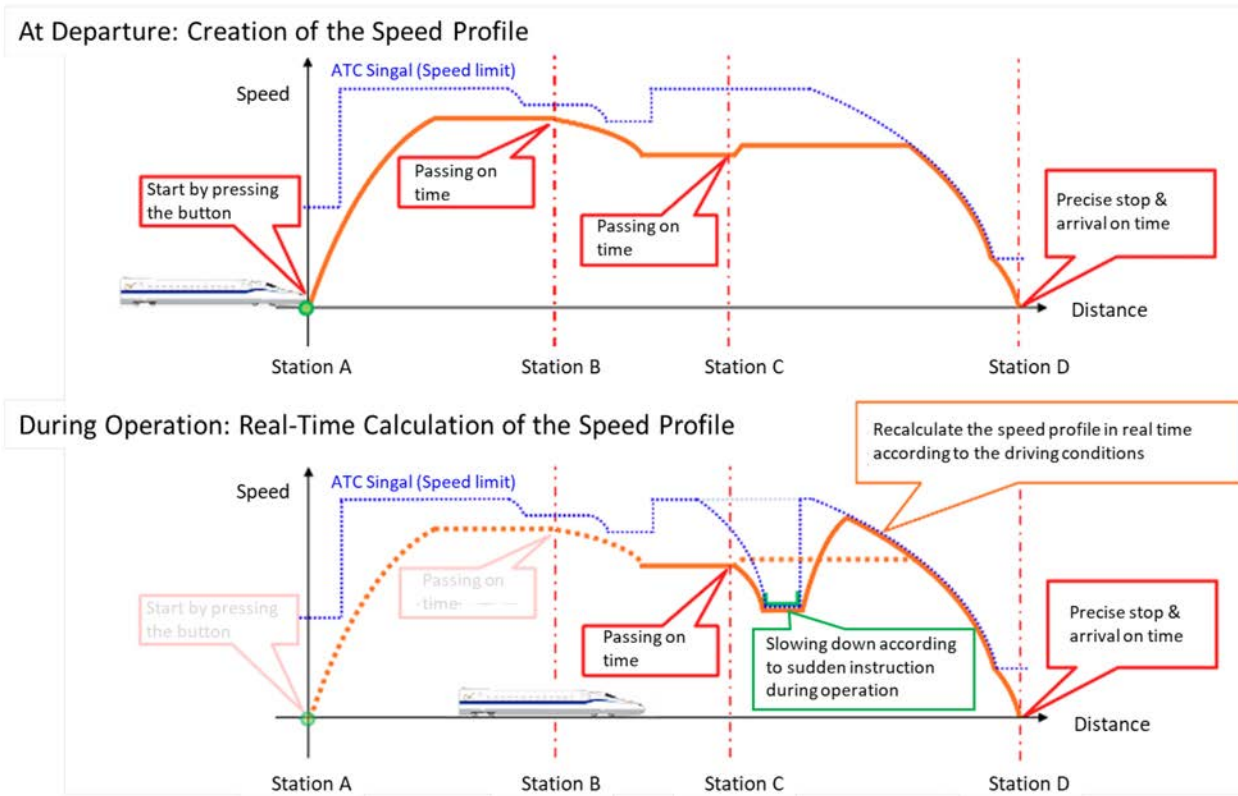


Figure 2: Speed Profile Generation and Real-time Adjustment by ATO [14]

In the lower part of Figure 2, after passing Station B on time, a sudden slowdown is instructed via a new ATC signal. In response, a new operation curve is calculated in real time to maintain the on-time passing at Station C and arrival at Station D, and the train's movement is controlled accordingly.

This approach allows the train to adjust speed not only for planned slowdowns but also for sudden speed restrictions caused by weather conditions or safety checks, while still keeping on schedule. Additionally, the system aims to minimize unnecessary acceleration and deceleration, providing a smoother ride for passengers. By selecting optimal acceleration rates and using energy-saving techniques such as coasting on downhill gradients, the system improves both ride comfort and energy efficiency.



Figure 3: An Operation Monitor during a Demonstration Test [15]

Figure 3 shows the operation monitor in the driver's cab during a demonstration test conducted under ATO interstation running mode [15].

- Purple curve: additional temporary speed limits issued by the OCC.
- Yellow curve: the current ATC speed limit calculated for this train. ATC computes this limit from three main inputs:
 1. the default (permanent) speed limits and vehicle braking performance data stored in its memory,
 2. the distance to the target stopping point (the rear of the preceding train or the next scheduled station stop) received from track circuit, and
 3. additional temporary speed limits (purple curve) issued by the OCC, when applicable.
- Orange curve: the target speed profile generated by ATO to keep the train on schedule while always remaining below the yellow curve.
- Blue curve: the actual speed trajectory up to that point.

ATO accelerates or brakes the train to follow the orange profile. If the vehicle is about to

exceed an ATC speed limit (yellow curve), ATC automatically applies the brakes.

TASC mode

ATO has also the TASC function [14]. TASC automatically applies brakes to stop the train precisely at the designated position on the platform . The system receives information from transponders installed at the station, generates a TASC brake profile, and automatically controls braking accordingly to achieve highly accurate station stops. TASC manages braking for speeds below 30 km/h.

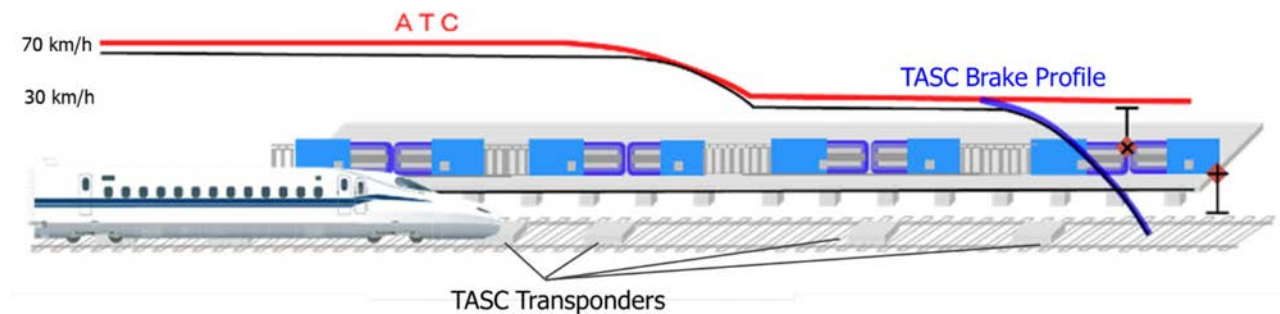


Figure 4: TASC braking profile for precise station stopping [14]

Figure 4 illustrates this process, where the TASC brake curve takes over from the ATC signal during the final phase of deceleration, allowing for precise stopping at the platform.

Finally, Table 2 summarizes ATC and the two ATO modes in terms of goal, control actions, and feedback or inputs. The key difference is that ATC exists purely for safety, whereas ATO mainly supports or replaces the driver. In the interstation running mode, ATO takes the ATC signal (speed limit) as a minimum safety constraint, but unlike ATC it also takes the operation schedule as an additional input.

Table 2: Summary of Goal, Control Actions, Feedback/Input of ATC and ATO

	ATC	ATO interstation running mode	ATO TASC mode
--	-----	-------------------------------	---------------

Main goal	Keep trains safely separated and below the speed limit to avoid collisions and derailments	Automatically adjusts the train's speed to achieve on-time operation	Automatically stop the train precisely at the designated position at a station
Control actions	Apply brakes when the train is about to exceed the ATC signal (speed limit)	Apply brakes and acceleration according to the generated speed profile	Apply brakes according to the generated TASC brake profile
Key feedback/input	<ul style="list-style-type: none"> •Distance to preceding train •Default speed limits •Emergency stop signal or temporary speed restriction signal •Current train speed, position •Track data (gradient, curve, station track layout) •Vehicle performance 	<ul style="list-style-type: none"> • ATC signal (speed limit) • Current train speed, position • Track data (gradient, curve, station track layout) • Vehicle performance • Operation schedule 	<ul style="list-style-type: none"> • Current train speed, position • Trigger from TASC transponders • Distance to stop position • Vehicle performance

3.2.2 Crew Role Adjustments and Renovation of Platform Facilities and

Along with the introduction of STO, not only will the control of train speed become automatic, but changes to crew roles and renovations to platform facilities are also planned.

First, the train driver will take over the task of opening and closing the train doors at stations, which has traditionally been done by the conductor [13]. As a result, the main operators involved in safety checks and door operations at station departure and arrival will change from three people, the train driver, platform attendant, and train conductor, to two people, the train driver and platform attendant.

To improve safety during station departures and arrivals, there is a plan to gradually install platform doors at all stations [1]. Currently, only some stations are equipped with them. For this reason, operations during departure and arrival will need to ensure safety while also coordinating with the opening and closing of platform doors.

These changes will greatly affect the safety check operation during train departure, because the components involved and the responsible operators will be different from before.

3.3 Safety Challenges in STO Implementation

The most serious accidents in high-speed rail are collisions and derailments. On the Tokaido Shinkansen, no major collisions or derailments have occurred since its opening, due to a safety design that is fundamentally based on ATC. Under the STO system, the same ATC logic will continue to function as the hard safety layer. However, with the introduction of ATO, it is necessary to carefully reassess whether any unexpected behaviors could arise that might compromise the safety provided by ATC, or whether ATO commands and behavior could unintentionally affect overall system behavior.

In addition, maintaining safe operation under STO requires careful design of when and how the train driver can manually intervene, as well as how the train driver interface is structured. Even in the new system, a train driver will remain in the cab to respond to emergencies. The Tokaido Shinkansen has experienced several past events where human intervention during emergencies played a critical role. For example, in 2015, a fire was started inside a train by arson [16]. In that case, the driver manually stopped the train at a location that allowed easier evacuation, and this quick and flexible action played an important role in ensuring passenger safety. Another incident occurred in 2018, when a fatal stabbing attack happened inside a train [17]. This event highlighted the unique risks of high-speed railways, where long distances between stations can limit immediate evacuation options, and reinforced the importance of flexible responses by human operators in emergencies.

Careful attention is also required for the departure phase at stations. Historically, the only fatal accident recorded on the Tokaido Shinkansen was a case where a passenger was caught in the train door at departure [18]. Even under the conventional system, the station departure phase involves complex interactions between multiple human operators and equipment. In the new STO system, changes in operator roles and system components during departure could

introduce new types of hazard scenarios that were not anticipated before.

4 System Theoretic Safety Analysis

4.1 Rationale for Applying STPA to Hazard Analysis in High-Speed Rail Automation

As explained at the end of the previous chapter, the Tokaido Shinkansen with STO introduces a new complex control structure. In this system, both ATC and ATO must cooperate in real time to control train speed, and the driver may provide manual control at any time in emergencies. The platform doors, train doors, drivers, and platform staff all work together during station departures and arrivals. In such a complex structure, even if each component operates exactly as designed, unexpected combinations of interactions can still lead to hazardous conditions. Therefore, traditional methods that focus only on individual failures may not be sufficient to fully capture the risks.

Moreover, STO is still in the concept design phase, where detailed component specifications and reliability data are not yet available. Traditional safety analysis methods that rely on failure probabilities of individual components are not well suited for this early phase, where design flexibility remains high. What is needed instead is a hazard analysis method that can evaluate the entire system design from a broader perspective, considering how components are combined and how they interact.

For these reasons, a safety analysis of high-speed rail automation at the concept design stage must consider the entire control structure and comprehensively evaluate unsafe interactions, even under normal operating conditions. Systems-Theoretic Process Analysis (STPA) was chosen for this reason.

4.2 Overview of STPA Methodology

STPA is a hazard analysis approach built on the System-Theoretic Accident Model and Processes (STAMP) framework [12]. Unlike traditional safety analyses methods that often concentrate on single-component failures or linear cause-and-effect event chains, STPA views safety as an emergent property of a complex system. In other words, accidents can result from unsafe interactions among components—human, hardware, or software—even if each component individually works as designed. This perspective is critical for large, complex systems like high-speed rail, where multiple components must work together safely.

STPA is carried out following the four steps shown in Figure 5.

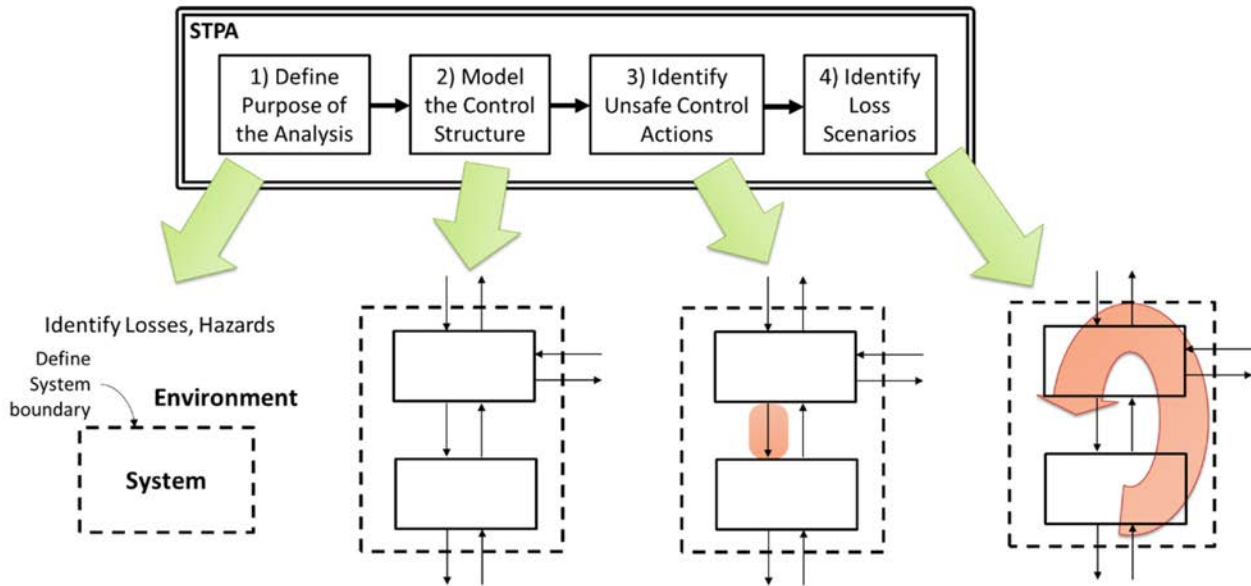


Figure 5: Four Steps of STPA [12]

1. Define the Purpose of the Analysis

During this stage, the losses (for instance, loss of life or damage to property) that must be prevented are identified. Next, the system-level hazards are identified — system states or conditions that, in a worst scenario, could cause one or more losses. Each hazard then yields system-level constraints specifying conditions that must be maintained for safe operation.

2. Model the Control Structure

Next, the system is modeled as a hierarchical control structure of controllers and controlled processes. As seen in Figure 6, the control structure is drawn with downward arrows for control actions (instructions or commands) and upward arrows for feedback (signals, information, or states). The controller makes decisions based on two key components. The first is the control algorithm, which determines what action to take. The second is the process model, which represents the controller's internal understanding of the system's current state, its goals, and how control actions affect the system.

