Systems Theoretic Process Analysis Applied to the Superconductive Maglev System

By

Hirotaka Yokoyama

Bachelor of Engineering in Applied Science, Osaka University, 2014
Master of Engineering in Applied Physics, Osaka University, 2016

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 2026

© 2026 Hirotaka Yokoyama. 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: Hirotaka Yokoyama
System Design and Management Program
May 8, 2026

Certified by: John P. Thomas
ESL Co-Director, Department of Aeronautics and Astronautics
Thesis Supervisor

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

Systems Theoretic Process Analysis Applied to the Superconductive Maglev System

by

Hirotaka Yokoyama

Submitted to the System Design and Management Program on May 8, 2026
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT

ABSTRACT

This study evaluates the safety of highly automated railway systems by applying Systems Theoretic Process Analysis (STPA) to the SC Maglev system, a next-generation ultra-high-speed railway system. Unlike conventional railways, SC Maglev trains operate without a driver on board, relying instead on remote control from the ground and advanced automated driving. In such software-intensive, complex systems, even if individual components do not fail, inappropriate interactions between components or design flaws can potentially cause serious hazards.

In this study, we focused on the safety role of a conductor, which remains a subject of ongoing debate. We defined two control structures—the "without conductor" model, in which the conductor does not participate in operational control, and the "with conductor" model, in which the conductor performs manual intervention in emergencies—and conducted a comparative analysis using STPA. The analysis demonstrated the effectiveness of STPA in comprehensively identifying hazard scenarios arising from design flaws and human-system interactions. While introducing the conductor into the system improves redundancy, it also induces new risks attributable to human factors, such as the distribution of responsibility between the conductor and control room operator, and inappropriate assumptions arising from information asymmetry within the isolated environment of the train cabin during high-speed operation. This suggests that simply adding personnel does not necessarily lead directly to improved system safety, highlighting the need to evaluate redundancy and safety distinctly in highly automated systems.

Finally, based on the analysis findings, we presented multi-layered safety design recommendations. The results of this study not only support decision-making during the conceptual design phase of the SC Maglev but also provide important insights for the safety design of all transportation systems as automation progresses in the future.

Thesis Supervisor: John P. Thomas

Title: ESL Co-Director, Department of Aeronautics and Astronautics

DISCLAIMER

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

ACKNOWLEDGMENTS

I want to express my deepest gratitude to all those who provided me with tremendous support in the preparation of this thesis.

First and foremost, I would like to express my heartfelt gratitude to my advisor, Dr. John P. Thomas. Throughout the thesis project, he consistently provided invaluable guidance and warm support. Our repeated discussions, which went beyond the STPA analysis framework to address the fundamental question of "what is the essence of safety in modern advanced systems," have provided me with insights that will be crucial to my future career.

I would also like to express my deep gratitude to my colleagues in the System Design and Management program. Their diverse backgrounds, admirable character, intellectually rich insights, and dedicated teamwork provided immeasurable inspiration and enriched my life.

I also extend my sincere thanks to Central Japan Railway Company for providing me with this study abroad opportunity and for their strong support in every aspect.

Finally, I would like to express my heartfelt gratitude to my family, who have shared both the joys and hardships with me in this new land, the United States. I extend my deepest gratitude—which words cannot fully express—to my wife, who has always stood by my side and supported me.

Table of Contents

Table of Figures *10*

Table of Tables *11*

Chapter 1: Introduction *13*

1.1 Research Background **13**

1.2 Research Objective **14**

1.3 Thesis Structure **15**

Chapter 2: Literature Review *16*

2.1 Accident Model **16**

2.1.1 Domino Accident Model 16

2.1.2 Swiss Cheese Model 17

2.1.3 System-Theoretical Accident Model and Processes 18

2.2 Traditional Accident and Hazard Analysis Methods **19**

2.2.1 FMEA 19

2.2.2 FTA 20

2.3 STPA overview **21**

2.3.1 Define the Purpose of the Analysis 22

2.3.2 Model the Control Structure 23

2.3.3 Identify Unsafe Control Actions 23

2.3.4 Identify Loss Scenarios 24

2.4 Prior Research Regarding the Hazard Analysis for Autonomous Transportation Using STPA **25**

2.4.1 Automobile 25

2.4.2 Airplane 25

2.4.3 Vessel 26

2.4.4 Railway 26

Chapter 3: System Description 27

3.1 SC Maglev System Technology 27

3.1.1 Fundamental Technology for the SC Maglev System 27

3.1.2 Propulsion Principle 28

3.1.3 Levitation Principle 29

3.1.4 Guidance Principle 30

3.1.5 Running Control 30

3.1.6 Safety Control 31

3.1.7 Emergency Brake System 31

3.1.8 Onboard Equipment Control 32

3.2 Development History and Safety Analysis in the SC Maglev System 32

3.2.1 Development History 32

3.2.2 Systematic Approach to Ensuring Safety and Reliability 33

3.2.3 Track Record in Hazard Analysis 33

3.2.4 Limitations and Challenges of Hazard Analysis 34

Chapter 4: Hazard Analysis of the SC Maglev System 35

4.1 Application of STPA to the "Without Conductor" Model 35

4.1.1 Define the Purpose of the Analysis 35

4.1.2 Model the Control Structure 37

4.1.3 Identify Unsafe Control Actions 44

4.1.4 Identify Loss Scenarios 49

4.2 Application of STPA to "With Conductor" Model 62

4.2.1 Define the Purpose of the Analysis 62

4.2.2 Model the Control Structure 63

4.2.3 Identify Unsafe Control Actions 69

4.2.4 Identify Loss Scenarios 72

Chapter 5: Discussion 78

5.1 The Change in the Responsibilities of Each Controller 78

5.2 Changes in the Number of Identified UCAs by Controller and Extract "Model-Specific UCAs." 81

5.3 Why the Model-Specific UCAs Occur in the Specific Model 88

5.3.1 Limitations of Remote Control in the "Without Conductor" Model 88

5.3.2 Side Effects of Redundancy and Risks of Isolation in the "With Conductor" Model 89

5.4 Characteristics and Challenges of Each Model 91

5.4.1 Without Conductor Model 91

5.4.2 With Conductor Model 92

5.5 Prioritization of Recommendations 94

5.5.1 Overview of MIL-STD-882E 94

5.5.2 Prioritization of Recommendations for the "Without Conductor" Model 95

5.5.3 Prioritization of Recommendations for the "With Conductor" Model 98

Chapter 6: Conclusion 101

6.1 Key Findings 101

6.2 Future Work 102

Appendices 103

Appendix A.1: Enlarged Control Structure for the "Without Conductor" Model 103

Appendix A.2: All UCAs Identified in the "Without Conductor" Model 104

Appendix A.3: All Safety Constraints for the "Without Conductor" Model 115

Appendix B.1: Enlarged Control Structure for the "With Conductor" Model 125

Appendix B.2: All UCAs Identified in the "With Conductor" Model 126

Appendix B.3: All Safety Constraints for the "With Conductor" Model 137

References 150

Table of Figures

Figure 1. Domino Accident Model [7] 17

Figure 2. Swiss Cheese Model [10] 17

Figure 3. Hierarchical Safety Control Structure [6] 19

Figure 4. Typical Fault Tree [13] 21

Figure 5. Overview of the Basic STPA Method [14] 22

Figure 6. Generic Hierarchical Control Structure [14] 23

Figure 7. Generation Mechanism of UCA: (1) Unsafe Controller Behavior and (2) Inadequate Feedback and Other Inputs [14] 24

Figure 8. Generation Mechanism of UCA: (3) Control Path and (4) the Controlled Process Itself [14] 25

Figure 9. Appearance of the SC Maglev System [19] 28

Figure 10. Comparison between Conventional Motor and Linear Motor [5] 28

Figure 11. Propulsion Principle [5] 29

Figure 12. Levitation Principle [5] 30

Figure 13. Guidance Principle [5] 30

Figure 14. Control Structure for the “Without Conductor” Model 37

Figure 15. Control Structure for the “With Conductor” Model 63

Figure 16. Enlarged Control Structure for the “Without Conductor” Model 103

Figure 17. Enlarged Control Structure for the “With Conductor” Model 125

Table of Tables

Table 1. Each Controller's Responsibilities, Control Action, Process Model, and Feedback/Other Input (the "Without Conductor" Model) 38

Table 2. Meanings and Contexts of Technical Terms 41

Table 3. UCA Templates 44

Table 4. Samples of the Identified UCAs in the "Without Conductor" Model..... 45

Table 5. Safety Constraint Template 48

Table 6. Samples of the Safety Constraints for the "Without Conductor" Model 49

Table 7. High-Level Scenario Archetype Table 50

Table 8. Each Controller's Responsibilities, Control Action, Process Model, and Feedback/Other Input (the "With Conductor" Model) 64