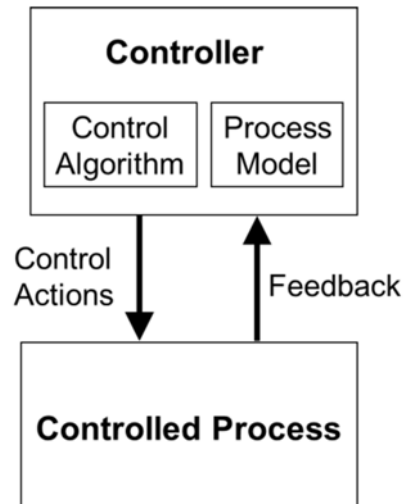


Figure 6: Generic Control Loop [12]

3. Identify Unsafe Control Actions (UCAs)

Once the control structure is established, each control action is examined to see how it could become unsafe in specific contexts. STPA identifies UCAs in four categories: (1) Not providing causes hazard, (2) Providing causes hazard, (3) Providing too early, too late, or out of order, and (4) Stopped too soon, applied too long. Each category may include multiple UCAs, and each UCA should be traced to one or more of the identified hazards. Similar to system-level constraints, safety requirements for each controller's behavior can be also identified from each UCA to specify the correct safe actions needed to prevent each UCA.

4. Identify Loss Scenarios

In the final step, causal scenarios are developed to explain why a UCA might occur. STPA identifies the causes of UCAs by generating causal scenarios. These scenarios typically involve controllers issuing unsafe commands because of flawed process models, which are often the result of inadequate feedback. Other types of scenarios include cases where a properly commanded control action is not actually executed, or where it leads to another behavior that is unsafe. Finally, STPA scenarios can then be used to generate recommendations aimed at mitigating the causal factors that lead to hazards and losses.

5 Application of STPA to the Tokaido Shinkansen with STO

5.1 Concept of Operation

This section outlines the concept of operations for a future high-speed rail system incorporating STO. The STPA analysis begins in Section 5.2.

This study focuses on the full operational sequence of a commercial high-speed train—from station departure, running at high speed between stations, to arrival and stopping at the next station. The following subsections describe these phases, which will serve as the foundation for the STPA.

The specifications presented here were independently developed by the author based on publicly available information from JR Central and recent technological advancements by other railway operators. As such, some assumptions are included, and the details may differ from actual system specifications.

5.1.1 Departure Phase

This phase refers to the period from when the train is at a complete stop at the station, through door opening and passenger boarding/alighting, to when the train departs after ensuring all conditions for safe departure are met.

This phase is particularly critical, as accidents such as departing with a passenger caught in the train door occur more frequently than collisions or derailments. Below is a chronological description of the standard procedure and involved components.

Normal procedures

1. After the train stops at the station, platform doors detect the train's stop and its stopping position, then automatically open.
2. Train driver confirms that the platform screed doors have opened via the indicator and then opens train passenger doors.
3. As departure time approaches, platform attendant confirms that the departure permission ATC signal is displayed on the platform indicator.
4. Platform attendant visually checks passenger boarding and alighting, both directly and via

platform monitors.

5. Platform attendant sends the train door close command to the driver by pressing a switch on the control panel. This action also initiates the closure of platform doors.
6. Train driver confirms the train door close command via the platform indicator and buzzer, then closes the train doors using a switch in the driver's cab.
7. Platform attendant visually verifies the following, both directly and via platform monitors:
 - ✓ No passengers are left between platform doors and train.
 - ✓ No passengers are trapped in train doors.
 - ✓ All train doors are fully closed (confirmed by the train's door indicator light).
 - ✓ All platform doors are fully closed (confirmed by the station control panel indicator).
8. Platform attendant sends the departure permission order to the driver by pressing a switch on the control panel.
9. Train driver verifies the following:
 - ✓ The departure permission ATC signal is displayed on the driver's cab monitor.
 - ✓ All train doors are fully closed (confirmed by the indicator in the driver's cab).
 - ✓ The departure permission order is issued by the platform attendant.
10. Train driver releases manual brakes and activates ATO function by pressing the switch.
11. ATO initiates the train's departure, controlling speed to leave the station.

Emergency Procedures and Safeguards

- If a passenger is trapped in the train door at step 7, platform attendant can issue train door reopen order to the driver by the indicator and buzzer.
- After issuing the departure permission order, if a passenger is left between platform doors and train, or if platform doors fail to close properly, platform attendant will press the emergency stop button on the station control panel. This sends an ATC stop signal to STO, preventing the train from departing regardless of driver operation. Additionally, if sensors detect a passenger between the platform doors and the train, an alert is automatically sent to platform attendant via the station control panel, which supports platform attendant's supervision at step 7.
- Once these issues are resolved, the operation restarts from step 5. If train doors remain closed, restart from step 8.
- An interlock circuit is implemented to ensure that the vehicle's acceleration circuit cannot be electrically activated under any circumstances if the train doors are not fully closed, regardless of input from either the driver or the system.

5.1.2 Running Phase

In this phase, the train runs between stations under ATO's interstation running mode, following the timetable while adhering to the ATC maximum speed limit. ATC continuously compares the actual speed with the permitted speed and will automatically apply the brakes if the train approaches or exceeds that limit, whether under ATO or manual control.

Normal procedures

1. ATO generates an optimal speed profile based on the received ATC signal, operation schedule, stored vehicle performance data, and track data (gradients, tunnels, curves, etc.). This calculation is updated every 0.1 seconds.
2. ATO controls train speed according to the generated speed profile.

Manual Intervention by the Driver

- The driver can manually switch ATO's interstation running mode on and off by pressing the switch. Or if the driver manually applies brakes, ATO automatically turns off, prioritizing the driver's manual operation. In any case, ATO does not automatically resume unless manually reactivated.
- ATC remains active at all times, regardless of whether ATO is enabled or disabled. The driver cannot disable ATC.

Emergency Stop/Slowdown

- OCC may issue an emergency stop/slowdown command depending on the situation. If the command is transmitted remotely via signal, the maximum allowable speed (ATC signal) and ATO speed profile are updated accordingly, allowing ATO/ATC to automatically apply the necessary braking.
- If OCC lacks time to set an emergency stop/slowdown signal, the instruction may be delivered verbally to the train driver via train radio. In this case, the driver must manually apply brakes.
- Emergency stop requests may also come from train conductors or passengers in response to an emergency situation inside the cabin.

5.1.3 Stopping Phase

This phase refers to the period when the train approaches a stopping station, decelerates, and comes to a precise stop at the designated stopping position. During this phase, ATO operates

in TASC mode. Specifically, TASC is responsible for controlling the braking once the train's speed falls below 30 km/h.

Normal procedures

1. As the train approaches the stopping station, it receives precise distance information to the stopping position via TASC ground transponders, activating the TASC function within ATO.
2. TASC generates a braking profile for the designated stopping position.
3. TASC controls braking to bring the train to a stop at the designated platform position.
4. Once the train has come to a complete stop, train driver applies manual brakes.
5. TASC detects that the train is stationary and turns off (brake command from TASC is released).

Manual Intervention by the Driver

- When the driver applies manual brakes, TASC remains active. The system prioritizes the stronger braking control of either the TASC or the manual brakes.

5.2 System Losses and Hazards

As the first step of the STPA analysis, the system losses and hazards are identified. For the high-speed rail with STO, the following simple two losses were defined according to safety.

Losses

L-1 Loss of life or injury to people

L-2 Loss of or damage to vehicle or objects outside of vehicle

The system-level hazards leading these two losses were defined as follows.

System-level hazards

H-1 Train does not maintain adequate distance from other trains or obstacles [L-1, L-2]

H-2 Train does not stay on the track (i.e., Train derailment) [L-1, L-2]

H-3 Train moves while a passenger is physically trapped in a train door [L-1]

H-4 Train moves while a passenger is positioned between platform doors and train [L-1]

H-5 Train stops outside the allowable tolerance range of the designated stopping position [L-1, L-2]

H-6 Train does not stop at a location where passengers can safely evacuate during an emergency [L-1]

H-1 and H-2 concern physical track hazards and interactions with other trains, where collisions and derailments—once they occur—can severely affect human life and infrastructure. Collisions result from failing to maintain enough distance from other trains, and derailments happen when entering curves or turnouts at excessive speeds. Even after the introduction of STO, preventing such high-impact hazards remains the top priority in safety design.

H-3 and H-4 involve passengers during boarding and alighting. H-3 is the hazard of departing with a passenger caught in the door, while H-4 is the hazard of starting the train when a passenger is still between the train and platform doors. The platform attendant, the driver, and the door systems must all confirm that it is safe to depart. With STO, some duties once handled by the conductor will shift to the driver, requiring a review of new hazard scenarios.

H-5 concerns overshooting the designated stop position, potentially causing door/platform misalignment or placing part of the train off the platform. In extreme cases, there is a risk of collision with station facilities. After STO introduction, station stops will rely largely on TASC, requiring new safety considerations.

H-6 addresses emergencies that require stopping only in safe locations. For instance, in the event of a train fire necessitating evacuation, the train must not stop in a tunnel or on a bridge. Because high-speed rail has long distances between stations, ensuring reliable and prompt station stops is crucial. In such high-stakes scenarios requiring advanced operational decisions, smooth coordination between human operators and the STO system is essential.

5.3 Control Structure

The second step in the STPA analysis is to create a control structure describing the high-speed rail with STO.

5.3.1 High-level Control Structure

Figure 7 is a high-level control structure that covers all operational phases described in

Section 5.1, placing the Operation Control Center (OCC) at the top in a top-down hierarchy. Although the OCC does not typically control the platform attendant during departure, the attendant may report to the OCC in abnormal situations so that the OCC can respond with appropriate control actions. Therefore, the OCC is positioned at the top level.

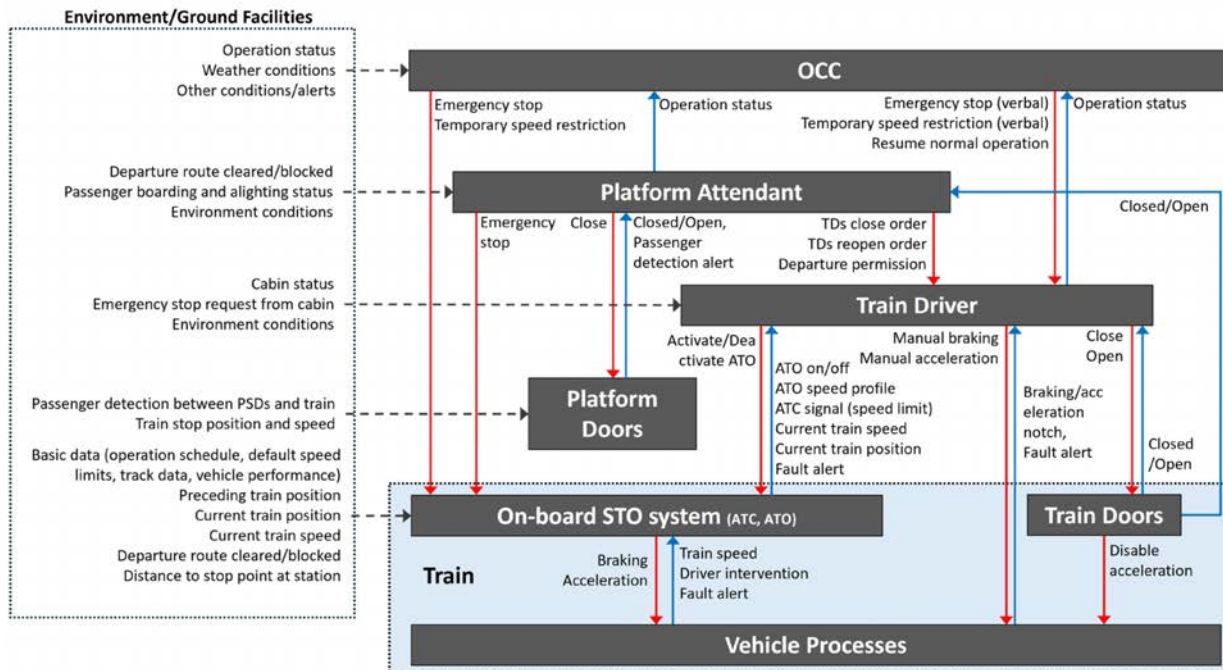


Figure 7: High-level Control Structure.

For an enlarged version of the image, see **Appendix A.1**.

Symbology: (Consistent through all control structures)

Downward (red) arrows: Control actions

Upward (blue) arrows: Feedback

Horizontal dotted (gray) arrows: Other Inputs

Because certain components and control actions only apply to specific phases (for example, the platform attendant is only involved in departure phase), the high-level control structure can be divided into two parts: one for departure phase, and the other for running and stopping phases. This focus on relevant components allows us to zoom in for more detailed analysis.

5.3.2 Control Structure for Departure Phase

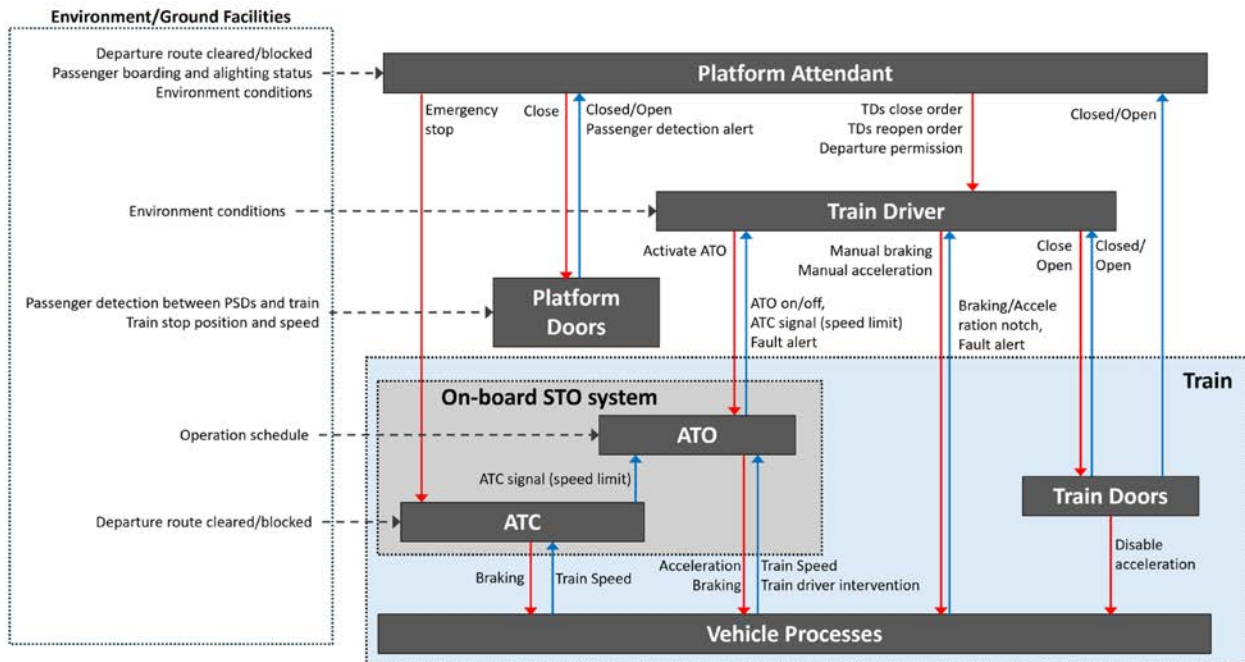


Figure 8: Control Structure for Departure Phase

For an enlarged version of the image, see **Appendix A.2**.