Table 9. Samples of the Identified UCAs in the "With Conductor" Model **Error! Bookmark not defined.**

Table 10. Samples of the Safety Constraints for the "Without Conductor" Model 72

Table 11. Comparison of Controller Responsibilities in Both Models: Responsibilities in red indicate those fully transferred to the conductor, while those in blue indicate responsibilities shared with the conductor. 79

Table 12. Number of each component UCA identified for each model. The numbers in parentheses indicate the number of UCAs common to both models. 81

Table 13. A list classifying UCAs not shared by both models as either "Transferred UCA" or "Model-Specific UCA"..... 83

Table 14. Model-Specific UCAs for each model and the Main Causal Factor..... 89

Table 15. Advantages and challenges of the "without conductor" model 92

Table 16. Advantages and challenges of the "with conductor" model 93

Table 17. Classifications of the recommendations for the "Without Conductor" Model according to the "Order of Precedence." 95

Table 18. Classifications of the recommendations for the "With Conductor" Model according to the "Order of Precedence." 98

Table 19. All UCAs Identified in the “Without Conductor” Model 104

Table 20. All Safety Constraints for the “Without Conductor” Model 115

Table 21. All UCAs Identified in the “With Conductor” Model..... 126

Table 22. All Safety Constraints for the “With Conductor” Model 137

Chapter 1: Introduction

1.1 Research Background

The Tokaido Shinkansen is a core piece of infrastructure that has supported Japan's economic development, serving as a transportation system connecting Tokyo, Nagoya, and Osaka—Japan's three major cities. The safety of the Tokaido Shinkansen is highly regarded worldwide; even after more than 60 years of operation, there have been no casualties from train operations [1]. Furthermore, its capacity to transport an average of 460,000 passengers per day and its ultra-high-density operation, with trains running at intervals as short as three minutes, far surpass those of other modes of transportation, such as airplanes and buses [1]. It meets diverse needs, from business to leisure travel, while providing the convenience of being available whenever needed. Moreover, while achieving safety and mass transportation, the average delay per train is only 1.4 minutes, making it an exceptionally excellent transportation system with high punctuality [2]. Naturally, these outstanding characteristics are supported by hardware, such as rolling stock and along-line facilities, and by software, such as operations management systems and signaling systems, and, crucially, by the dedicated employees who carry out the mission of supporting Japan's vital transportation arteries.

Demand for the Tokaido Shinkansen temporarily slumped significantly due to COVID-19 disruptions. However, with the recovery of the Japanese economy and the increase in inbound travelers, demand has now surpassed pre-pandemic levels and continues to grow [3]. Meanwhile, the transport capacity of the Tokaido Shinkansen has already reached its limit, making it extremely difficult to accommodate further demand by simply increasing train frequency. Furthermore, as more than 60 years have passed since its inception and the facilities have aged, large-scale repairs to the track infrastructure are now required. Additionally, the areas along the Tokaido Shinkansen route, such as Aichi and Shizuoka Prefectures, are expected to suffer extensive damage from the anticipated Nankai Trough earthquake, predicted to occur within the next 30 years [4]. The Tokaido Shinkansen is also highly likely to suffer prolonged operational shutdowns due to the collapse of ground facilities. A prolonged suspension of the Tokaido Shinkansen, Japan's vital artery, would completely halt the movement and exchange of people between Japan's three major metropolitan areas, causing significant economic stagnation.

To address these challenges, construction is currently underway on the Chuo Shinkansen (SC Maglev), a bypass transportation system for the Tokaido Shinkansen. The SC Maglev represents an entirely new high-speed rail system, fundamentally different from the conventional high-speed rail systems used by the Tokaido Shinkansen and other high-speed railways. First, while conventional high-speed rail systems use electricity and run on tracks, the SC Maglev uses magnetic levitation as its power source and levitates along a guideway. The SC Maglev's maximum speed is 311 miles per hour, far exceeding the 177 miles per hour of the Tokaido Shinkansen and

many other high-speed rail systems, making it the world's fastest ground transportation system [5]. The second major difference is that while conventional high-speed rail systems require a driver to control the train, the SC Maglev operates without a driver on board. Instead, each train is remotely controlled from the ground by the operation management system and ground-based operators. The operations management system automates routine train control, with operators only manually intervening via remote control during emergencies requiring human input.

The safety of the SC Maglev is guided by a safety design philosophy inherited from the Tokaido Shinkansen, cultivated over many years. However, due to its entirely different propulsion and control systems, a new hazard analysis for the SC Maglev is required. In this new high-speed rail system, automated systems must collaborate with operators and conductors to ensure safety. Yet the higher the level of automation, the more challenging the coordination between systems and humans becomes. The complex interactions between automated systems, humans, and physical facilities at stations and along the line could give rise to unexpected hazards not seen in conventional high-speed rail systems. Therefore, it is crucial to identify hazards throughout the entire system and implement preventive measures early in system design and development. Furthermore, since the SC Maglev system operates without a driver, the conductor is solely responsible for on-site responses to emergencies occurring inside the train or along the line during both train operation and station stops. Therefore, redefining the conductor's safety role within a highly automated system is essential, and discussions continue regarding what responsibilities conductors should assume during emergencies.

Systems Theoretic Process Analysis (STPA) is a new hazard analysis method that differs from conventional hazard analysis methods focused on physical failures of individual system components [6]. STPA enables the identification not only of hazards caused by physical failures of individual components, but also of hazards arising from interactions and communication mismatches between components or within the entire system—hazards that conventional analysis methods could not identify. Furthermore, in today's software-intensive systems, hazards often arise not from hardware failures but from software design flaws, deficiencies in human-software interactions, or interactions between software components. STPA is an excellent analysis method for identifying these hazards and proposing countermeasures, and its application is expanding across various fields.

1.2 Research Objective

This study uses STPA to analyze the safety of the SC Maglev, comprehensively identify potential safety issues that could lead to hazards, and propose recommended design measures to address them. Specifically, to analyze the role of the conductor during emergencies—a topic still under ongoing discussion—two control structure models are defined: a “without conductor” model where the conductor does not manually control the train even in emergencies, relying instead on

remote control by operators or train operation management systems; and a “with conductor” model where the conductor performs manual train control during emergencies.

This study applies STPA to each model to identify hazardous scenarios arising from interactions between operators, conductors, and train operation management systems. It particularly focuses on complex interactions between human operations and systems, or between humans themselves. By comparing the hazardous scenarios and analysis results identified for each system, the advantages and challenges in both models are clarified. Furthermore, by deriving design recommendations for the conceptual design phase of the integrated system, we mitigate potential risks in the SC Maglev system and enhance its safety.

The second objective is to demonstrate the effectiveness of STPA by identifying system-level hazards that conventional hazard analysis methods, such as FMEA and FTA, cannot detect. Conventional railway hazard analyses focus on identifying hazards caused by failures of individual hardware components—such as signals, tracks, and rolling stock—and on implementing countermeasures, such as redundancy and fail-safe mechanisms. However, the SC Maglev differs from conventional systems: it is highly automated, driven by software, yet it also involves human operation, making it complex. Consequently, even in non-failure scenarios in which all components operate as specified, the likelihood of hazards at the system level increases significantly. This research demonstrates that STPA is effective at comprehensively identifying non-failure hazardous scenarios within components and at the system level that conventional hazard analysis methods might overlook.

1.3 Thesis Structure

Chapter 1 introduces the background and objectives of this study. Chapter 2 presents representative accident models and hazard analysis methods, including an overview of STPA, and introduces recent cases of automated systems in transportation infrastructure. Chapter 3 outlines the SC Maglev system, detailing its operating principles and remote-control mechanisms—key aspects that differ significantly from those of conventional high-speed rail systems. Chapter 4 presents the analysis results from applying STPA to the SC Maglev system, including the derivation of losses and hazards, safety constraints, control structures, unsafe control actions, scenarios leading to hazards, and recommendations. The STPA safety analysis is applied to two control structure models: the “without conductor” and “with conductor” models. First, the STPA analysis for the “without conductor” model is performed. Next, the STPA analysis for the “with conductor” model is conducted, focusing specifically on components affected by the conductor's manual control interventions to avoid duplicating the analysis of the “without conductor” model. Chapter 5 evaluates the STPA analysis results for both models and examines how the conductor affects the SC Maglev system's safety. Chapter 6 presents the conclusions, summarizing the key insights gained from this research.