Figure 8 shows the control structure for departure phase, with the platform attendant at the top. It highlights the attendant’s platform safety checks and instructions, along with the driver’s door and departure operations. The STO system is divided between ATC and ATO. This explicitly shows the control action sequence: once safety checks are complete, the driver activates the ATO, and the ATO accelerates the train. It also indicates that ATC can apply the brakes in response to an emergency-stop command from the platform attendant, or if the train accelerates while the departure route is blocked.

5.3.3 Control Structure for Running and Stopping Phases

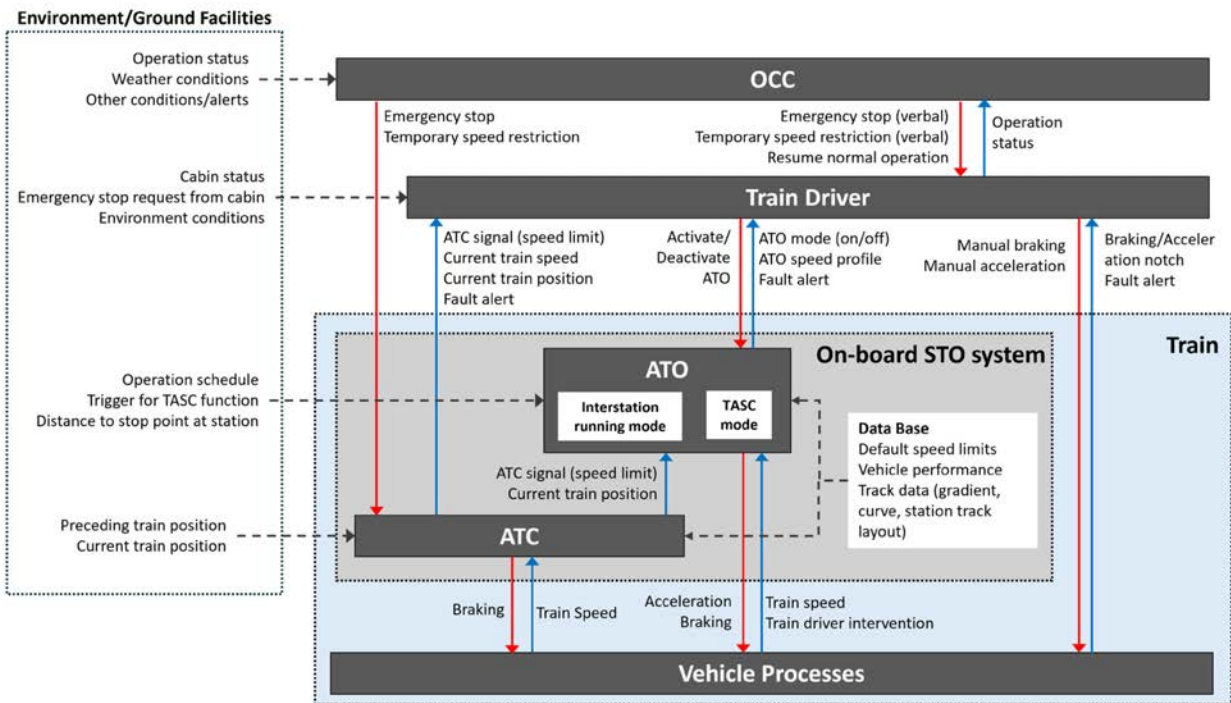


Figure 9: Control Structure for Running and Stopping Phases

For an enlarged version of the image, see **Appendix A.3**.

Figure 9 shows the control structure for the running and stopping phases. The OCC is placed at the top, and the STO system is divided between ATC and ATO just as in Figure 8. Because ATC and ATO are more actively involved during these phases, the relevant feedback, input information, and ATO modes are shown in more detail than in Figure 8. The ATO has two modes: interstation running mode and TASC mode. The ATO itself has two modes: interstation running mode and TASC mode.

While some control actions, such as the “manual braking” performed by the train driver, appear in both control structures of Figure 8 and Figure 9, most can be distinctly classified into those in two control structures. Therefore, the subsequent analysis will be based on these two control structures.

5.3.4 Defined Control Actions

The control actions determined are defined below, including what controller is acting on which controlled process. The following section is organized by phase. The format of each

bulleted control action is as follows:

- **Control Action** (*Controller → (acts on) Controlled Process*)
Definition

Control Actions Common in All Phases (Figure 8 and Figure 9)

- **Manual braking** (*Train Driver → Vehicle Processes*)
Train driver adjusts the brake handle, directly commanding the vehicle processes to brake at the chosen braking notch level.
- **Manual acceleration** (*Train Driver → Vehicle Processes*)
Train driver adjusts the master controller, directly commanding the vehicle processes to accelerate at the chosen acceleration notch level.
- **Activate ATO** (*Train Driver → ATO*)
Train driver turns on the ATO interstation running mode by pressing a button. This is done with when starting the train during the departure phase or when switching the ATO interstation running mode from off to on in the running phase.
- **Acceleration** (*ATO → Vehicle Processes*)
ATO commands the vehicle processes to accelerate according to its generated speed profile.
- **Braking (ATO)** (*ATO → Vehicle Processes*)
ATO commands the vehicle processes to brake according to its generated speed profile or TASC braking profile.
- **Braking (ATC)** (*ATC → Vehicle Processes*)
ATC commands the vehicle processes to brake when the train's speed approaches or exceeds the speed limit set by ATC signal.

Control Actions in Departure Phase (Figure 8)

- **Emergency stop** (*Platform attendant → ATC*)
Platform attendant sends a stop signal to on board ATC by pressing a button on the station control panel, preventing the train from departing regardless of driver operation.
- **Close platform doors** (*Platform attendant → Platform doors*)
Platform attendant closes platform doors by pressing a button.
- **Train doors close order** (*Platform attendant → Train Driver*)
Platform attendant sends the train door close order to the driver by pressing a button.
- **Train doors reopen order** (*Platform attendant → Train Driver*)
Platform attendant sends the train door reopen order to the driver by pressing a button

especially when a passenger is trapped in the train door.

- **Departure permission** (*Platform attendant → Train Driver*)

Platform attendant sends the departure permission order to the driver by pressing a button.

- **Close train doors** (*Train Driver → Train Doors*)

Train driver closes the train doors using a switch in the driver's cab

- **Open train doors** (*Train Driver → Train Doors*)

Train driver opens the train doors using a switch in the driver's cab after the train stops at the station or when platform attendant issues the train door reopen order.

- **Disable acceleration** (*Train Doors → Vehicle Processes*)

When the train doors are not fully closed, an interlock circuit in the train doors interrupts the vehicle's acceleration circuit, electrically disabling any acceleration command.

Control Actions in Running and Stopping Phases (Figure 9)

- **Emergency stop** (*OCC → ATC*)

OCC sends an emergency stop signal to on-board ATC via ground infrastructure remotely.

- **Temporary speed restriction** (*OCC → ATC*)

OCC sends a temporary speed restriction signal to on-board ATC via ground infrastructure remotely.

- **Emergency Stop (verbal)** (*OCC → Train Driver*)

OCC issues an emergency stop order verbally to train driver via train radio when OCC lacks time to set an ATC signal.

- **Temporary speed restriction (verbal)** (*OCC → Train Driver*)

OCC issues a temporary speed restriction order verbally to train driver via train radio when OCC lacks time to set an ATC signal.

- **Resume Normal Operation** (*OCC → Train Driver*)

OCC issues a resume normal operation order verbally to release verbal emergency stop/slowdown orders.

- **Deactivate ATO** (*Train driver → ATO*)

Train driver turns off the ATO interstation running mode by pressing a button to switch to manual operation.

5.4 Unsafe Control Actions

Based on these control actions, unsafe control actions that could lead to system-level hazards were identified according to the four categories. Table 3 provides examples of UCAs derived from the “Manual Braking” control action by the train driver. For additional UCAs, see **Appendix B: UCAs**.

Some terms and phrases are used in the creation of UCAs to help provide context for the action. For the reader’s understanding, these terms are here defined:

- **Critical track hazard:** Track hazard that requires an immediate stop (e.g., track obstruction, earthquake, extreme weather, or emergency in the cabin).
- **Moderate track hazard:** Track hazard that requires speed reduction(e.g., track maintenance, or adverse weather).
- **The train does not automatically brake:** A situation where the train does not automatically apply the necessary brakes due to reasons such as the OCC not setting ATC signals for track hazards.

Table 3: Example of Identified UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Manual braking	UCA-32: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2] UCA-33: Train driver does not	UCA-36: Train driver applies insufficient manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]	UCA-37: Train driver applies manual brakes too late after the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2] UCA-38: Train driver applies	UCA-40: Train driver stops applying manual brakes too early before the train comes to a complete stop when the train does not automatically brake for a critical track

	apply manual brakes when the train has a critical fault condition. [H-1, H-2]		manual brakes too late after the train has a critical fault condition. [H-1, H-2]	hazard. [H-1, H-2] UCA-41: Train driver stops applying manual brakes too early before reducing speed to the target speed limit when the train does not automatically brake for a moderate track hazard. [H-1, H-2]
--	---	--	---	---

Identified UCAs can be translated into safety requirements for each controller’s behavior. Table 4 shows the safety requirements for the driver’s manual braking, derived from the UCAs in Table 3. For additional safety requirements, see **Appendix C: Safety Requirements**.

Table 4: Example of Safety Requirements

Requirements
R-32: Train driver must apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [UCA-32]
R-33: Train driver must apply manual brakes when the train has a critical fault condition. [UCA-33]
R-36: Train driver must not apply manual brakes that is insufficient to reduce speed to the target speed limit (or to stop) by the start point of the track hazard when the train does not automatically brake for a critical/moderate track hazard. [UCA-36]
R-37: Train driver must apply manual brakes within TBD seconds after the train does not automatically brake for a critical/moderate track hazard. [UCA-37]

R-38: Train driver must apply manual brakes within TBD seconds after the train has a critical fault condition. [UCA-38]

R-40: Train driver must not stop applying manual brakes before the train comes to a complete stop when the train does not automatically brake for a critical track hazard. [UCA-40]

R-41: Train driver must not stop applying manual brakes before reducing speed to the target speed limit when the train does not automatically brake for a moderate track hazard. [UCA-41]

5.5 High-level Scenarios

For scenario generation, high-level scenarios were first identified following the new formal approach proposed by Thomas[19]. The original scenario generation method in the STPA Handbook [12] —searching backward or forward along the control loop to find how a hazard arises—remains effective. However, the new method provides more structure, clarity, and coverage checks, allowing users to systematically produce scenarios and verify more easily whether anything is missing.

This new scenario method defines four scenario classes:

- **Class 1:** The controller issues an unsafe control action despite having correct feedback or inputs.
- **Class 2:** The controller issues an unsafe control action because it received incorrect or unsafe inputs.
- **Class 3:** The controller issues a safe control action, but something in the control path (or conflict with another controller) effectively causes a condition as if the UCA had occurred.
- **Class 4:** The UCA did not occur and was not received, yet the controlled process behaves as though it did.

Figure 10 visually summarizes these four classes. This figure shows where in the control loop an unsafe element can arise in each class and turn into a hazard. It also shows that these four classes comprehensively analyze all parts of the control loop that could be unsafe.

STPA: Four Classes of Formal Scenarios

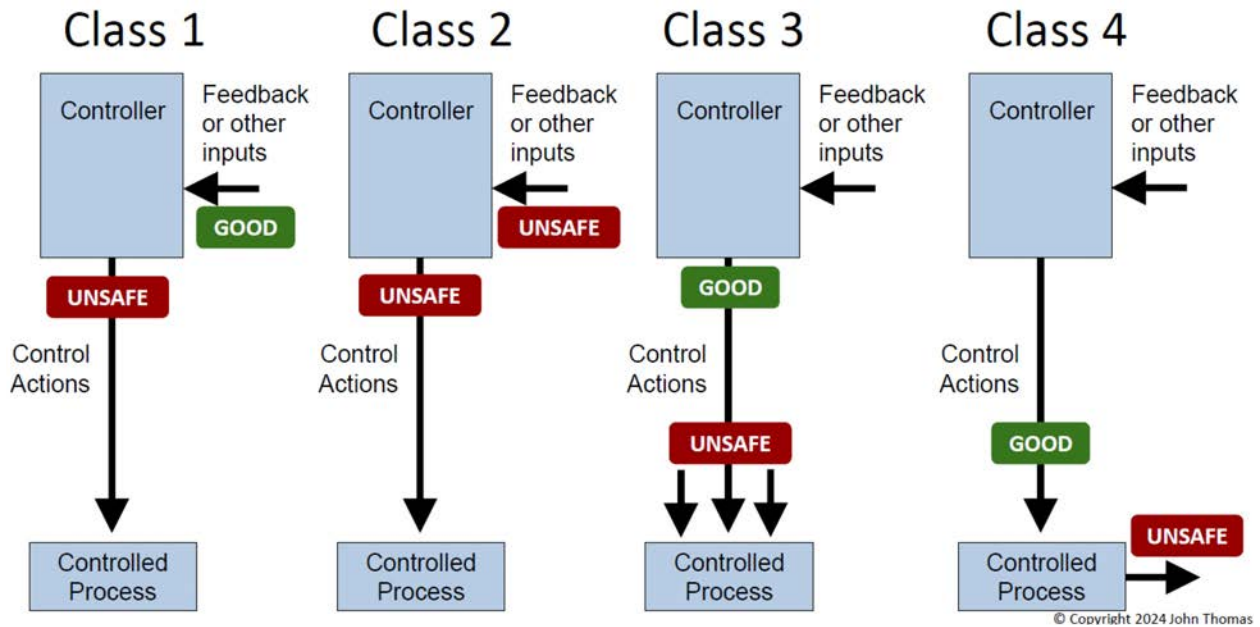


Figure 10: Four Classes of Formal Scenarios[19]

By systematically covering these four classes for each UCA, a more rigorous, comprehensive set of scenarios emerges. In this study, the method is used to draft high-level scenarios, and refined scenarios are developed for those requiring additional detail. Table 5 serves as a template for creating basic scenarios for each type of UCA. Each high-level scenario is stated in a concise two-sentence format that captures its essential features. presents examples of high-level scenarios derived from the UCAs in Table 1, generated using this approach.

Table 5: A Template to High-level Scenarios for Each Type of UCA

UCA-#: (For reference)				
...				
	UCA Type 1: not providing causes Hazard (UCA-#)	UCA Type 2: providing causes Hazard (UCA-#)	UCA Type 3: too early, too Late, out of order (UCA-#)	UCA Type 4: stopped too soon, applied too long (UCA-#)
Scenario Class 1: Unsafe	1)<controller> doesn't provide <cmd> when	1)<controller> provides <cmd> when <context>	1)<controller> provides <cmd> too late/early	1)<controller> stops/continues providing <cmd>

Controller Behavior	<context> 2)<controller> received feedback (or other inputs) that indicates <context>	2)<controller> received feedback (or other inputs) that indicates <context>	after/before <context> 2)<controller> received feedback (or other inputs) that indicates <context> on time / in order	too soon/long 2)<controller> received feedback (or other inputs) that indicates <context> on time
Scenario Class 2: Unsafe Feedback Path	1)feedback (or other inputs) received by <controller> does not adequately indicate <context> 2)<context> is true	1)feedback (or other inputs) received by <controller> does not adequately indicate <context> 2)<context> is true	1)feedback (or other inputs) received by <controller> does not indicate <context> (too late/early/out of order) 2)<context> is true	1)feedback (or other inputs) received by <controller> does not indicate <context> (inappropriate duration) 2)<context> is true
Scenario Class 3: Unsafe Control Path	1)<controller> does provide <cmd> when <context> 2)<cmd> is not received by <controlled process> when <context>	1)<controller> does not provide <cmd> when <context> 2)<controlled process> receives <cmd> when <context>	1)<controller> does not provide <cmd> <context> (not too late/early/out of order) 2)<cmd> is received by <controlled process> <context> (too late/early/out of order)	1)<controller> provides <cmd> with appropriate duration 2)<cmd> is received by <controlled process> with <context> (inappropriate duration)
Scenario Class 4: Unsafe Controlled	1)<cmd> is received by <controlled process> when <context>	1)<cmd> is not received by <controlled process> when	1)<cmd> is not received by <controlled process>	1)<cmd> is received by <controlled process> with

Process Behavior	2)<controlled process> does not respond by <...>	<context> 2)<controlled process> responds by <...>	<context> (not too late/early/out of order) 2)<controlled process> responds by <...> <context> (too late/early/out of order)	appropriate duration 2)<controlled process> does not respond by <...> with <context> (inappropriate duration)
------------------	--	---	---	--

To illustrate how the four-class template is applied in practice, the following generates a sample set of high-level scenarios for several UCAs from Table 3.

- UCA Type 1: Not providing causes hazard
UCA-32: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]
- UCA Type 2: Providing causes hazard
UCA-36: Train driver applies insufficient manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]
- UCA Type 3: Too early, too Late, out of order
UCA-37: Train driver applies manual brakes too late after the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]
- UCA Type 4: Stopped too soon, applied too long
UCA-40: Train driver stops applying manual brakes too soon before the train comes to a complete stop when the train does not automatically brake for a critical track hazard. [H-1, H-2]

These UCAs are all related to situations where the train driver is required to apply manual brakes in the context of “the train does not automatically brake for a critical/moderate track hazard.” Figure 11 shows the simplified control loop related to these UCAs. Here, the controller is the train driver, the controlled process is the vehicle processes, and the control action is manual braking. The train driver makes decisions mainly based on feedback from the train, including vehicle processes, and control actions from the OCC as input. The context

of “the train does not automatically brake for a critical/moderate track hazard” specifically refers to situations where the OCC issues an emergency stop or temporary speed restriction order in response to a critical/moderate track hazard, and the instructions are only verbal and not controlled by ATC signals. Figure 11 also shows where each of the four scenario types is associated with the control loop.

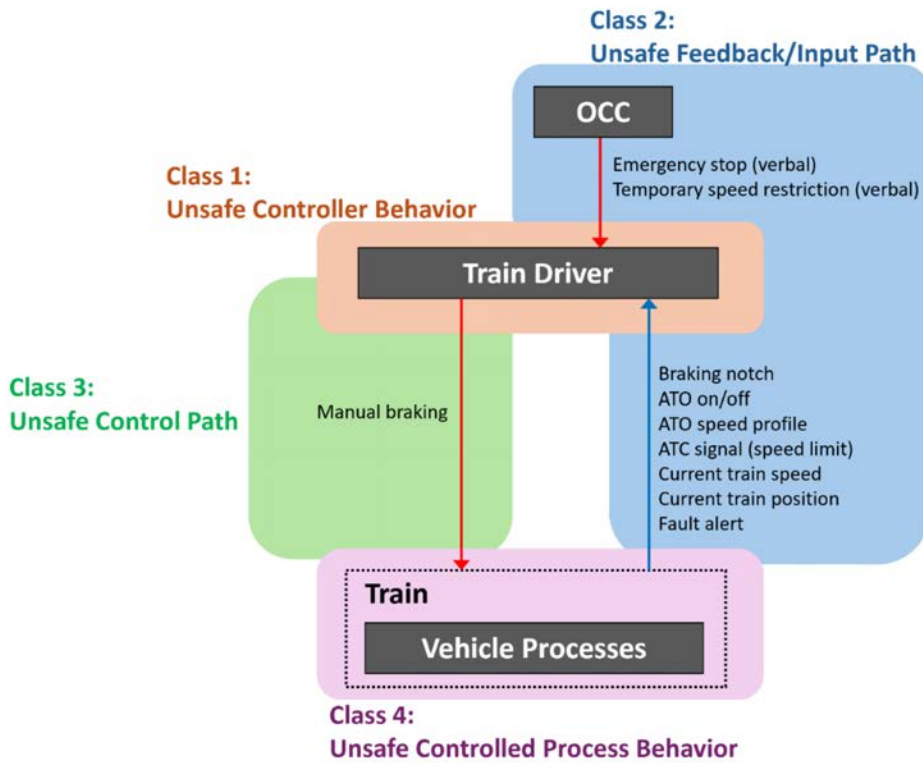


Figure 11: Scenario Classes in the Train Driver’s Control Loop

Figure 12 shows an example of creating high-level scenarios for UCA-32 (Type 1: Not providing causes hazard). At this stage the terms feedback or input remain abstract. The scenario will be refined through analysis later by specifying and detailing the content of feedback/input, such as ATC signals or emergency stop orders from the OCC.

UCA Type 1: Not providing causes hazard

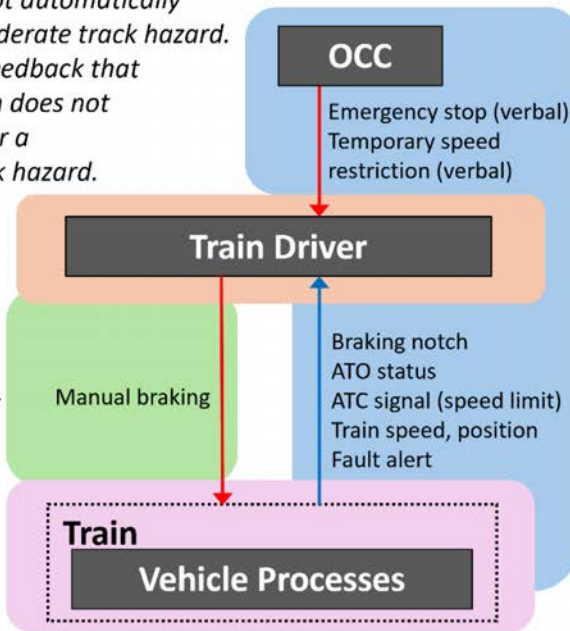
UCA-32: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]

Class 1: Unsafe Controller Behavior

- Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard.
- Train driver received feedback that indicates that the train does not automatically brake for a critical/moderate track hazard.

Class 3: Unsafe Control Path

- Train driver apply manual brakes when the train does not automatically brake for a critical/moderate track hazard.
- Manual braking command is not received by vehicle processes when the train does not automatically brake for a critical/moderate track hazard.



Class 2: Unsafe Feedback/Input Path

- Feedback received by train driver does not adequately indicate that the train does not automatically brake for a critical/moderate track hazard.
- It is true that the train does not automatically brake for a critical/moderate track hazard.

Class 4: Unsafe Controlled Process Behavior

- Manual braking command is received by vehicle processes when the train does not automatically brake for a critical/moderate track hazard.
- Vehicle processes does not respond by applying brakes.

Figure 12: High-level Scenario Generation for UCA Type 1

The scenarios can also be expressed in a table format, similar to the template in Table 5. Table 6 shows the same set of high-level scenarios as those presented in Figure 12, but in a table format. In Table 6, the structure of the table has been modified by switching the rows and columns from the original template in Table 5.

Table 6: High-level Scenario Generation for UCA Type 1

UCA-32: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]				
	Scenario Class 1: Unsafe Controller Behavior	Scenario Class 2: Unsafe Feedback Path	Scenario Class 3: Unsafe Control Path	Scenario Class 4: Unsafe Controlled Process Behavior
UCA Type 1: not providing causes Hazard (UCA-32)	HS-32.1: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. Train driver received feedback that indicates that the train does not automatically brake for a critical/moderate track hazard.	HS-32.2: Feedback received by train driver does not adequately indicate that the train does not automatically brake for a critical/moderate track hazard. It is true that the train does not automatically brake for a critical/moderate track hazard.	HS-32.3: Train driver apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. Manual braking command is not received by vehicle processes when the train does not automatically brake for a critical/moderate track hazard.	HS-32.4: Manual braking command is received by vehicle processes when the train does not automatically brake for a critical/moderate track hazard. Vehicle processes does not respond by applying brakes.

As shown in Table 5, the syntax for each scenario class differs depending on the UCA type. The same template was applied to the three remaining types, and the resulting high-level scenarios are presented in Figure 13, Figure 14, and Figure 15. While the structure of each figure follows the same format as in Figure 12, the logic and emphasis vary slightly according to the nature of each UCA type.

Figure 13 shows the high-level scenarios generated for UCA-36 (Type 2: Providing causes hazard). Here the unsafe element is “applying insufficient manual brakes,” and the four classes track how that element could originate with the driver, with the feedback, with the command path, or with the vehicle response.

UCA Type 2: Providing causes hazard

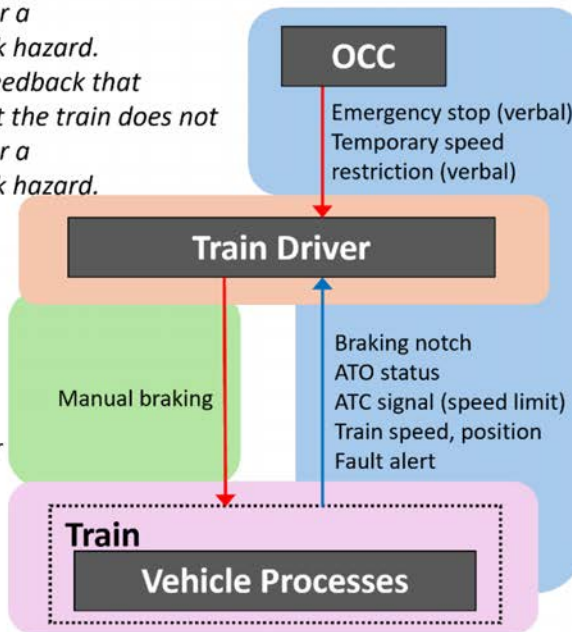
UCA-36: Train driver applies insufficient manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]

Class 1: Unsafe Controller Behavior

- Train driver applies insufficient manual brakes when the train does not automatically brake for a critical/moderate track hazard.
- Train driver received feedback that correctly indicates that the train does not automatically brake for a critical/moderate track hazard.

Class 3: Unsafe Control Path

- Train driver does not apply insufficient manual brakes when the train does not automatically brake for a critical/moderate track hazard.
- Vehicle processes receives insufficient manual brakes command when the train does not automatically brake for a critical/moderate track hazard.



Class 2: Unsafe Feedback/Input Path

- Feedback received by train driver does not adequately indicate that the train does not automatically brake for a critical/moderate track hazard.
- It is true that the train does not automatically brake for a critical/moderate track hazard.

Class 4: Unsafe Controlled Process Behavior

- Insufficient manual brakes command is not received by vehicle processes when the train does not automatically brake for a critical/moderate track hazard.
- Vehicle processes respond by applying insufficient brakes.

Figure 13: High-level Scenario Generation for UCA Type 2

Figure 14 presents high-level scenarios for UCA-37 (Type 3: Too early, too late, out of order). In this case the unsafe element is late braking. The figure shows how the four classes map that late timing to different parts of the loop.

UCA Type 3: Too early, too Late, out of order

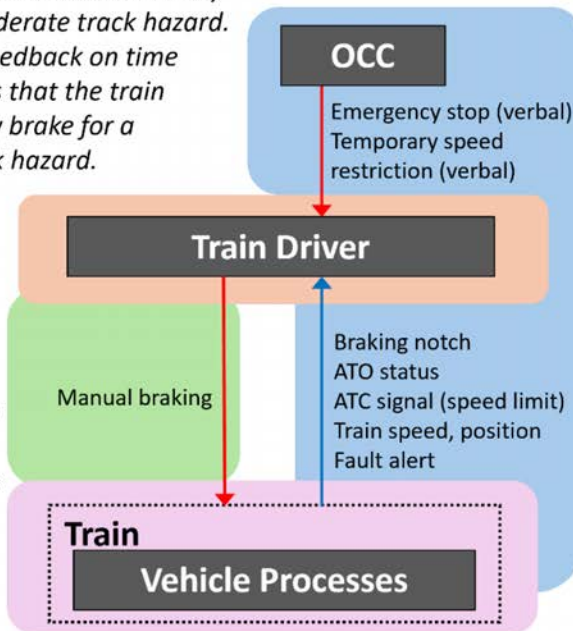
UCA-37: Train driver applies manual brakes too late after the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]

Class 1: Unsafe Controller Behavior

- Train driver applies manual brakes too late after the train does not automatically brake for a critical/moderate track hazard.
- Train driver received feedback on time that correctly indicates that the train does not automatically brake for a critical/moderate track hazard.

Class 3: Unsafe Control Path

- Train driver does not apply manual brakes too late after the train does not automatically brake for a critical/moderate track hazard.
- Manual braking command is received by vehicle processes too late



Class 2: Unsafe Feedback/Input Path

- Feedback received by train driver does not indicate that the train does not automatically brake for a critical/moderate track hazard.
- It is true that the train does not automatically brake for a critical/moderate track hazard.

Class 4: Unsafe Controlled Process Behavior

- Manual braking command is received by vehicle processes on time when the train does not automatically brake for a critical/moderate track hazard.
- Vehicle processes respond by applying brakes too late.

Figure 14: High-level Scenario Generation for UCA Type 3

Figure 15 presents high-level scenarios for UCA-40 (Type 4: Stopped too soon, applied too long). It follows the same pattern, showing how an early release of the manual brake can originate in each of the four classes

UCA Type 4: Stopped too soon, applied too long

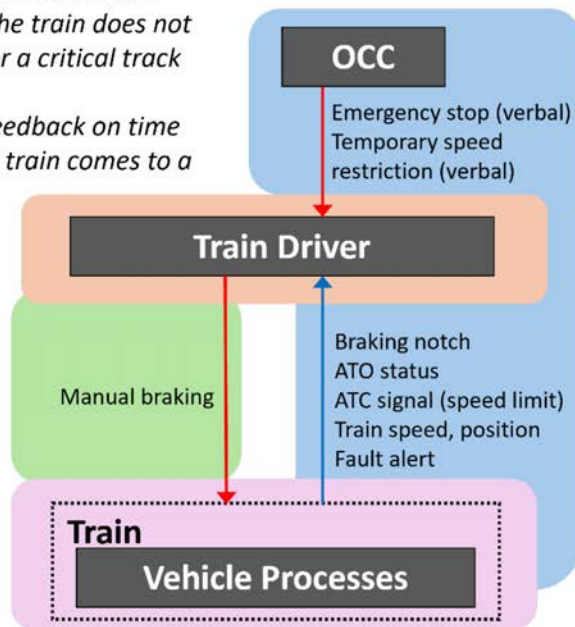
UCA-40: Train driver stops applying manual brakes too soon before the train comes to a complete stop when the train does not automatically brake for a critical track hazard. [H-1, H-2]

Class 1: Unsafe Controller Behavior

- Train driver stops applying manual brakes too soon before the train comes to a complete stop. when the train does not automatically brake for a critical track hazard.
- Train driver received feedback on time that indicates that the train comes to a complete stop.