Chapter 2: Literature Review

This chapter provides an overview of accident models and the methods for accident and hazard analysis developed to maintain the safety of increasingly complex modern systems. An accident model is a formalized framework that describes the processes through which hazards and accidents occur. The hazard analysis methods, based on these accident models, are designed to qualitatively or quantitatively analyze the causal factors underlying accidents and hazards. These methods serve not only to identify the causal factors that should be addressed but also to propose countermeasures to eliminate or control them. Section 2.1 outlines representative accident models. Section 2.2 describes the traditional accident and hazard analysis methods, such as FMEA and FTA. Section 2.3 details the STPA analysis process, the methodology employed in this study. Additionally, section 2.4 introduces prior research regarding the hazard analysis of various automated transportation systems using STPA.

2.1 Accident Model

An accident model is a conceptual framework to explain why and how an accident occurs. Rather than merely analyzing isolated incidents, it aims to structurally understand the underlying contexts and mechanisms behind accidents, thereby facilitating the formulation of measures to prevent recurrence. This section introduces three representative accident models: the Domino Accident Model, the Swiss-Cheese Model, and the System-Theoretical Accident Model and Processes.

2.1.1 Domino Accident Model

The Domino Accident Model explains how hazards and accidents occur in a chain reaction, as shown in Figure 1. This model is based on the concept of a “Chain-of-Events”, the idea that when one domino falls, the others follow suit. It was proposed in the 1930s by American safety engineer H.W. Heinrich and provides a framework for analyzing the causes of accidents by breaking them down into five distinct problems (dominoes) [7]. These problems consist of “Ancestry, Social environment”, “Fault of person”, “Unsafe act or condition”, “Accident”, and “Injury”.

The model is closely related to Heinrich’s Law, the concept that 29 minor accidents and 300 near misses occur for every major accident [8]. This law reduces minor accidents and near misses, thereby decreasing major accidents. On the other hand, the Domino Accident Model is a framework to analyze why minor accidents and near misses occur. However, a challenge with the Domino Accident Model is its tendency to focus excessively on eliminating direct factors, relegating measures to address the underlying organizational issues behind accidents to a secondary priority.

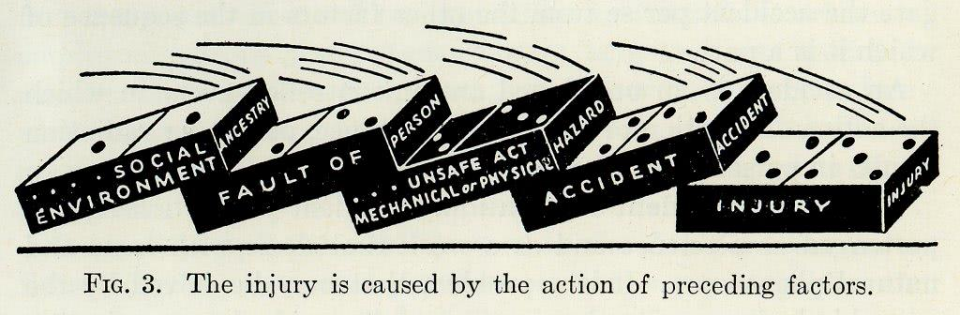


FIG. 3. The injury is caused by the action of preceding factors.

Figure 1. Domino Accident Model [7]

2.1.2 Swiss Cheese Model

The Swiss Cheese Model, proposed in the 1990s by Reason, describes the progression from human error to hazards and accidents [9]. The model is also based on the concept of a "Chain-of-Events".

Generally, corporations and organizations establish multiple barriers, such as regulations, inspections, and safety devices, to prevent accidents and maintain safety through the redundancy of these protective measures. However, these barriers have weaknesses represented as holes in slices of cheese. A hazard passes through holes in all the barriers, leading to a loss, as shown in Figure 2. Therefore, the focus of analysis shifts from individuals to systems and organizations.

In the Swiss Cheese Model, a clear distinction is drawn between active failures and latent failures. Active failures refer to acts or events, such as errors committed by frontline personnel, that directly trigger a hazard. Latent failures, conversely, are weaknesses embedded in management, design, or administrative systems that indirectly affect the likelihood of a loss; they are metaphorically represented as holes in cheese slices. A loss can thus be conceptualized as the result of latent failures becoming manifest, allowing active failures to pass through these holes in a cascading sequence. Consequently, the safety strategy advocated by the Swiss Cheese Model involves erecting additional defensive barriers to plug these holes and prevent losses through a multifaceted approach that combines measures such as periodic equipment inspections, standardized work procedures, and personnel training.

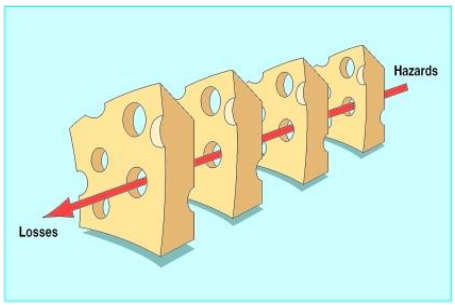


Figure 2. Swiss Cheese Model [10]

2.1.3 System-Theoretical Accident Model and Processes

The System-Theoretical Accident Model and Processes (STAMP) is a novel accident model grounded in systems theory that serves as an alternative to the traditional Chain-of-Events model. It was formulated by Nancy G. Leveson [11]. Both the Domino Accident Model and the Swiss Cheese Model are predicated on the Chain-of-Events concept, positing that accidents result from a sequential chain of failures. In contrast, in complex modern systems, accidents can arise from inappropriate interactions among components, even when no individual component has failed. Consequently, rather than treating accidents or losses merely as issues involving the failure of a single component, STAMP frames them as problems of dynamic control of the interactions among the components that constitute the system. Thus, STAMP is a model designed to prevent accidents and losses by focusing specifically on the safety constraints governing the behaviors and interactions among multiple system components.

By incorporating systems theory into accident models, STAMP has successfully integrated the following distinctive concepts:

- Treating the system as a whole, rather than merely as a collection of components
- Focusing on emergent properties arising from the interactions among system components
- Addressing emergent properties appropriately by considering all technical and social aspects

Emergent properties are characteristics possessed by the system as a whole that are not found in its individual components. To control emergent properties, such as safety, security, maintainability, reliability, and operability, it is necessary to manage the behaviors and interactions among the components appropriately.

Complex real-world systems possess a multi-layered structure; at various levels within the system, there exist components that act as controllers responsible for safety-related control and components that represent the controlled processes, as shown in Figure 3. A controller, based on its process model, exerts control actions over the processes immediately beneath it by enforcing the system's operational constraints. System safety is maintained when the interactions between the controller and the process function appropriately within the established constraints. When these system constraints are violated, unsafe control actions (UCAs) are generated, leading to an accident. Furthermore, feedback is transmitted from the process back to the controller. If this feedback is inappropriate, missing, or delayed, the controller may misperceive the process's actual state, leading to the generation of UCAs.

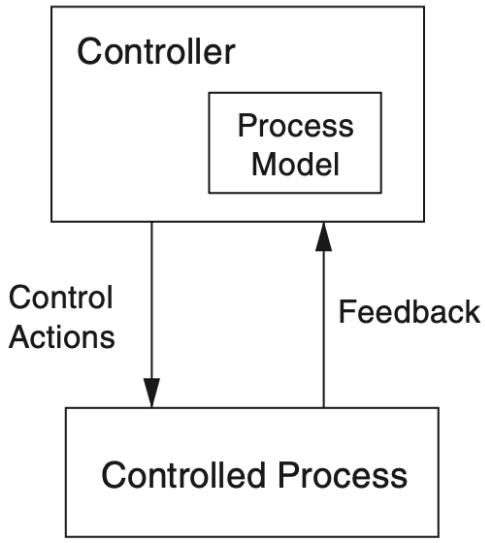


Figure 3. Hierarchical Safety Control Structure [6]

STAMP can include non-physical components, such as software, humans, and organizations, within its models. Currently, the most widely used accident and hazard analysis methods based on STAMP are STPA and Causal Analysis based on Systems Theory (CAST). STPA is a proactive analysis method used during development to identify potential accident factors and focus on eliminating or controlling hazards. CAST, conversely, is a retrospective analysis method used to evaluate accidents and incidents that have already occurred and identify their causes.

2.2 Traditional Accident and Hazard Analysis Methods

Accident and Hazard Analysis Methods translate the conceptual frameworks of accident models into concrete processes, enabling the identification of root causes and the proposal of countermeasures to eliminate them. This section provides an overview of the Failure Mode and Effects Analysis (FMEA) and the Fault Tree Analysis (FTA); they are representative hazard analysis methods based on the Domino Accident Model and the Swiss Cheese Model, respectively, and have also been adopted for use in the SC Maglev system.

2.2.1 FMEA

FMEA is an analytical methodology developed by the U.S. military in the 1940s to proactively prevent hazards by identifying potential failure modes in the key components of machinery or systems, assessing their impact, and implementing appropriate countermeasures [12]. Because the analysis begins with identifying individual failure modes, it is classified as a bottom-up approach. The risks that could cause machinery or systems to malfunction are referred to as “failure modes”, which include a wide variety of issues, such as severed wiring, short circuits,

and the wear or deterioration of components. Once identified, these failure modes are quantitatively evaluated using three metrics: severity, occurrence, and detection. Eventually, a Risk Priority Number (RPN) is calculated by multiplying these metrics, and countermeasures are prioritized for consideration, starting with failure modes with the highest RPN values.

The primary advantage of FMEA is its ability to quantitatively and comprehensively manage failure risks. However, it can only analyze single-point component failures, making it difficult to capture events resulting from complex interactions. In addition, because it presupposes the completion of detailed design, countermeasures often remain limited to adding redundancy rather than fundamental design changes, thereby leading to substantial rework costs.

2.2.2 FTA

Bell Laboratories developed FTA in the 1960s for the U.S. Air Force to assess the potential consequences of the Minuteman missile system, and it is now widely utilized across a diverse range of industries, including aerospace, nuclear energy, automotive, and, of course, railways [13]. This analytical methodology employs a top-down approach; it focuses on a "top event", a critical failure affecting the entire system, and systematically identifies its underlying causes. By doing so, it clarifies the root cause of problems and visually describes the logical pathways leading to failure through a graphical model known as a fault tree, shown in Figure 4. Furthermore, based on the probabilities of individual factors, the probability of the top event can be calculated. This calculation result enables the identification of the most critical factors and the pathway most likely to lead to failure.

FTA offers several advantages: it visualizes the pathways leading to a hazard, thereby facilitating the interpretation of analysis results, and it enables the quantitative calculation of the probability of a top event occurring. Conversely, challenges have been identified: the scope of analysis is primarily limited to physical component failures, making it difficult to capture non-failure factors and systemic factors. Furthermore, because a single fault tree can analyze only one event, conducting a comprehensive analysis of large-scale systems requires substantial time.

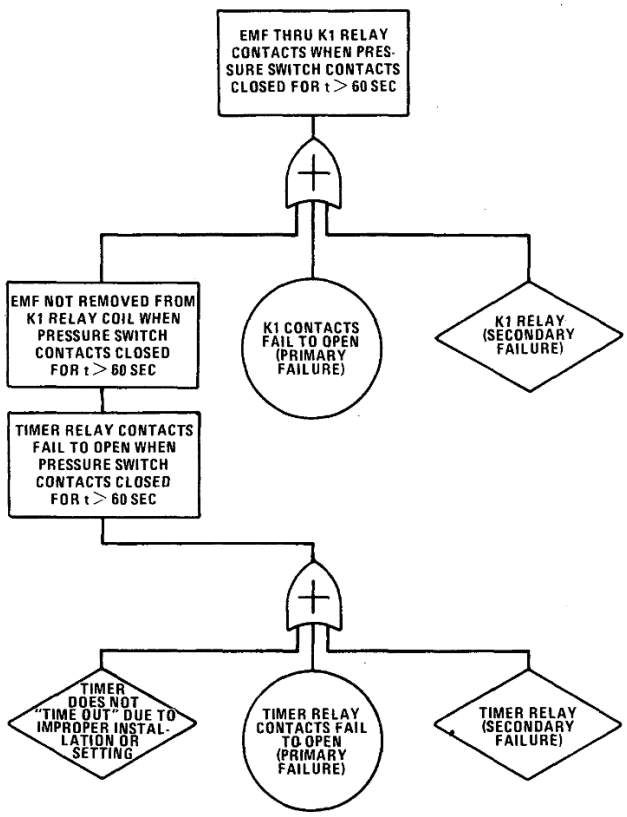


Figure 4. Typical Fault Tree [13]

2.3 STPA overview

STPA is a hazard analysis method that analyzes potential accident factors during the development phase and eliminates or controls hazards. This methodology is grounded in the System-Theoretical Model and Processes (STAMP) – a novel accident causality model based on system theory – and enables the analysis of hazards arising from complex processes and interactions among system components, extending beyond the scope of individual component failures or aging. STPA analyzes potential accident factors within a system by following the four steps outlined below.

- Define the Purpose of the Analysis
- Model the Control Structure
- Identify Unsafe Control Actions
- Identify Loss Scenarios

The following section provides a brief overview of each step, following the STPA Handbook [14].

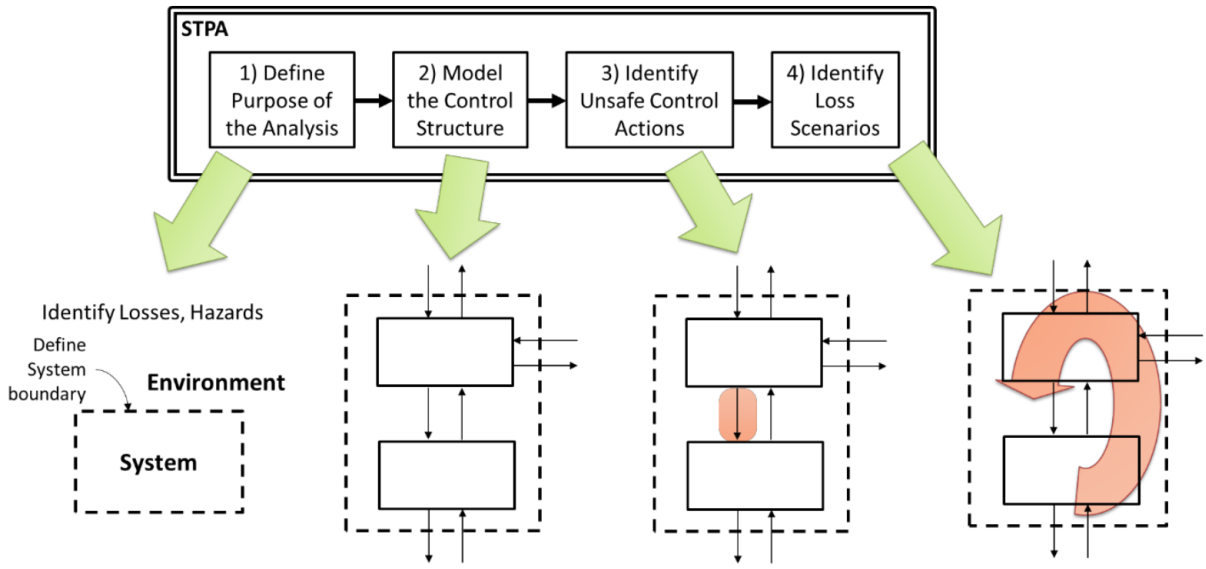


Figure 5. Overview of the Basic STPA Method [14]

2.3.1 Define the Purpose of the Analysis

In the first step, the analysis's purposes are defined. Defining the analysis objectives consists of three components: identifying losses, identifying system-level hazards, and identifying system-level safety constraints.

Losses are defined, such as loss of human life or injury, property damage, environmental contamination, mission failure, loss of trust, or leakage of confidential information, all of which would be deemed unacceptable by stakeholders. Typically, it is recommended to identify approximately five distinct losses. This is because identifying more losses carries the risk that the analysis may become unfocused or that individual analyses may become superficial and overly abstract.

In identifying system-level hazards, the first step is to define the system boundaries. The subsequent step involves identifying hazards, specifically, system states and conditions that could lead to a loss under worst-case environmental conditions. System-level hazards should not be described in detail as component-level causes, such as the physical failure of a specific component; rather, they should be strictly described as system-level states or conditions. Furthermore, hazards must not incorporate vague or recursive terminologies, such as “unsafe” or “unintended.”

System-level safety constraints are requirements that must be met to prevent hazards. They are identified by inverting the states of system-level hazards.

2.3.2 Model the Control Structure

In this step, a hierarchical control structure, a diagram consisting of blocks and arrows organized hierarchically according to levels of control authority, is modeled. The blocks represent the system components, such as controllers and processes, while the arrows represent control actions and feedback, as shown in Figure 6.

A controller can issue control actions, such as commands or requests, to a process to control its operation and enforce constraints. The control algorithm is the controller's decision-making mechanism that determines which control actions to apply to the process. The process model represents the controller's beliefs and serves as the foundation for its decision-making. This process model is updated periodically based on feedback received from the process.