Class 3: Unsafe Control Path

- Train driver stops applying manual brakes on time when the train comes to a complete stop.
- Stopping applying manual brakes is received by vehicle processes too soon.



Class 2: Unsafe Feedback/Input Path

- Feedback received by Train driver indicates that the train comes to a complete stop too soon when the train does not automatically brake for a critical track hazard.
- It is true that the train has not come to a complete stop.

Class 4: Unsafe Controlled Process Behavior

- Stopping applying brakes is received by vehicle processes on time.
- Vehicle processes respond by stopping brakes too soon.

Figure 15: High-level Scenario Generation for UCA Type 4

Each of these figures demonstrates how the four-class formal approach can be applied consistently while adapting to the unique characteristics of each UCA type. With this method, high-level scenarios for other UCAs can also be identified in a systematic and efficient way.

5.6 Refined Scenarios

After identifying UCAs and high-level scenarios in the previous sections, the next step is to

create refined scenarios. Each high-level scenario is examined in detail by asking questions such as “Why would the controller do this?” or “How could the process behave as though that UCA were issued?” This deeper investigation considers responsibilities, control algorithms, process models, feedback paths, and operating modes, including both failure and non-failure causes.

This section presents 11 representative refined scenarios covering various phases and controllers, each accompanied by proposed recommendations. The scenarios emphasize instances where hazards can occur even without physical or functional failures, focusing on cases in which the design behaves as intended yet still permits hazardous outcomes. Regarding the recommendations, the aim is to go beyond merely correcting human factors (e.g., “follow the manual” or “provide more training”) and include technical or design-oriented measures that can be incorporated into the system itself.

Note on Recommendations: All recommendations here are only potential design options. Whether any particular measure is adopted depends on further engineering and operational decisions. Once a recommendation is incorporated into the design, an updated STPA analysis should be performed—new control actions or feedback might need to be added to the control structure, and any additional hazard scenarios must be assessed.

Refined Scenario 1 (RS-4.3)

Unsafe Control Action

UCA-4: OCC provides a temporary speed restriction at an excessive speed or for an incorrect section when a moderate track hazard occurs. [H-1, H-2]

High-level Scenario

HS-4.3: OCC does not provide a temporary speed restriction at an excessive speed or for an incorrect section when a moderate track hazard occurs. ATC receives a temporary speed restriction at an excessive speed or for an incorrect section when a moderate track hazard occurs.

Refined Scenario

RS-4.3: *The OCC sets a reduced speed limit of 120 km/h in section A due to an environmental condition. However, part of Section A (called Section B) already had a 70 km/h limit (ATC signal) due to another condition, like track maintenance. At almost the same time, OCC learns that maintenance is finished and attempts to remove the 70 km/h limit. However, the command “remove all speed restrictions in Section B” removes not only the 70 km/h limit*

for maintenance but also the new 120 km/h limit in Section B. ATC believes that Section B (inside Section A) now has no speed restriction, so trains run at normal speed in Section B.

Recommendations

- Rather than using a single “remove all” command for an entire geographic section, the OCC must specify precisely which individual speed restriction(s) to remove. This prevents unintentionally deleting newly added or still-necessary limits.
- Provide an integrated map or labeling system that clearly shows overlapping or nested sections (e.g., Section B within Section A) and the distinct restrictions in each. This helps avoid confusion about multiple limits in partially overlapping areas.

Refined Scenario 2 (RS-11.2)

Unsafe Control Action

UCA-11: OCC provides an order to resume normal operation when a critical/moderate track hazard is not finished. [H-1, H-2, H-6]

High-level Scenario

HS-11.2: The feedback received by OCC does not adequately indicate that a critical/moderate track hazard is not finished.

Refined Scenario

RS-11.2: The OCC received a report from outside that there might be a hazardous object (such as a large piece of metal or a fallen tree) on the track in Section A. The OCC instructed the train driver approaching Section A to manually slow down to 70 km/h and visually check if there were any obstacles. Shortly after entering Section A, the driver found a small object (such as a branch or part of a sheet). The driver reported to the OCC that there was a small object on the track, but it would not affect train operation. The OCC trusted the driver’s report and decided that no further checking was needed. Then, the OCC told the train to return to normal speed. However, in reality, a larger and more dangerous object was located farther inside Section A, and it was not related to the small object found earlier. As a result, the train entered the area with the dangerous object at normal speed.

Recommendations

- Introduce a secondary check or question to the reporting driver: “Did you check the entire section length or only the entrance area?” The OCC operator can then decide whether partial confirmation is enough.
- After issuing a verbal order for manual braking in Section A, OCC will follow up by setting ATC signal of the temporary speed restriction for that entire section. This ensures that even if the driver were to accelerate beyond the verbally instructed limit, the ATC would prevent

the train from exceeding the specified speed.

- Where operationally allowed, the driver might set a “local” or “manual” temporary speed restriction into ATO/ATC directly (e.g., via a cab interface), rather than needing an OCC voice instruction. This would be distinct from a permanent or scheduled limit. A simple UI could show how long this “local” restriction remains active or prompt the driver to confirm if it should be released.

Refined Scenario 3 (RS-21.2)

Unsafe Control Action

UCA-21: Platform attendant provides departure permission when a passenger is physically trapped in the train door. [H-3]

High-level Scenario

HS-21.2: The feedback received by platform attendant does not adequately indicate that a passenger is physically trapped in the train door.

Refined Scenario

RS-21.2: A passenger wore a bag with a very thin strap, which got stuck in the passenger door. But the door system did not detect this thin obstruction, and the pilot lamp (used to confirm doors were fully closed) switched off as if all doors were fully closed. Because of that, the platform attendant got no sign that the door was still partly open and thought departure was fine, giving departure permission. The train driver started the departure process without knowing the passenger’s bag strap was caught in the door.

Recommendations

- Implement a system (the anti-drag detection function) that, when the train starts to depart, activates the emergency brake if any abnormal pulling force or vibration is detected near the doors. This serves as a final safeguard to prevent passengers from being dragged along during operation in the event that door entrapment detection fails.

Refined Scenario 4 (RS-22.1)

Unsafe Control Action

UCA-22: Platform attendant provides departure permission when a passenger is positioned between the platform doors and the train. [H-4]

High-level Scenario

HS-22.1: Platform attendant provides departure permission when a passenger is positioned between the platform doors and the train. Platform attendant received feedback that correctly indicates that a passenger is positioned between the platform doors and the train.

Refined Scenario

RS-22.1: *A passenger stood between the train door and the platform screen door. This passenger was a short child, so the platform attendant could not see the child through direct sight or on the platform monitor. There was a sensor that could detect something between the platform screen door and the train door, and it sent an alert to the platform attendant. In most cases when this sensor was activated, the platform attendant could also visually confirm that a passenger was left between the doors, either by looking directly or through the monitor. Because of this, it became common for platform attendants not to pay enough attention to the sensor alert when they could not see anything through direct sight or on the platform monitor. In this case, the attendant ignored the sensor alert, failed to notice the child, and gave departure permission.*

Recommendations

- If the sensor issues a warning, configure the system so that platform staff must proactively enter a command on the terminal to clear the sensor warning before they can grant departure permission.
- Provide repeated training scenarios where only the sensor reacts and the monitor shows nothing, so attendants learn not to ignore sensor-based warnings.

Refined Scenario 5 (RS-29.1)

Unsafe Control Action

UCA-29: Train driver does not deactivate ATO when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2, H-6]

High-level Scenario

HS-29.1: Train driver does not deactivate ATO when the train does not automatically brake for a critical/moderate track hazard. Train driver received the feedback that correctly indicates that the train does not automatically brake for a critical/moderate track hazard.

Refined Scenario

RS-29.1: *The train driver learned from the conductor's report that an emergency (e.g., a violent attack) had occurred in the cabin, requiring an emergency stop at the next station so passengers could evacuate. However, the driver thought it was not necessary to deactivate the ATO at that moment, because the train should continue to the station rather than stopping immediately between stations. The next station was originally not scheduled for stopping, so the OCC needed to set a new ATC route to allow the train to stop there. Since the train continued to operate at high speed under the normal ATO schedule, it passed through the station before the OCC could complete the ATC stop route. As a result, the train*

had to continue to another station for passenger evacuation.

Recommendations

- During regular training, by educating train drivers on how long it takes for the OCC to set a stopping route via ATC, the drivers can estimate in advance how much time remains before the train must stop at the station and determine whether to slow down or speed up when communicating with the OCC.
- By adding an “Emergency Station Stop Request” button on the driver’s console, the driver can immediately alert the OCC to begin setting up the required station-stop route. Once pressed, this switch also deactivates and locks out ATO, requiring the driver to operate the train manually.

Refined Scenario 6 (RS-32.1)

Unsafe Control Action

UCA-32: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]

High-level Scenario

HS-32.1: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. Train driver received the feedback that correctly indicates that the train does not automatically brake for a critical/moderate track hazard.

Refined Scenario

RS-32.1: The OCC received a report from outside that there was a moderate track hazard (e.g., obstructions on the track) ahead of the train’s path. With no time to set an ATC slowdown signal, the OCC verbally instructed the train driver to immediately reduce speed to 70 km/h manually and proceed at reduced speed. At the same time, the OCC discovered another track hazard (for example, excessive soil moisture levels due to heavy rainfall) in an even further section of track, and issued an additional slowdown signal via an ATC signal for that further section. Seeing an ATC slowdown signal reflected on the cab monitor, the driver mistakenly believed this new ATC speed limit was just the reflection of the original verbal instruction, thus concluding that manual slowdown was no longer necessary. Consequently, the driver continued traveling through the section that required manual slowdown at a higher speed.

Recommendations

- Instruct drivers that any manual slowdown order given to them remains in effect unless it is explicitly canceled by a verbal instruction from the OCC.
- (The same approach used in RS-11.2) After issuing a verbal order for manual braking in

Section A, OCC will follow up by setting ATC signal of the temporary speed restriction for that entire section. This ensures that even if the driver were to accelerate beyond the verbally instructed limit, the ATC would prevent the train from exceeding the specified speed.

- (The same approach used in RS-11.2) Where operationally allowed, the driver might set a “local” or “manual” temporary speed restriction into ATO/ATC directly (e.g., via a cab interface), rather than needing an OCC voice instruction. This would be distinct from a permanent or scheduled limit. A simple UI could show how long this “local” restriction remains active or prompt the driver to confirm if it should be released.

Refined Scenario 7 (RS-38.2)

Unsafe Control Action

UCA-38: Train driver applies manual brakes too late after the train has a critical fault condition. [H-1, H-2, H-5]

High-level Scenario

HS-38.2: The feedback received by train driver does not adequately indicate that the train has a critical fault condition.

Refined Scenario

RS-38.2: Normally, when the train passes the ground beacon before entering the station, TASC activates, a braking profile is generated, and the driver is notified that the ATO’s TASC function is enabled. However, if for some reason TASC does not activate upon passing the beacon, the system does not issue a clear “failed to activate” alert (because TASC is usually turned off and this in itself is not an error), causing the driver to assume TASC is working and wait for it to brake. It is only after the train does not slow down that the driver realizes TASC did not activate only after the train does not automatically slow down, and the driver applies manual brakes too late.

Recommendations

- The train driver is required to check that TASC is active before the train enters the platform area.
- Introduce a monitoring function that compares train speed, schedule data (whether a stop is planned at this station), and train location. The function judges if the train is entering the station and issues an error alert if TASC function is not activated in certain conditions.

Refined Scenario 8 (RS-53.4)

Unsafe Control Action

UCA-53: ATO applies insufficient brakes when the train approaches the designated stop position at the station. [H-5]

High-level Scenario

HS-53.4: Insufficient brakes command is not received by vehicle processes when the train approaches the designated stop position at the station. Vehicle processes respond by applying insufficient brakes.

Refined Scenario

RS-53.4: *In the conventional manual station-stop braking method, even if the final stop position was correct, if the driver had to use a stronger brake notch than usual multiple times, they would suspect a decline in brake performance and report it to maintenance. However, in the new system, as long as the ATO brings the train to a stop within the allowable stopping range, there will be no alerts even if a stronger brake notch than usual is applied. Over time, the wear on the brakes will accumulate invisibly, but the ATO will make corrections quietly without issuing any alerts. Eventually, the brakes will become insufficient and the train will overrun the designated platform position, resulting in [H-5].*

Recommendations

- Introduce a monitoring function that compares ATO’s expected brake notch with the actual brake notch. If the required brake level is consistently higher than nominal, trigger a maintenance alert before an actual overrun occurs.

Refined Scenario 9 (RS-56.2.1)

Unsafe Control Action

UCA-56: ATO applies acceleration when the train speed exceeds the speed limit. [H-1, H-2]

High-level Scenario

HS-56.2: The feedback received by ATO does not adequately indicate that the train speed exceeds the speed limit.

Refined Scenario

RS-56.2.1: *A temporary speed limit of 220 km/h was issued (only as a verbal instruction to the driver), and at that point, the speed profile created by the ATO was below 220 km/h, so the driver chose to continue with the ATO rather than switch to manual operation. However, due to another change in running conditions, the schedule-based speed profile was automatically updated, and the ATO began accelerating, exceeding the speed limit of 220 km/h.*

Recommendations

- Instruct drivers that if a temporary speed restriction is in effect but not reflected in the ATC signal and thus cannot be entered into the ATO, they must switch to manual operation regardless of the ATO's speed profile or the train's current speed.
- (The same approach used in RS-11.2) After issuing a verbal order for manual braking in Section A, OCC will follow up by setting ATC signal of the temporary speed restriction for that entire section. This ensures that even if the driver were to accelerate beyond the verbally instructed limit, the ATC would prevent the train from exceeding the specified speed.
- (The same approach used in RS-11.2) Where operationally allowed, the driver might set a "local" or "manual" temporary speed restriction into ATO/ATC directly (e.g., via a cab interface), rather than needing an OCC voice instruction. This would be distinct from a permanent or scheduled limit. A simple UI could show how long this "local" restriction remains active or prompt the driver to confirm if it should be released.

Refined Scenario 10 (RS-56.2.2)

Unsafe Control Action and High-level Scenario are the same as Refined Scenarios 9.

Refined Scenario

RS-56.2.2: A temporary speed limit of 220 km/h was issued by an ATC signal. However, within the onboard STO system, some software malfunction caused that ATC signal for the temporary speed limit not to be communicated to the ATO, so the ATO did not update its speed profile under that condition. There is no built-in feedback in the onboard STO system to check whether the ATC signal is correctly passed to the ATO, and the driver is not informed of it either. The driver can see the ATC signal itself and the current speed profile on the cab monitor, but unless the driver actively checks, there is no way to know if the ATO's speed profile really matches the ATC signal's requirements. As a result, the ATO's speed profile remained one that ignored the 220 km/h temporary speed limit, so the ATO tried to accelerate beyond that speed limit.

Recommendations

- Within the onboard STO system, the software should confirm that the ATO has correctly received the ATC signal. If it is not received correctly, trigger an ATO fault alert and switch the ATO off.
- When sending information to the driver's monitor, first gather and consolidate the ATO and ATC data centrally in the onboard STO system. At that point, check whether the ATO's speed profile meets the ATC signal. If it does not meet it, trigger an ATO fault alert and switch the ATO off.

Refined Scenario 11 (RS-57.2)

Unsafe Control Action

UCA-57: ATO applies acceleration when the train driver applies manual brakes. [H-1, H-2, H-3, H-4, H-6]

High-level Scenario

HS-57.2: The feedback received by ATO does not adequately indicate that the train driver applies manual brakes.

Refined Scenario

RS-57.2: After the train had stopped at the previous station, the software switched the ATO's TASC mode to off (standby). However, even though TASC mode itself was turned off, a control algorithm that prevents any driver intervention from overriding TASC mode remained enabled. While running in the ATO's interstation running mode after departing from the station, the driver tried to switch to manual operation by applying a one-notch brake for the section that required temporary manual operation. However, the remaining "preventing override" algorithm for TASC mode also prevented ATO's interstation running mode from being turned off, and the ATO continued sending acceleration command. The driver did not realize that the ATO's interstation running mode was still on and tried to coast by releasing the brakes, which caused the ATO to start accelerating again according to the speed profile.

Recommendations

- When the TASC mode is off (standby) after stopping at station, the system should perform an internal check to ensure that no "preventing override" algorithm for TASC mode is left active. If any leftover flag is detected, raise an error or disable ATO.
- Implement a rule into the final synthesis stage of the software that any manual command input immediately switches off the ATO's interstation running mode. Even if an upper-level setting is still trying to block manual intervention, the lowest-level logic treats the driver's manual command as absolute priority, which prevents the unintentional continuation of the ATO's interstation running mode.

6 Evaluation of STPA Applied to New High Speed Rail System

This chapter reviews the refined scenarios and recommendations described in Section 5.6 and shows how STPA can uncover more potential hazard scenarios than traditional failure-focused methods. Section 6.1 looks at the hazard scenarios and recommendations, pointing out what kinds of design problems they expose and how the suggested solutions differ from standard “reliability-based” approaches. Section 6.2 then covers the broader technical and academic contributions of using STPA, focusing on its value in early design stages, its whole-system view, its ability to handle non-failure scenarios, and how it supports improvements based on safety principles.

6.1 Discussion on Identified Scenarios and Recommendations

This section examines the eleven refined scenarios in Section 5.6 along with the related recommendations. These scenarios show many situations where hazards happen not because hardware fails but because the system’s design or procedures are inadequate or inconsistent, even though the hardware is working as intended. This shows a key feature of STPA that sets it apart from methods like FMEA or FTA, which often miss unsafe conditions that arise precisely because everything is “working correctly.”

The following parts discuss how each scenario’s recommended solutions fit into different types of changes, stressing how they can be built into the design in ways that differ from traditional approaches.

1. Redundant components

Although hardware redundancy is often considered in FMEA or FTA, many scenarios in Section 5.6 do not come from broken components. Rather, they involve unsafe interactions among subsystems and human operations, all functioning normally—making mere redundancy insufficient.

Indeed, no recommendation in Section 5.6 explicitly proposes adding redundant hardware. Most of the suggested measures focus on revising functionalities, procedures, or introducing new UIs (“software or operational” approaches). While redundancy can still be valuable in some contexts, the hazard scenarios identified here arise primarily from design gaps under

normal conditions, thus solutions need more than just extra hardware.

2. Improved human procedures

Improved human procedures (e.g., strengthening operator training or strictly enforcing manuals) are already recognized in conventional methods, although they are often treated as supplementary measures. However, STPA encourages the development of system-level mechanisms that absorb or mitigate human mistakes rather than merely stating “operators need to pay attention.”

Concretely, several recommendations in this study focus on enriching operational steps or training. For instance:

- RS-11.2: Adding extra confirmation steps or verbal questions (“Did you check the entire section?”) to avoid prematurely assuming everything is safe.
- RS-22.1: Providing repeated training scenarios so that staff do not dismiss a sensor alert.
- RS-29.1: Training drivers about how long the OCC needs to set a stopping route by ATC signals, improving the driver’s knowledge to time speed adjustments properly.
- RS-32.1: Clarifying that a verbally ordered manual slowdown remains valid unless explicitly canceled by the OCC, ensuring the driver does not abandon manual deceleration incorrectly.
- RS-38.2: Requiring the driver to physically check whether TASC is active before entering the platform.
- RS-56.2.1: Instructing that if a temporary speed restriction is verbally issued only, the driver must switch to manual operation to avoid confusion with other ATO commands.

All of these rely more on new operational steps or reinforced training for humans rather than large-scale UI or software changes. By analyzing human procedures at the same depth as hardware or software design, STPA produces practical operational improvements that go beyond simply telling humans “be more careful.”

3. Improved functional requirements for automation and software

In some scenarios, the ATO or TASC systems appear to function “normally,” but hazards still arise due to unfinished mode transitions, missed sensor alerts, or logical errors. These situations emphasize the need for stronger functional requirements for automation and software. While FMEA focuses on component or software failures, STPA digs deeper into

the software logic itself and reveals places where requirements are either missing or insufficient. For instance:

- RS-38.2 addresses “TASC-off is not explicitly fed back as an error, causing the driver to assume TASC is working.” The recommended solution is to monitor train speed and location and generate an alert if TASC remains off when approaching the station.
- RS-53.4 notes “frequent use of a higher brake notch is hidden because the ATO can still stop the train properly,” so it recommends comparing the ATO’s expected brake notch with the actual brake input and triggering maintenance requests if they diverge too often.
- RS-56.2.2 suggests continuously verifying that ATC signals have been received by the ATO, disabling ATO if mismatched, and merging ATO/ATC data to check for contradictory speed profiles.
- RS-57.2 proposes modifications to ATO-mode logic, e.g., forcibly halting ATO’s interstation running mode if the driver applies manual brakes.

By revealing “specifications or mode transitions that are insufficiently safe,” STPA prompts new software requirements, such as monitoring logic, alarms, or forced mode-switch rules. This goes beyond hardware failure probabilities to address fundamental design gaps in automation—an advantage over traditional reliability-focused methods.

4. Constraints on the interactions between different systems

When multiple controllers (e.g., the OCC, the driver, and the ATO) operate simultaneously, their conflicting commands or information can create hazards. Methods such as FMEA typically focus on hardware failures and may not adequately capture coordination failures across different systems, whereas STPA takes a holistic view of the control structure and clarifies which commands should take precedence at what time.

A prime example is RS-29.1, where the driver learns of an onboard emergency requiring a station stop but continues at high speed under ATO control. The recommended measure includes adding an “Emergency Station Stop Request” button in the cab that simultaneously alerts the OCC and locks out the ATO, ensuring a manual takeover. Similarly, RS-32.1 shows how a driver, having been verbally instructed to slow down, may see a new ATC speed limit and mistakenly drop the manual slowdown. The solution clarifies that a verbally-ordered slowdown remains valid unless explicitly canceled by the OCC, and suggests aligning any new ATC signals with the manual request.

By focusing on interactions among multiple controllers, STPA spots these “multi-system collisions” that common failure-based checks can miss.

5. Changing the type of feedback to more useful information

Traditional FMEA mostly checks whether sensors or communications fail, but STPA also asks if the information is interpreted and used correctly even when everything is working. Misinterpretation or neglect of valid data can lead to hazards under normal operation.

For instance, RS-22.1 addresses a platform door sensor that detects a passenger but is overlooked by staff when they cannot visually confirm it. The recommendation proposes requiring staff to clear the sensor alert before proceeding, ensuring that the warning is properly acknowledged. Likewise, RS-56.2.2 deals with a mismatch between ATC signals and the ATO, where ATC instructions are not recognized by the ATO, leading to potential overspeed. Proposed measures include continuously monitoring whether ATC data is received by the ATO, disabling the ATO if mismatched, and merging ATO/ATC information to check for contradictory speed profiles.

Thus, STPA not only addresses “What if a sensor fails?” but also “How is sensor data used, and can it be misunderstood or ignored?” Solutions such as forced acknowledgment buttons or real-time data consistency checks go beyond hardware fixes to ensure correct interpretation and utilization of normal sensor signals or feedback.

6. Modifying intended functions that may be unsafe when interacting with other systems

Sometimes the hazard comes from the design of a feature itself, even if hardware or software do not fail. In RS-4.3, the “remove all speed restrictions” command accidentally removes needed limits in some areas. STPA questions if this all-in-one command is risky by nature and suggests replacing it with an option to remove limits in parts or sections.

In standard reliability studies, a feature might be called safe as long as it doesn't break. By studying the control structure from the system-wide point of view, though, STPA finds that certain commands increase risk under normal use. Therefore, the best solution may be to redesign the command fully, not just add a guard against hardware failures.

7. Adding or removing functionality

In some cases, fixing hazards means not only adjusting existing functions but also creating entirely new ones. For example, RS-29.1 proposes an “Emergency Station Stop Request” button in the driver’s cab, which goes beyond a verbal instruction by also turning the ATO off. Likewise, RS-21.2 adds an “anti-drag detection” feature to apply an emergency brake if unusual force is detected at the doors after departure, covering cases where door sensors do not detect a thin object.

On the other hand, RS-4.3 shows how removing a risky “remove all” command or making it more limited can improve safety by preventing the accidental deletion of needed speed limits. These examples show how STPA prompts major redesigns or removal of certain functions, checking if each feature truly helps overall safety.

In summary, these findings show that many hazard scenarios are linked to normal system behavior rather than purely to hardware failures. By mapping out control structures, examining how people and machines interact, and studying software behaviors, STPA uncovers scenarios that traditional safety methods often miss. This approach emphasizes the need for design and procedural changes, not simply component-level fixes.

6.2 Technical and Academic Contributions, and Evaluation of STPA

This section discusses the broader technical and academic contributions from this study’s application of STPA.

1. Effectiveness of STPA in Early Conceptual Design

The STPA method proved effective at an early stage of conceptual design, when major decisions about system architecture and operations are made. By reviewing 20 control actions, we identified 59 Unsafe Control Actions (UCAs) and created related safety requirements. These results let us propose system-level design steps—like changing procedures, adding new software features, and improving user interfaces—long before the detailed design phase. For a large system like high-speed rail, the cost of changes goes up quickly in later stages. Thus, doing a complete safety review early can lower the risk and expense of redesigning or retrofitting later on.

2. Total-System Scope: Integrating Human Operation, Automation, and Physical Infrastructure

One key outcome of this study is merging multiple controllers into a single control structure, covering the train driver, platform attendant, Operation Control Center (OCC), Automatic Train Operation (ATO), and Automatic Train Control (ATC). In many railway projects, hazard analyses like FTA or FMEA are divided by procurement categories—for example, examining signaling gear or rolling stock separately. Yet high-speed rail systems rely on complex cooperation among people, equipment, and software in every phase. By using a whole-system perspective, this work found hazard scenarios that can happen during normal interactions, not just from isolated part failures. This combined approach also pointed out where better coordination, improved feedback loops, and clearer procedures could prevent problems.

To make the analysis easier to follow, a single high-level control structure showed the entire system, and separate control structures illustrated each operation phase (departure, running and stopping). This two-level setup gave an overall view of the system but also allowed for focused, phase-specific study of control actions.

3. Effectiveness of STPA in Identifying Non-Failure Scenarios

The analysis found many hazard scenarios that do not happen because of hardware problems or common failure modes. Instead, they come from leftover software states, weak feedback, confusing or conflicting orders, or miscommunications between automated functions and human operators—even though everything works “as specified.”

Traditional railway safety checks often focus on hardware dependability and known human-error patterns, overlooking bigger hazards caused by system-level interactions. STPA fills this gap by systematically checking how normal operation, when there are no outright failures, can still lead to accidents if control actions, feedback, or system interfaces are not well designed.

4. Technical Solutions Considering the Hierarchy of Controls

STPA’s broader view accepts that human errors will happen, and that system design can either reduce or increase these errors. Rather than just blaming “operator mistakes,” it looks at how unclear interfaces, missing or conflicting data, or mismatched procedures can steer people toward unsafe actions.

This analysis produced various design-centered solutions, going beyond typical fixes like redundancy or more operator training. For instance, new interface elements that require important confirmations, automatic safety features to override wrong assumptions, and organized communication methods for OCC, drivers, and platform attendants. By using the hierarchy of controls—first removing or replacing hazards, then using engineering controls before finally depending on people—STPA helps groups put robust technical fixes in place early in design.

7 Conclusions

This study applied STPA to the introduction of STO in the Tokaido Shinkansen as a model case. Its goal was to systematically identify new safety challenges in high-speed rail with STO and to propose design improvements. Traditional failure-based hazard analyses, such as FTA and FMEA, have been widely used in the railway industry to identify physical or functional failures of components. However, in large-scale rail systems that also involve human operators, there remain situations where system-level hazards can arise even when all components are functioning normally. In STO, complex interactions between human operators and both the existing ATC and the newly introduced ATO can give rise to potential risks that might be overlooked by traditional methods.

By applying STPA, several specific hazard scenarios were identified, especially for station departures and emergency responses during running. For instance, even if both train and platform systems are operating normally, a passenger could be left between the platform doors and the train. In addition, conflicts between verbal instructions and ATC signal could cause a delay in the driver's manual deceleration, allowing the train to enter the target section without reducing speed. These scenarios are not treated as failures of equipment or functions, so they are difficult to detect with traditional methods. In reality, they reflect hazardous interactions between fully operational components that may escalate into a serious problem. Moreover, if these scenarios are overlooked until later phases of system development or organizational coordination, they could lead to major redesign work or redefinition of operational rules at the final stage of implementation.

This study demonstrated the value of applying STPA to detect such risks in advance. STPA views the train control system and human operations as a single hierarchical control structure. It then examines under what conditions unsafe control actions might occur and how each element interacts including potential commands and feedback. In general, railways carry out procurement and design by subsystem, including rolling stock, signaling equipment, and infrastructure. Although such vertical segmentation can be efficient, it does not necessarily capture all interactions. Many of the hazard scenarios identified in this study involve the operation of multiple subsystems from a total-system viewpoint. There are few examples of safety analyses at the total system level of railways. In this context, demonstrating that STPA can be applied to both operations and infrastructure as a combined package, and can proceed from identifying realistic hazard scenarios to proposing design improvements, is highly

significant.

The design improvements derived from this study go beyond reinforcing existing operating manuals and training programs. They extend to more fundamental technical changes, such as adding new monitoring and detection functions for brake systems and passenger doors, modifying or expanding the interfaces for communication between train drivers and OCC, and strengthening the software logic that coordinates ATO and ATC. If STPA analysis is not performed, these types of design improvements might not be implemented at the conceptual design stage, potentially leading to higher redesign costs later. This underscores one of STPA's advantages: it allows safety analyses at the conceptual design level. This benefit is even more important for high-speed rail, where development costs are large, development periods are long, and the potential impact of any incidents during operation could be extremely severe.

These findings are broadly applicable to high-speed rail systems that plan to introduce automated operation. Although this study focused on the operating methods of the Tokaido Shinkansen, the core design principles are common to many other high-speed rail systems, even if their operational practices and infrastructure specifications differ. Therefore, the hazard scenarios and design improvements identified here could be applied to a wide range of high-speed rail operations. It is anticipated that the number of high-speed rail systems introducing GoA2 will continue to increase. However, existing standards for urban rail and failure-based design approaches alone may not be sufficient for dealing with the combined risks in high-speed, long-distance operations. Demonstrating the effectiveness of STPA in high-speed automated rail operations reinforces the importance of a comprehensive, system-theoretic approach during the introduction of new technologies. It is hoped that the outcomes of this study will contribute to the safety design and operational standards of a wide range of railway systems.