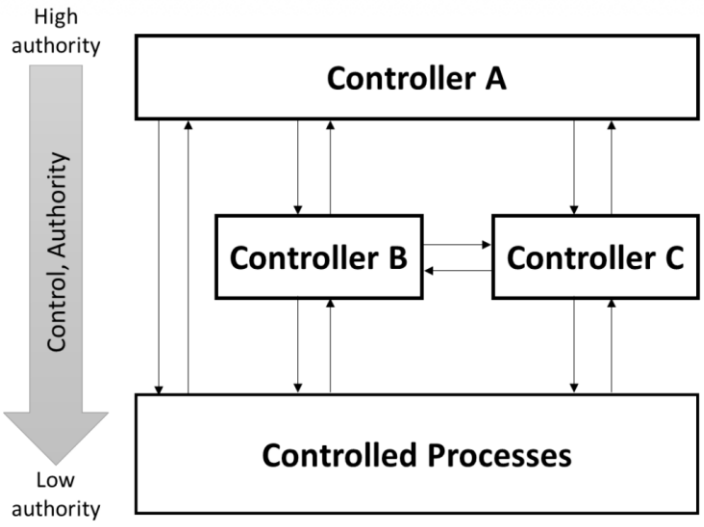


Figure 6. Generic Hierarchical Control Structure [14]

2.3.3 Identify Unsafe Control Actions

An unsafe control action (UCA) is a control action that leads to a hazard within a specific context and under worst-case conditions. UCAs can be categorized into the following four groups:

- Not providing causes hazard
- Providing causes hazard
- Providing too early, too late, or out of order
- Stopped too soon, applied too long

To identify UCAs, it is necessary to clearly define the context in which a control action becomes unsafe. This context must specify the actual states and conditions, rather than merely

what the controller's process model believes to be true. Each UCA must be linked to one or more hazards.

Furthermore, once a UCA is identified, it can be converted into controller constraints for each controller that must be satisfied to prevent the UCA.

2.3.4 Identify Loss Scenarios

Finally, scenarios are generated to describe the causes that could lead to UCAs or hazards. To generate these scenarios, it is necessary to consider why a UCA was executed or why a safe control action was executed inappropriately. Potential factors that cause a UCA to be executed include (1) unsafe controller behavior and (2) inadequate feedback and other inputs, as shown in Figure 7.

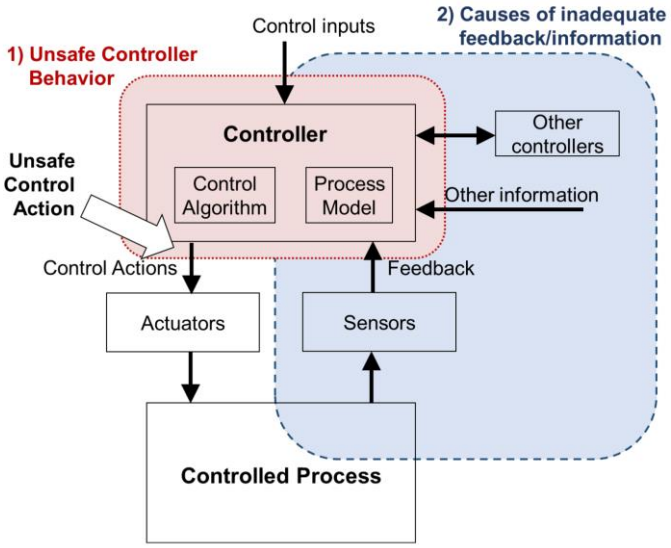


Figure 7. Generation Mechanism of UCA: (1) Unsafe Controller Behavior and (2) Inadequate Feedback and Other Inputs [14]

Conversely, factors leading to the improper execution of a safe control action include malfunctions in the control action transmission path or within the controlled process itself, as shown in Figure 8. Each scenario is formatted in a sentence structure and should be linked to the UCA.

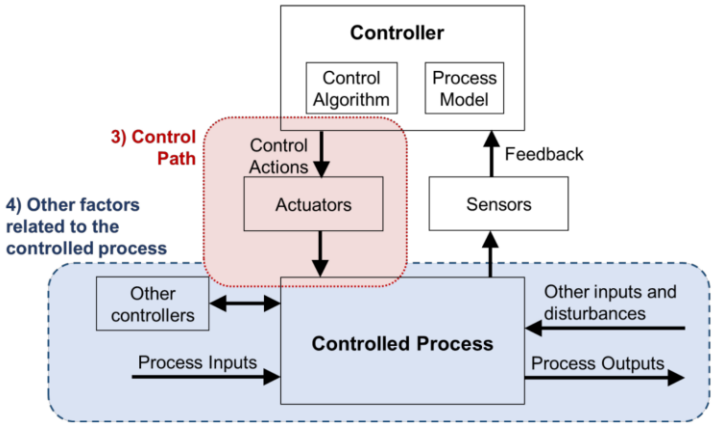


Figure 8. Generation Mechanism of UCA: (3) Control Path and (4) the Controlled Process Itself [14]

2.4 Prior Research Regarding the Hazard Analysis for Autonomous Transportation Using STPA

Autonomous driving relies more on software-based control than traditional manual driving; conventional safety analysis methods have proven inadequate for evaluating safety. Consequently, there has been a recent surge in research and initiatives to apply STPA to assess the safety of autonomous driving systems. This section provides an overview of prior research on the safety evaluation of autonomous systems across the automotive, aviation, maritime, and railway sectors using the STPA method.

2.4.1 Automobile

Rachel Cabosky focused on "highway traffic assist" features in automobiles. She employed STPA to conduct a safety analysis of the interactions between human operators and this specific function[15]. This study utilized a three-tiered Control Structure—each at a different level of abstraction—to perform the analysis. It successfully generated a comprehensive set of recommendations ranging from organizational-level guidelines to specific technical recommendations, thereby demonstrating the utility of STPA for evaluating the safety of autonomous driving systems in automobiles. Furthermore, the study highlights that, when conducting an STPA analysis, iteration and refinement at every step are crucial for rapidly generating more effective recommendations.

2.4.2 Airplane

Ryan Bowers and John P. Thomas conducted a study utilizing STPA to identify risks associated with neural network-based autonomous flight software [16]. STPA not only identified novel risks, vulnerabilities, and critical undocumented assumptions but also proposed effective countermeasures against scenarios that could lead to catastrophic accidents or losses. Since this

study was conducted after software development had been completed—specifically, before the commencement of test flights—it generated recommendations that enhanced the safety of subsequent test flights. However, the authors note that had STPA been applied during upstream phases—such as requirements definition or design—it would have been possible to implement the necessary design modifications and solutions to ensure safe testing and operation, thereby potentially reducing overall development costs. This constitutes a significant piece of prior research that underscores the critical importance of applying STPA at the earliest possible stages of development.

2.4.3 Vessel

Blake Ryan Abrecht conducted a study evaluating the safety of software-controlled Naval Offshore Supply Vessels (OSVs) using FTA, FMEA, and STPA [17]. The study reports that STPA not only successfully identified all failure scenarios previously identified by FTA and FMEA but also identified non-failure scenarios—those that could not be detected using traditional analysis methods.

2.4.4 Railway

A hazard analysis utilizing STPA was conducted on the automated driving technology (GoA2) currently under development for the Tokaido Shinkansen [18]. This study, too, reports that STPA demonstrated its effectiveness in identifying non-failure scenarios when compared to conventional analysis methods. The railway sector is a mature industry, and it has historically been customary to evaluate its safety using traditional analysis techniques such as FTA and FMEA. Based on this research, it is concluded that applying STPA—even to increasingly complex railway systems—makes it possible to construct safer systems.

Chapter 3: System Description

This chapter provides an overview of the technology behind the SC Maglev system, its development history, and the achievements and challenges in the system's hazard analysis. Section 3.1 introduces the fundamental technologies underpinning the SC Maglev system. While the system incorporates a wide range of technologies, this section focuses on the system's basic configuration, the principles of train levitation and propulsion, and safety-related control technologies. Section 3.2 traces the long history of the SC Maglev system's development. It also examines the hazard analyses conducted throughout this history and explains the challenges they pose.

3.1 SC Maglev System Technology

The technical specifications and system architecture described in this section are based on the work of Oshima [19].

3.1.1 Fundamental Technology for the SC Maglev System

The appearance of the SC Maglev system is shown in Figure 9. The technology essential for ultra-high speed levitation travel at 311 miles per hour is the superconducting magnet. Superconductivity is the phenomenon where electrical resistance drops to zero when certain metals or compounds are cooled to extremely low temperatures. The SC Maglev system uses superconducting coils made of niobium-titanium alloy, cooled to 4K using liquid helium. Because electrical resistance is zero, when current is applied to the superconducting coil, it flows semi-permanently within the coil, forming an extremely powerful superconducting magnet. This powerful magnetic field enables the SC Maglev vehicle to levitate.

Superconducting magnets are mounted on the lower sections of the coupling points and vehicle front ends of SC Maglev trains, positioned on both sides of the vehicle. Each superconducting magnet contains four superconducting coils. The track for the SC Maglev system is a U-shaped structure that fully encloses the vehicle's lower half. This track is called the guideway. Ground coils are installed in the guideway's side walls. Ground coils are conventional coils made of materials such as copper or aluminum. There are two types of ground coils: propulsion coils and levitation and guidance coils. Propulsion coils are positioned on the surface of the side walls, while levitation and guidance coils are mounted behind the propulsion coils.

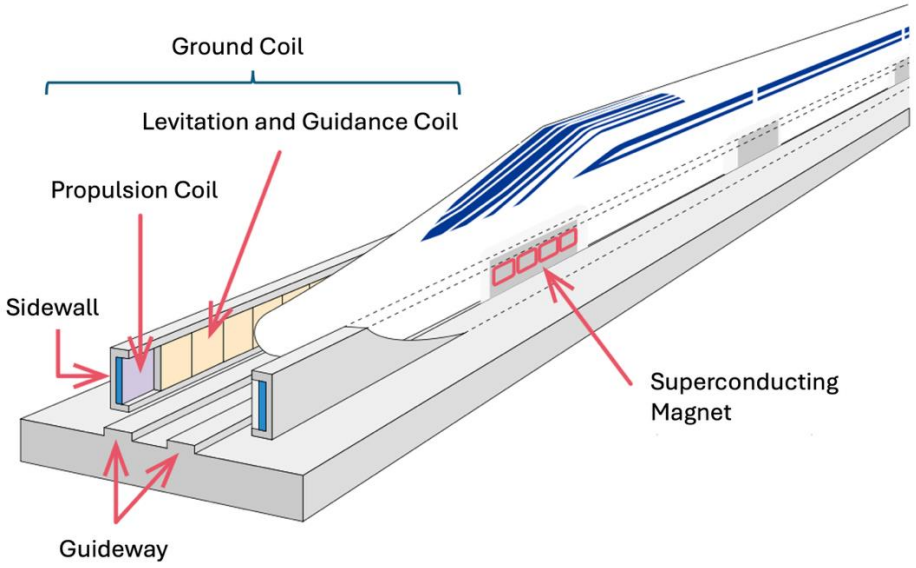


Figure 9. Appearance of the SC Maglev System [19]

3.1.2 Propulsion Principle

The SC Maglev system uses ground-controlled linear motor propulsion. *Ground control* refers to supplying the power required for propulsion to ground coils, eliminating the need for pantograph-style power collection on the vehicle, as seen in conventional railway systems.

A linear motor can be compared to a conventional rotating motor, with the latter cut open and extended linearly, as shown in Figure 10. The rotor inside the conventional motors corresponds to the superconducting magnets mounted on the SC Maglev vehicle, while the outer stator corresponds to the propulsion coils on the ground. When an alternating current of the appropriate frequency is applied to the propulsion coils, a traveling magnetic field is generated that moves at the same speed as the vehicle. The superconducting magnets have alternating N and S poles. Between the magnetic fields of the superconducting magnets and the traveling magnetic field on the ground, attractive forces occur between opposite magnetic poles, while repulsive forces occur between like magnetic poles.

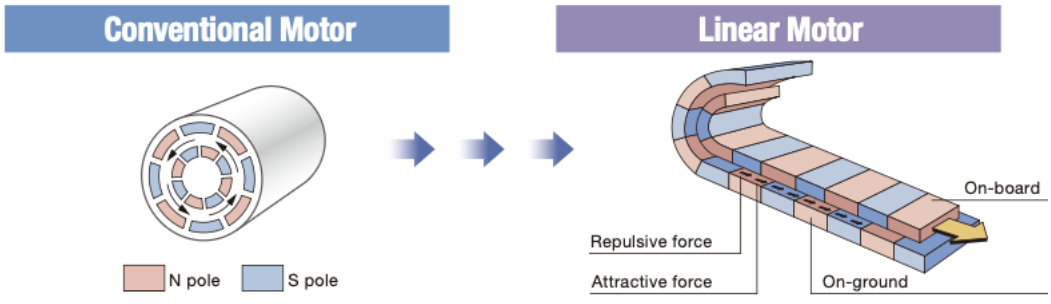


Figure 10. Comparison between Conventional Motor and Linear Motor [5]

Applying an AC with a phase that generates forward-attraction and backward-repulsion forces in the superconducting magnets provides propulsion, as shown in Figure 11. Reversing the phase generates braking force. Therefore, by precisely detecting the position and speed of the SC Maglev vehicle while controlling the AC flowing through the propulsion coils, the train's acceleration, deceleration, and stopping can be controlled.

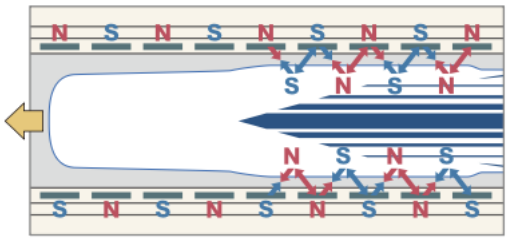


Figure 11. Propulsion Principle [5]

3.1.3 Levitation Principle

The levitation system for SC Maglev vehicles employs an electrodynamic suspension, as shown in Figure 12. When the superconducting magnets of an SC Maglev vehicle pass through the levitation and guidance coils, an induced current is generated by electromagnetic induction, turning the coils into electromagnets. The levitation and guidance coils consist of two coils arranged vertically, connected in a figure-eight configuration.

When the center height of the vehicle's superconducting magnet matches the center height of the levitation and guidance coil, no current flows through the levitation and guidance coil, and no levitation force is generated. When the center height of the vehicle's superconducting magnet is lower than that of the levitation and guidance coil, current flows through the levitation and guidance coil. An attractive force acts between the superconducting magnet and the upper coil of the levitation and guidance coil, while a repulsive force acts between the superconducting magnet and the lower coil. These forces generate an upward force on the vehicle, namely the levitation force. Conversely, when the center height of the vehicle's superconducting magnet is higher than that of the levitation and guidance coil, a downward electromagnetic force is generated, preventing the vehicle from deviating outside the guideway.

Note that at low speeds, a sufficient levitation force cannot be obtained. Therefore, when traveling at speeds below around 75 miles per hour, the vehicle is supported by the support wheels.

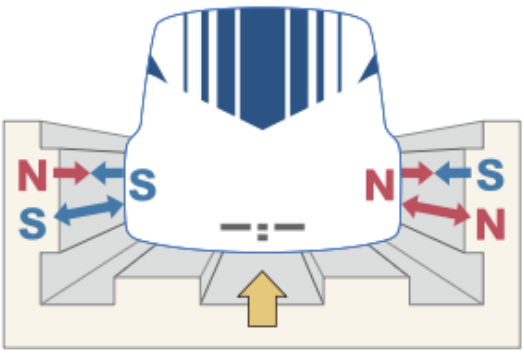


Figure 12. Levitation Principle [5]

3.1.4 Guidance Principle

The lateral guidance force employs the same principle as the levitation force shown in Figure 13. The levitation and guidance coils installed on both side walls of the guideway are connected by cables. When the vehicle deviates from the center toward either side, an attractive force acts in the direction it is moving away from the center. In contrast, a repulsive force acts toward the side it is approaching. These forces generate a lateral guidance force that pushes the vehicle back toward the center of the guideway.

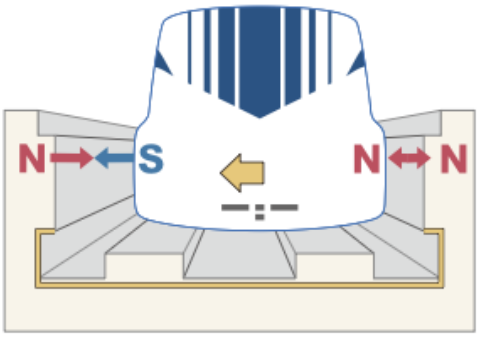


Figure 13. Guidance Principle [5]

3.1.5 Running Control

Since all control of the SC Maglev system is performed from the ground, there is no driver on board. Instead, various systems work together to automate the running control of each train [20]. The core running control system, the Train Operation Management System, creates and manages the timetable, and comprehensively monitors and controls the running of each train. The Train Operation Management System generates *run curve* information that continuously indicates where each train should be and at what speed it should travel. The system provides the information to the Drive Control System. The Drive Control System manages the train's acceleration and

deceleration. Based on the run curve information, it sequentially calculates the current and phase to apply to the propulsion coils, then supplies an AC to them.