Appendix

Appendix A.1: Enlarged High-level Control Structure

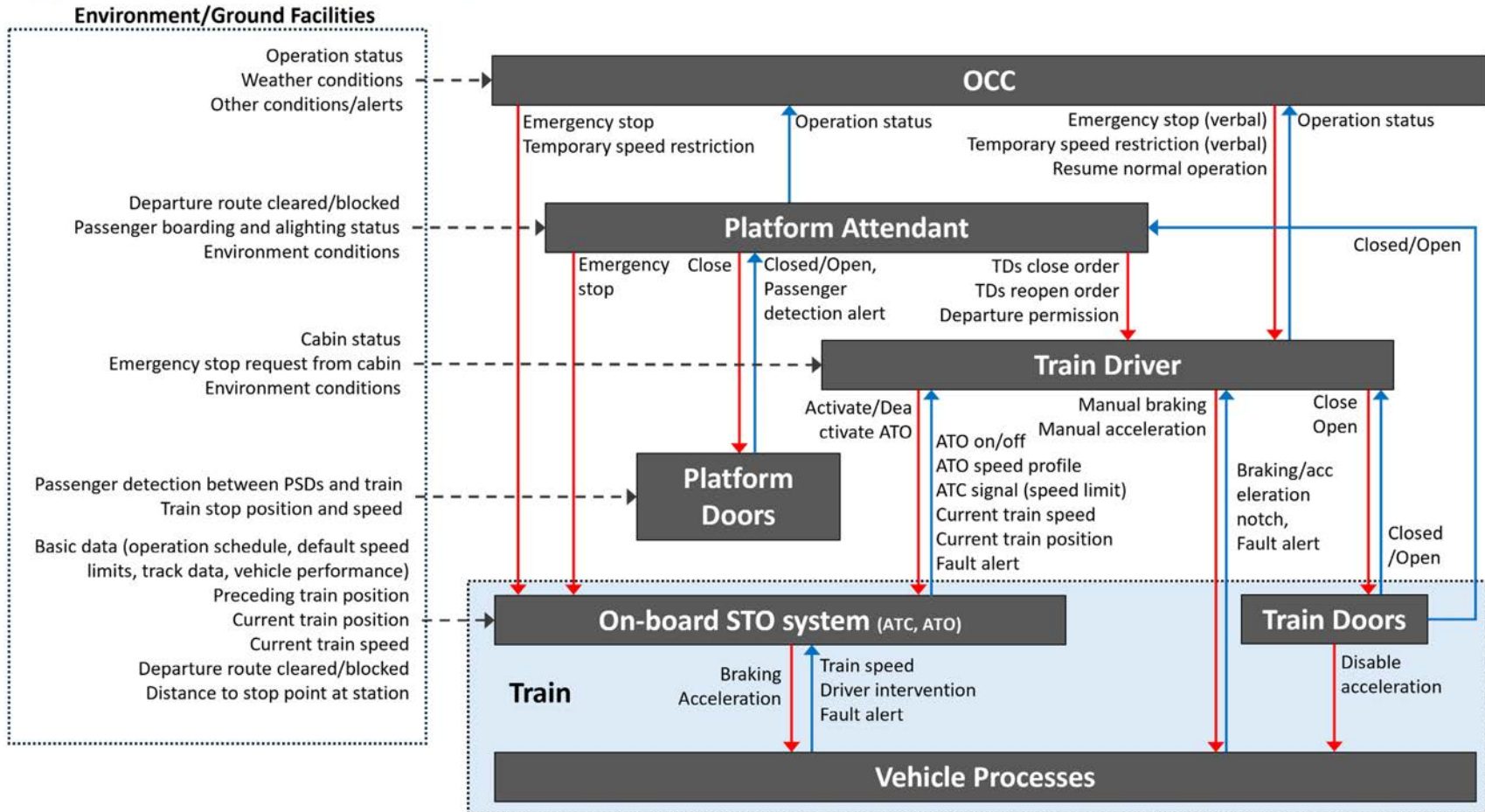


Figure 16: Enlarged High-level Control Structure

Appendix A.2: Enlarged Control Structure for Departure Phase

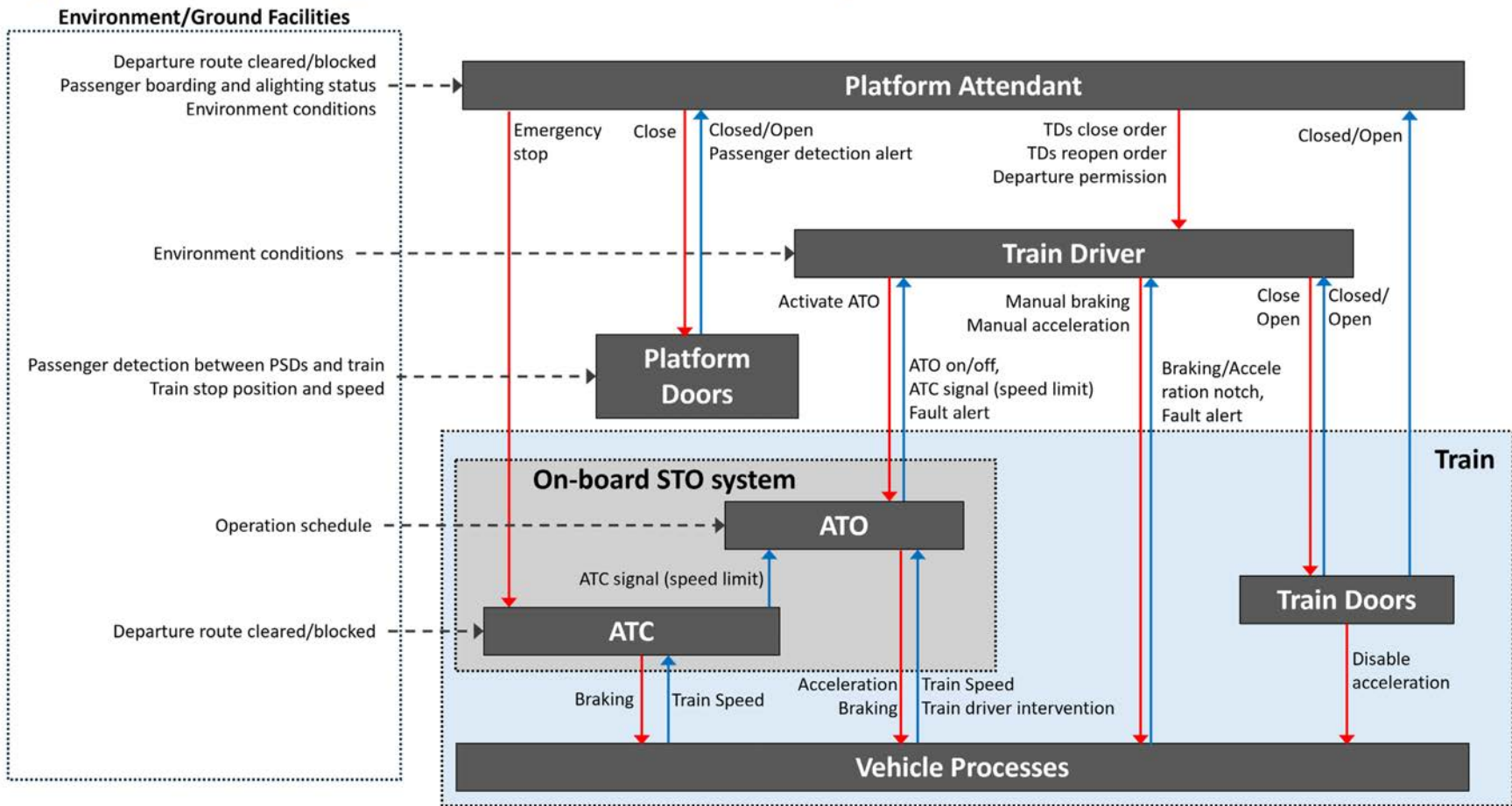


Figure 17: Enlarged Control Structure for Departure Phase

Appendix A.3: Enlarged Control Structure for Running and Stopping Phases

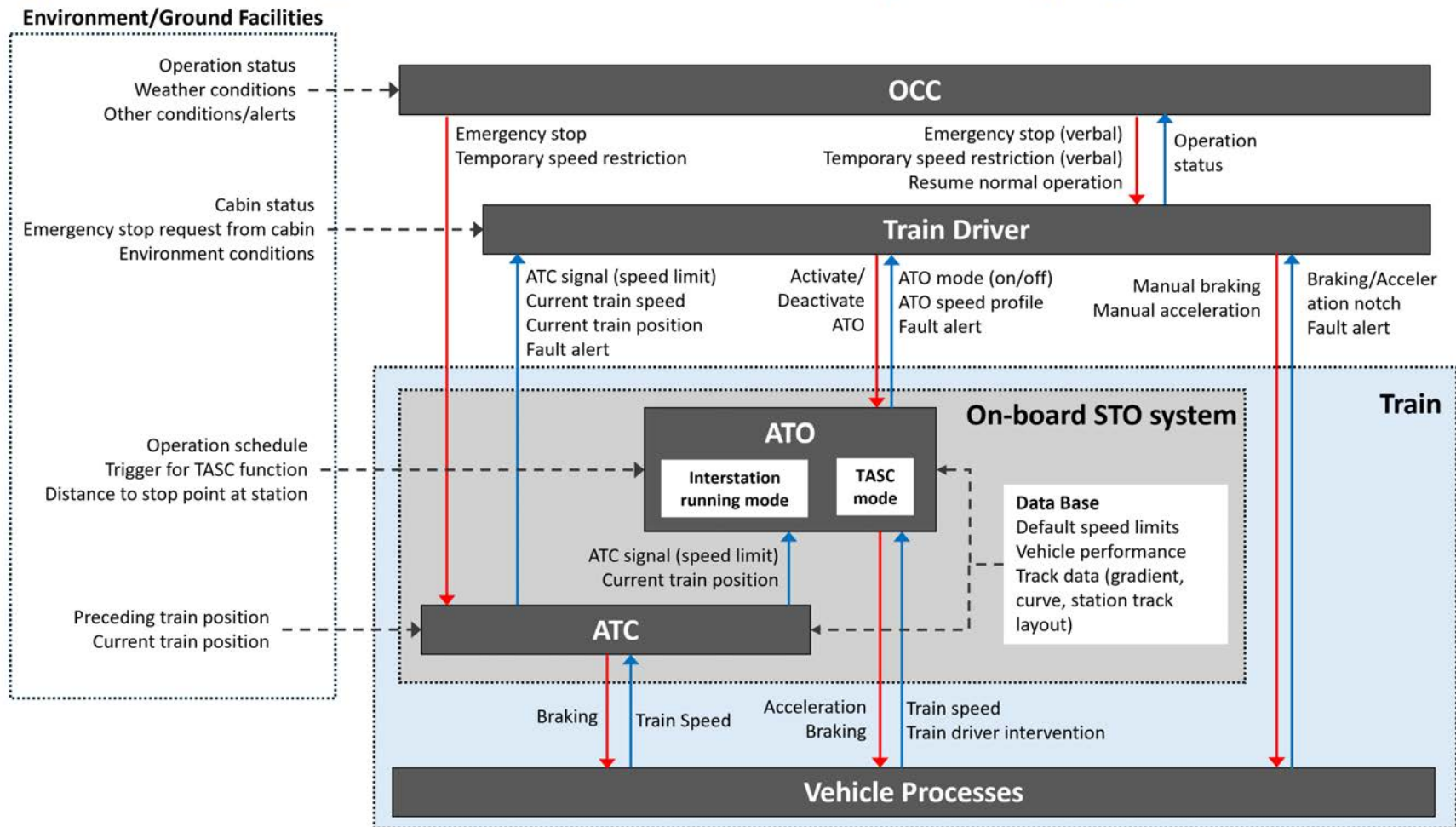


Figure 18: Enlarged Control Structure for Running and Stopping Phases

Appendix B: UCAs

Table 7: Identified UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Emergency stop (OCC)	UCA-1: OCC does not provide an emergency stop signal when a critical track hazard occurs. [H-1, H-2, H-6]		UCA-2: OCC provides an emergency stop signal too late after a critical track hazard occurs. [H-1, H-2, H-6]	
Temporary speed restriction	UCA-3: OCC does not provide a temporary speed restriction when a moderate track hazard occurs. [H-1, H-2]	UCA-4: OCC provides a temporary speed restriction at an excessive speed or for an incorrect section when a moderate track hazard occurs. [H-1, H-2]	UCA-5: OCC provides a temporary speed restriction too late after a moderate track hazard occurs. [H-1, H-2]	
Emergency stop (verbal)	UCA-6: OCC does not provide a verbal emergency stop order when a critical track hazard occurs without ATC stop signal. [H-1, H-2, H-6]		UCA-7: OCC provides a verbal emergency stop order too late after a critical track hazard occurs without ATC stop signal. [H-1, H-2, H-6]	

<p>Temporary speed restriction (verbal)</p>	<p>UCA-8: OCC does not provide a temporary speed restriction verbally when a moderate track hazard occurs without ATC slowdown signal. [H-1, H-2]</p>	<p>UCA-9: OCC provides a temporary speed restriction verbally at an excessive speed or for an incorrect section when a moderate track hazard occurs without ATC slowdown signal. [H-1, H-2]</p>	<p>UCA-10: OCC provides a temporary speed restriction verbally too late after a moderate track hazard occurs without ATC slowdown signal. [H-1, H-2]</p>	
<p>Resume normal operation</p>		<p>UCA-11: OCC provides an order to resume normal operation when a critical/moderate track hazard is not finished. [H-1, H-2, H-6]</p>		
<p>Emergency stop (Platform attendant)</p>	<p>UCA-12: Platform attendant does not provide an emergency stop signal when a passenger is positioned between the platform doors and the train after issuing departure permission. [H-4]</p>		<p>UCA-14: Platform attendant provides an emergency stop signal too late after a passenger is positioned between the platform doors and the train after issuing departure permission. [H-4]</p>	

	UCA-13: Platform attendant does not provide an emergency stop signal when train doors or platform doors are not fully closed after issuing departure permission. [H-3, H-4]		UCA-15: Platform attendant provides an emergency stop signal too late after train doors or platform doors are not fully closed after issuing departure permission. [H-3, H-4]	
Close platform doors		UCA-16: Platform attendant closes platform doors when passengers are still boarding or alighting. [H-4]		
Train doors close order		UCA-17: Platform attendant provides a train doors close order when passengers are still boarding or alighting. [H-3, H-4] UCA-18: Platform		

		attendant provides a train doors close order when train departure route is blocked. [H-1, H-2]		
Train doors reopen order	UCA-19: Platform attendant does not provide a train doors reopen order when a passenger is physically trapped in the train door. [H-3]		UCA-20: Platform attendant provides a train doors reopen order too late after a passenger is physically trapped in the train door. [H-3]	
Departure permission		UCA-21: Platform attendant provides departure permission when a passenger is physically trapped in the train door. [H-3] UCA-22: Platform attendant provides departure permission when		