Run curve information consists of two profiles: the operating and emergency patterns. The operating pattern is generated by considering factors such as the timetable, delays, route conditions (e.g., gradients and curve radii), the vehicle's acceleration and power capacities, ride comfort, and energy efficiency. It functions as a guideline for trains to run efficiently and on schedule. On the other hand, the emergency pattern is generated based on the distance to the preceding and following trains, braking deceleration performance, changes in braking distance due to gradients, and stopping distance under worst-case conditions. It serves as a guide rail to ensure safe train operation. The speed displayed in the emergency pattern is called the safety allowable speed.

3.1.6 Safety Control

The fundamental principle of safe rail operation is controlling train movement within the permitted section and speed range, and this naturally applies to the SC Maglev system as well.

The Drive Control System controls the SC Maglev vehicle's speed and position based on the operating pattern. Therefore, if the train's speed exceeds the speed displayed in the operating pattern, the system first attempts to reduce the speed. Specifically, it generates the service brake by applying an alternating current to the propulsion coils, inducing a backward electromagnetic force on the vehicle and thereby decelerating it.

Meanwhile, the Safety Control System, separate from the Drive Control System, continuously monitors the running position and speed. When deceleration via the service brake proves insufficient for any reason, causing the train to reach the safety allowable speed, the Safety Control System immediately applies the emergency brake. By physically separating the control system and the safety system, the system design is fail-safe: even if the Drive Control System malfunctions, the Safety Control System can still bring the train to a stop.

3.1.7 Emergency Brake System

The emergency brake on SC Maglev trains combines an aerodynamic brake with a wheel disc brake. The aerodynamic brake deploys panels on the vehicle roof to increase air resistance and slow the train. Since air resistance increases proportionally to the square of the speed, this brake is particularly effective at high speeds. On the other hand, the wheel disc brake slows the vehicle by generating friction between the support wheels and the brake discs. They are primarily effective at low to medium speeds.

3.1.8 Onboard Equipment Control

The Onboard Train Control System controls on-board functions, including monitoring and controlling onboard equipment, as well as brake control, door control, and the deployment and retraction of the support wheels, in response to ground control commands. Based on control commands from the ground and the running information, such as train position and speed, the system performs automatic centralized control of the vehicle's various equipment and devices.

3.2 Development History and Safety Analysis in the SC Maglev System

The development history and safety analysis in the SC Maglev system described in this section are based on the report published by the Technical Evaluation Committee for Superconducting Maglev Practical Application (hereinafter referred to as the "Technical Evaluation Committee") [21].

3.2.1 Development History

Development of the SC Maglev system began in 1962 under the Japanese National Railways (JNR). Following the breakup and privatization of JNR in 1987, the project was taken over by the Railway Technical Research Institute, a public interest incorporated foundation, which has continued to advance the technology.

In 1990, the Basic Plan for the Development of Superconducting Maglev System Technology and the Construction Plan for the Yamanashi Maglev Line were approved by the Minister of Transport. This approval marked the start of technological development aimed at establishing a roadmap for practical application, as well as the commencement of development on the Yamanashi Maglev Line, with full-scale operational tests beginning in 1997.

In 2000, the Technical Evaluation Committee, based on three years of operational tests and technological development, assessed that although there were some issues regarding long-term durability and economic viability, the achievement of the technical goals for the practical implementation of an ultra-high-speed mass transit system was in sight.

At the 2005 committee meeting, the Technical Evaluation Committee evaluated both the performance requirements for a railway transport system and the equipment characteristics specific to the SC Maglev system, concluding that "the foundation technologies for the practical application of the SC Maglev system have been established." Future challenges identified included continuing operational tests to verify long-term durability, developing technologies to further reduce costs, and reviewing equipment specifications for application on commercial lines. In response, construction began on an initial section of the commercial line, and long-distance operational tests were initiated.

At the 2009 committee meeting, the progress of technological development since 2005 and the prospects for establishing practical technologies required for commercial operation were evaluated separately; the Technological Evaluation Committee concluded that “the technologies necessary for a commercial SC Maglev system have been comprehensively and systematically developed.”

Since then, the system has accumulated operational test records designed to simulate actual service, including tests involving multiple trains running simultaneously, passing tests, and long-duration endurance runs. At a committee meeting in 2017, it was determined that the necessary technical development for commercial operation had been completed.

Central Japan Railway Company is continuing to develop the technologies necessary to reduce costs further and improve ride comfort. Not only did the cumulative mileage on the Yamanashi Maglev Line exceed 3.11 million miles in 2024, but the company also introduced a new, improved test vehicle in 2025 and has begun running tests with it.

3.2.2 Systematic Approach to Ensuring Safety and Reliability

While the Technological Evaluation Committee has already conducted a preliminary assessment of the safety and reliability of the SC Maglev system, this section outlines a systematic approach to ensuring safety and reliability throughout the development, design, manufacturing, and operation of a commercial line.

To ensure safety and reliability, the SC Maglev system has established and operates a safety and reliability management system centered on design reviews. These design reviews are conducted at each stage of the project – conceptual design, procurement, manufacturing, installation, and operation – in accordance with project progress. They involve discussions among all stakeholders across technical disciplines and utilize checklists for verification. In addition, there is an independent department responsible for conducting these reviews, ensuring that evaluations are performed from a perspective distinct from that of the developers.

3.2.3 Track Record in Hazard Analysis

During design reviews, hazard analyses using Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) were conducted. In the 2017 Technical Evaluation Report, the status of FTA and FMEA was verified using the SC Maglev system’s safety devices as an example, and the results indicated that the analyses were deemed sufficient. Guidelines for future hazard analyses have also been established, aiming to refine further and quantify FTA and FMEA, and to identify specific countermeasures against anticipated emergency events.

3.2.4 Limitations and Challenges of Hazard Analysis

The primary focus of FMEA and FTA is on hardware failures and component lifespans. Therefore, these analyses are effective analytical methods for addressing reliability issues, specifically situations in which "a component fails, and a hazard occurs." However, they cannot address safety issues where "a hazard occurs due to improper control actions or interactions between components, even though the components themselves have not failed."

The Technical Evaluation Report on the SC Maglev system addressed the safety and reliability of the Train Operation Management System, the Safety Control System, and the Drive Control System. Based on the results of FTA and FMEA, as well as years of operational testing, the report concluded that the development necessary for practical implementation had been completed. However, the SC Maglev system is highly automated, with most of its control functions performed by software rather than humans. Software does not have the same concepts of failure or aging as hardware; instead, hazards arise from deficiencies in design or specifications. In other words, even if individual components operate according to specifications, unsafe behavior may occur at the system level, indicating limitations in conducting hazard analyses using FTA and FMEA, which focus on failures and lifespans.

Furthermore, in emergencies, the operational framework anticipates manual control interventions by the operator and conductor, in addition to automated control by the system. While this intervention makes the interactions between humans and the system extremely complex, methodologies such as FTA and FMEA face significant difficulty in identifying hazards, as they struggle to analyze the specific context underlying human decision-making – that is, why a particular judgment was reached – as well as the intricate interactions occurring between humans and the system. Additionally, there is no detailed mention of the roles of the operator and conductor; consequently, the system's safety constraints, including the specific human roles and decision-making criteria applicable during emergencies, have not been defined.

Therefore, in addition to conventional reliability analyses such as FTA and FMEA, implementing STPA is required to conduct safety analyses that focus on the system, specifically addressing design and specification deficiencies and inappropriate interactions. This approach not only identifies hazards that cannot be detected through FTA and FMEA but also facilitates the formulation of recommendations on the necessary system specifications and safety constraints for the operator and conductor.

Chapter 4: Hazard Analysis of the SC Maglev System

In this chapter, we will conduct a hazard analysis of the SC Maglev system using the STPA method. Although the basic configuration of this system incorporates insights from the Tokaido Shinkansen, the fact that trains are controlled remotely from the ground, without a driver on board, is a key feature that distinguishes it from conventional railway systems. Furthermore, while two to three conductors are scheduled to be on board each train, their specific roles are still under discussion.

Specifically, the question is whether conductors will not be involved in operational control or the control of onboard equipment (such as doors and landing gears), focusing solely on passenger service and evacuation guidance in emergencies, or whether they will bear more direct responsibility for ensuring safety, such as controlling doors during boarding and alighting and operating emergency brakes.

Therefore, in this study, we assume that the control structure changes depending on whether the conductor has safety responsibilities, and we apply STPA to two cases: a model that does not include the conductor as a system component (the "without conductor" model) and a model that includes the conductor as a system component (the "with conductor" model). In the following sections, Section 4.1 details the analysis flow and results for the "without conductor" model, and Section 4.2 shows these results with the "with conductor" model.