		<p>a passenger is positioned between the platform doors and the train. [H-4]</p> <p>UCA-23: Platform attendant provides departure permission when train doors or platform doors are not fully closed. [H-3, H-4]</p>		
<p>Activate ATO</p>		<p>UCA-24: Train driver activates ATO when train doors or platform doors are not fully closed. [H-3, H-4]</p> <p>UCA-25: Train driver activates ATO when a passenger is positioned between the platform doors and the train. [H-4]</p>		

		<p>UCA-26: Train driver activates ATO when train departure route is blocked. [H-1, H-2]</p> <p>UCA-27: Train driver activates ATO when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2, H-6]</p> <p>UCA-28: Train driver activates ATO when ATO has a fault condition. [H-1, H-2]</p>		
Deactivate ATO	UCA-29: Train driver does not deactivate ATO when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2, H-6]		UCA-31: Train driver deactivates ATO too late after ATO has a fault condition. [H-1, H-2]	

	UCA-30: Train driver does not deactivate ATO when ATO has a fault condition. [H-1, H-2]			
Manual brake	<p>UCA-32: Train driver does not apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]</p> <p>UCA-33: Train driver does not apply manual brakes when the train has a critical fault condition. [H-1, H-2, H-5]</p> <p>UCA-34: Train driver does not apply manual brakes when ATO braking force is insufficient to stop inside the allowable</p>	UCA-36: Train driver applies insufficient manual brakes when the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]	<p>UCA-37: Train driver applies manual brakes too late after the train does not automatically brake for a critical/moderate track hazard. [H-1, H-2]</p> <p>UCA-38: Train driver applies manual brakes too late after the train has a critical fault condition. [H-1, H-2, H-5]</p> <p>UCA-39: Train driver applies manual brakes too late after ATO braking is released (TBD seconds after ATO has</p>	<p>UCA-40: Train driver stops applying manual brakes too soon before the train comes to a complete stop when the train does not automatically brake for a critical track hazard. [H-1, H-2]</p> <p>UCA-41: Train driver stops applying manual brakes too soon before reducing speed to the target speed limit when the train does not automatically brake for a moderate track</p>

	<p>tolerance range of the designated stop position. [H-5]</p> <p>UCA-35: Train driver does not apply manual brakes when the train is stopped at station. [H-4]</p>		<p>completely stopped the train). [H-5]</p>	<p>hazard. [H-1, H-2]</p>
Manual acceleration		<p>UCA-42: Train driver applies manual acceleration when the train speed exceeds the speed limit. [H-1, H-2]</p>	<p>UCA-43: Train driver applies manual acceleration too early before a critical/moderate track hazard is finished. [H-1, H-2]</p>	
Close train doors		<p>UCA-44: Train driver closes train doors when passengers are still boarding or alighting. [H-3, H-4]</p>		

Open train doors	UCA-45: Train driver does not open train doors when a passenger is physically trapped in the train door. [H-3]	UCA-46: Train driver opens train doors at station when brakes are not applied. [H-4]		
Braking (ATC)	UCA-47: ATC does not apply brakes when a critical/moderate track hazard occurs. [H-1, H-2, H-6] UCA-48: ATC does not apply brakes when the train speed exceeds the speed limit. [H-1, H-2, H-3, H-4, H-5]	UCA-49: ATC applies insufficient brakes when a critical/moderate track hazard occurs. [H-1, H-2, H-6]	UCA-50: ATC applies brakes too late after a critical/moderate track hazard occurs. [H-1, H-2, H-6] UCA-51: ATC applies brakes too late after the train speed exceeds the speed limit. [H-1, H-2, H-3, H-4, H-5]	
Braking (ATO)	UCA-52: ATO does not apply brakes when the train approaches the designated stop position at the station. [H-5]	UCA-53: ATO applies insufficient brakes when the train approaches the designated stop position at the station. [H-5]	UCA-54: ATO applies brakes too late after the train exceeds the minimum braking distance to the designated stop position at the station. [H-5]	UCA-55: ATO stops applying brakes too soon before the train comes to a complete stop at the station. [H-5]
Acceleration		UCA-56: ATO applies acceleration when		

		<p>the train speed exceeds the speed limit. [H-1, H-2]</p> <p>UCA-57: ATO applies acceleration when the train driver applies manual brakes. [H-1, H-2, H-3, H-4, H-6]</p> <p>UCA-58: ATO applies acceleration when train doors or platform doors are not fully closed. [H-3, H-4]</p>		
Disable acceleration	UCA-59: Train doors do not disable acceleration of vehicle when they are not fully closed. [H-3]			

Appendix C: Safety Requirements

Table 8: Identified safety requirements

Safety Requirements
R-1: OCC must provide an emergency stop signal when a critical track hazard occurs. [UCA-1]
R-2: OCC must provide an emergency stop signal within TBD seconds after a critical track hazard occurs. [UCA-2]
R-3: OCC must provide a temporary speed restriction when a moderate track hazard occurs. [UCA-3]
R-4: OCC must provide a temporary speed restriction at a speed not more than the target speed limit and for a correct section when a moderate track hazard occurs. [UCA-4]
R-5: OCC must provide a temporary speed restriction within TBD seconds after a moderate track hazard occurs. [UCA-5]
R-6: OCC must provide a verbal emergency stop order when a critical track hazard occurs without ATC stop signal. [UCA-6]
R-7: OCC must provide a verbal emergency stop order within TBD seconds after a critical track hazard occurs without ATC stop signal. [UCA-7]
R-8: OCC must provide a temporary speed restriction verbally when a moderate track hazard occurs without ATC slowdown signal. [UCA-8]
R-9: OCC must provide a temporary speed restriction verbally at a speed not more than the target speed limit and for a correct section when a moderate track hazard occurs without ATC slowdown signal. [UCA-9]
R-10: OCC must provide a temporary speed restriction verbally within TBD seconds after a moderate hazard occurs without ATC slowdown signal. [UCA-10]
R-11: OCC must not provide an order to resume normal operation when a critical/moderate track hazard is not finished. [UCA-11]
R-12: Platform attendant must provide an emergency stop signal when a passenger is positioned between the platform doors and the train after issuing departure permission. [UCA-12]
R-13: Platform attendant must provide an emergency stop signal when train doors or platform doors are not fully closed after issuing departure permission. [UCA-13]
R-14: Platform attendant must provide an emergency stop signal within TBD seconds after a passenger is positioned between the platform doors and the train after issuing

departure permission. [UCA-14]
R-15: Platform attendant must provide an emergency stop signal within TBD seconds after train doors or platform doors are not fully closed after issuing departure permission. [UCA-15]
R-16: Platform attendant must not close platform doors when passengers are still boarding or alighting. [UCA-16]
R-17: Platform attendant must not provide a train doors close order when passengers are still boarding or alighting. [UCA-17]
R-18: Platform attendant must not provide a train doors close order when train departure route is blocked. [UCA-18]
R-19: Platform attendant must provide a train doors reopen order when a passenger is physically trapped in the train door. [UCA-19]
R-20: Platform attendant must provide a train doors reopen order within TBD seconds after a passenger is physically trapped in the train door. [UCA-20]
R-21: Platform attendant must not provide departure permission when a passenger is physically trapped in the train door. [UCA-21]
R-22: Platform attendant must not provide departure permission when a passenger is positioned between the platform doors and the train. [UCA-22]
R-23: Platform attendant must not provide departure permission when train doors or platform doors are not fully closed. [UCA-23]
R-24: Train driver must not activate ATO when train doors or platform doors are not fully closed. [UCA-24]
R-25: Train driver must not activate ATO when a passenger is positioned between the platform doors and the train. [UCA-25]
R-26: Train driver must not activate ATO when train departure route is blocked. [UCA-26]
R-27: Train driver must not activate ATO when the train does not automatically brake for a critical/moderate track hazard. [UCA-27]
R-28: Train driver must not activate ATO when ATO has a fault condition. [UCA-28]
R-29: Train driver must deactivate ATO when the train does not automatically brake for a critical/moderate track hazard. [UCA-29]
R-30: Train driver must deactivate ATO when ATO has a fault condition. [UCA-30]
R-31: Train driver must deactivate ATO within TBD seconds after ATO has a fault

condition. [UCA-31]
R-32: Train driver must apply manual brakes when the train does not automatically brake for a critical/moderate track hazard. [UCA-32]
R-33: Train driver must apply manual brakes when the train has a critical fault condition. [UCA-33]
R-34: Train driver must apply manual brakes when ATO braking force is insufficient to stop inside the allowable tolerance range of the designated stop position. [UCA-34]
R-35: Train driver must apply manual brakes when the train is stopped at station. [UCA-35]
R-36: Train driver must not apply manual brakes that is insufficient to reduce speed to the target speed limit (or to stop) by the start point of the track hazard when the train does not automatically brake for a critical/moderate track hazard. [UCA-36]
R-37: Train driver must apply manual brakes within TBD seconds after the train does not automatically brake for a critical/moderate track hazard. [UCA-37]
R-38: Train driver must apply manual brakes within TBD seconds after the train has a critical fault condition. [UCA-38]
R-39: Train driver must apply manual brakes within TBD seconds after ATO has completely stopped the train. [UCA-39]
R-40: Train driver must not stop applying manual brakes before the train comes to a complete stop when the train does not automatically brake for a critical track hazard. [UCA-40]
R-41: Train driver must not stop applying manual brakes before reducing speed to the target speed limit when the train does not automatically brake for a moderate track hazard. [UCA-41]
R-42: Train driver must not apply manual acceleration that is excessive to exceed speed limits. [UCA-42]
R-43: Train driver must not apply manual acceleration before a critical/moderate track hazard is finished. [UCA-43]
R-44: Train driver must not close train doors when passengers are still boarding or alighting. [UCA-44]
R-45: Train driver must open train doors when a passenger is physically trapped in the train door. [UCA-45]
R-46: Train driver must not open train doors at station when brakes are not applied. [UCA-46]

R-47: ATC must apply brakes when a critical/moderate track hazard occurs. [UCA-47]
R-48: ATC must apply brakes when the train speed exceeds the speed limit. [UCA-48]
R-49: ATC must not apply brakes that is insufficient to reduce speed to the target speed limit (or to stop) by the start point of the hazard when a critical/moderate track hazard occurs. [UCA-49]
R-50: ATC must apply brakes within TBD seconds after a critical/moderate track hazard occurs. [UCA-50]
R-51: ATC must apply brakes within TBD seconds after the train speed exceeds the speed limit. [UCA-51]
R-52: ATO must apply brakes when the train approaches the designated stop position at the station. [UCA-52]
R-53: ATO must not apply brakes that are insufficient to stop inside the allowable tolerance range of the designated stop position when the train approaches the designated stop position at the station. [UCA-53]
R-54: ATO must apply brakes within TBD seconds after the train exceeds the minimum braking distance to the designated stop position at the station. [UCA-54]
R-55: ATO must not stop applying brakes before the train comes to a complete stop. [UCA-55]
R-56: ATO must not apply acceleration when the train speed exceeds the speed limit. [UCA-56]
R-57: ATO must not apply acceleration when the train driver applies manual brakes. [UCA-57]
R-58: ATO must not apply acceleration when train doors or platform doors are not fully closed. [UCA-58]
R-59: Train doors must disable acceleration of vehicle when they are not fully closed. [UCA-59]

References

- [1] Central Japan Railway Company, “最新の技術を活用した経営体力の再強化～より安全で、より便利で、より快適な鉄道を目指して～,” 2022. [Online]. Available: https://jr-central.co.jp/news/release/_pdf/000042355.pdf
- [2] International Electrotechnical Commission, “IEC 62290-1: Railway applications -Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts,” 2014.
- [3] East Japan Railway Company, “JR East’s plans for driverless Shinkansen operation,” 2024, [Online]. Available: <https://www.jreast.co.jp/e/press/2024/pdf/20240910.pdf>
- [4] “JR Central targeting Tokaido Shinkansen ATO from 2028,” Railway Gazette International. [Online]. Available: <https://www.railwaygazette.com/jr-central-targeting-tokaido-shinkansen-ato-from-2028/63929.article>
- [5] “FEATURE: Japan’s shinkansen bullet trains gearing up for automatic driving,” KYODO NEWS. [Online]. Available: <https://english.kyodonews.net/news/2023/07/9af73a9ef286-feature-japans-shinkansen-bullet-trains-gearing-up-for-automatic-driving.html>
- [6] M. H. Wong, “Driverless bullet train speeds across China,” CNN. Accessed: Feb. 19, 2025. [Online]. Available: <https://www.cnn.com/travel/article/driverless-bullet-train-china/index.html>
- [7] “SNCF to run high speed driverless trains by 2023,” Railway PRO. Accessed: Apr. 24, 2025. [Online]. Available: <https://www.railwaypro.com/wp/sncf-to-run-high-speed-driverless-trains-by-2023/>
- [8] International Electrotechnical Commission, “IEC 62267: Railway applications - Automated urban guided transport (AUGT) - Safety requirements.” 2009.
- [9] International Electrotechnical Commission, “IEC 62278: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS).” 2002.
- [10] C. S. Wasson, *System Engineering Analysis, Design, and Development: Concepts, Principles, and Practices*, 2nd Edition. Wiley, 2015.
- [11] L. Sun, Y.-F. Li, and E. Zio, “Comparison of the HAZOP, FMEA, FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems,” *ASCE-ASME J Risk Uncert Engrg Sys Part B Mech Engrg*, vol. 8, no. 031104, Oct. 2021, doi: 10.1115/1.4051940.

- [12] N. Leveson and J. Thomas, “STPA Handbook,” 2018. [Online]. Available: <https://psas.scripts.mit.edu/home/books-and-handbooks/>
- [13] Central Japan Railway Company, “Integrated Report 2024,” 2024. [Online]. Available: <https://global.jr-central.co.jp/en/company/ir/annualreport/>
- [14] Central Japan Railway Company, “東海道新幹線の自動運転システムに関する技術開発.” Accessed: Feb. 18, 2025. [Online]. Available: https://company.jr-central.co.jp/company/technology/_pdf/report_02.pdf
- [15] “新幹線の自動運転、JR 東海は「とてつもない精度」をどう実現したのか?,” DIAMOND online. Accessed: Feb. 20, 2025. [Online]. Available: <https://diamond.jp/articles/-/323227>
- [16] “Two dead after suicide on Japanese bullet train: reports,” *ABC News*, Jun. 30, 2015. [Online]. Available: <https://www.abc.net.au/news/2015-06-30/japan-bullet-train-two-in-cardiac-arrest-after-smoke-reports/6584064>
- [17] “Knife rampage aboard Japanese bullet train kills 1, injures 2,” KYODO NEWS. [Online]. Available: <https://english.kyodonews.net/news/2018/06/b41b93ab2b66-several-injured-on-shinkansen-bullet-train-man-detained.html>
- [18] “JAPAN REPORTS 1ST FATALITY FROM BULLET TRAIN ACCIDENT,” Orlando Sentinel. Accessed: Apr. 26, 2025. [Online]. Available: <https://www.orlandosentinel.com/1995/12/29/japan-reports-1st-fatality-from-bullet-train-accident/>
- [19] J. Thomas, “Developing STPA Scenarios,” presented at the MIT STAMP workshop, 2024. [Online]. Available: <https://psas.scripts.mit.edu/home/wp-content/uploads/2024/STPA-Scenarios-New-Approach.pdf>