4.1 Application of STPA to the "Without Conductor" Model

This section presents the results of applying STPA to the "without conductor" model. Based on the analysis process defined in Section 2.3, we will sequentially report on the analytical steps, ranging from defining the analysis purpose to modeling the control structure, identifying UCAs, and identifying loss scenarios.

4.1.1 Define the Purpose of the Analysis

First, following the STPA procedure, we define the analysis's objectives. Specifically, we identify the losses, system-level hazards, and corresponding system-level safety constraints.

The Losses

In the SC Maglev system, the losses extend far beyond direct physical damage, such as passenger injuries or fatalities, and damage to facilities or vehicles. They also include a wide range of other consequences, such as reduced customer satisfaction due to service interruptions or significant delays, and a loss of social trust resulting from environmental impact. This study focuses specifically on evaluating the impact that the presence or absence of safety responsibilities for the conductor has on the system. Therefore, while prioritizing physical losses directly related

to safety, the following three types of losses were defined to ensure a comprehensive analysis that accounts for the system's role as a public transportation service.

- **L-1**: Injury or death to humans
- **L-2**: Physical Damage to the vehicle, guideway, or other equipment
- **L-3**: Loss of the transportation mission (Transport passengers to their destination)

System-Level Hazards

Once the losses have been defined, system-level hazards are identified. Hazards must be linked to one or more losses and should be related to the system as a whole or its state. To meet these criteria, hazards are described in the following format [14].

<Hazard> = <System> & <Unsafe Condition> & <Link to Losses>

In this study, we defined the following six hazards.

- **H-1:** The SC Maglev is in a state of overspeed. [L-1, L-2, L-3]
- **H-2:** Two or more SC Maglev trains exist in the same block section (state of not maintaining a safe margin from other trains). [L-1, L-2, L-3]
- **H-3:** The SC Maglev traps passengers, leaving no evacuation route. [L-1, L-2, L-3]
- **H-4:** The SC Maglev is not being stopped during passenger boarding or alighting. [L-1, L-3]
- **H-5**: The SC Maglev is colliding with an obstacle, the guideway, or another train [L-1, L-2, L-3]
- **H-6:** The SC Maglev significantly delays. [L-3]

System-Level Safety Constraints

Once system-level hazards have been defined, system-level safety constraints are automatically defined as well. This is because they can be derived simply by inverting the condition. The format for system-level safety constraints is as follows [14]. Each safety constraint should be traceable to one or more hazards.

<Safety Constraint> = <System> & <Condition to Enforce> & <Link to Hazards>

In this study, the following five safety constraints were identified.

- **SC-1:** The SC Maglev must be controlled in accordance with the run curve information. [H-1, H-2, H-5]
- **SC-2:** Only one SC Maglev must exist in a block section at a time. [H-2, H-3]
- **SC-3:** The SC Maglev must ensure an evacuation route is available. [H-3]
- **SC-4:** The SC Maglev must be stopped during passenger boarding and alighting. [H-4]

- **SC-5:** The SC Maglev must avoid any collision with an obstacle, the guideway, or another train. [H-5]
- **SC-6:** The SC Maglev must operate on time. [H-6]

4.1.2 Model the Control Structure

Control Structure for the "Without Conductor" Model

Once the analysis's purpose has been determined, the next step is to model the system's hierarchical control structure. Figure 14 shows the control structure of the "without conductor" model. An enlarged version is included in Appendix A.1.

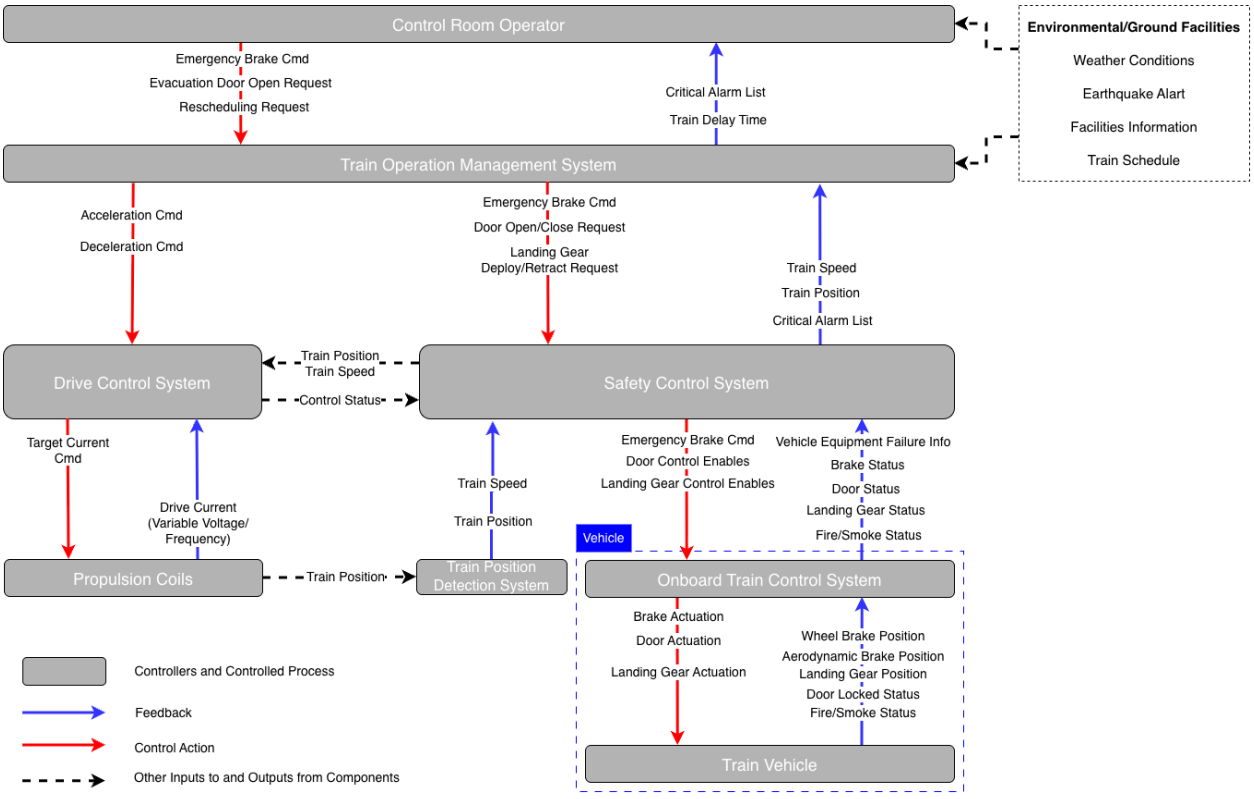


Figure 14. Control Structure for the "Without Conductor" Model

Responsibilities, Control Actions, Process Model, and Feedback

Each controller depicted in the control structure diagram forms a feedback loop with other controllers and control processes, and they are closely interrelated. For each controller, the following should be defined: the responsibilities it must fulfill to maintain system safety; the

control actions that impose constraints on subordinate controllers and control processes; the process model that serves as the basis for decision-making; and the feedback required for decision-making. Table 1 shows the definitions of each controller's responsibilities, control actions, process model, and feedback.

Table 1. Each Controller's Responsibilities, Control Action, Process Model, and Feedback/Other Input (the "Without Conductor" Model)

Controller	Responsibilities	Control Action	Process Model	Feedback & Other Input
Control Room Operator	Prevent the escalation of losses when external disturbances (e.g., earthquakes or fires) occur. Prevent the escalation of losses when abnormal behavior within the vehicle (e.g., abnormal vibration, noise, or odors) occurs. Ensure the safe evacuation of passengers. Minimize train delays and ensure the prompt restoration of the schedule. Maximize the operational efficiency of rolling stock and crew.	Emergency brake command Evacuation door open request Reschedule request	External disturbances occur. Abnormal behavior in the vehicle occurs. Passengers need evacuation. The train is delayed. The schedule is disturbed.	Critical Alarm List Train Delay Time Weather Condition Earthquake Alert Facilities Information Train Schedule
Train Operation Management System	Maintain the train's target speed.	Acceleration command Deceleration command	The train speed exceeds or falls below the target speed.	Train Speed Train Position

Controller	Responsibilities	Control Action	Process Model	Feedback & Other Input
	Ensure that the train operates according to schedule. Provide opportunities for passengers to board and alight. Maintain vehicle support and levitation in accordance with the train's speed. Ensure that commands from the Control Room Operator are transmitted to the Safety Control System.	Emergency brake command Door open/close request Landing gear deploy/retract request	The train speed exceeds or falls below the levitation threshold. The train stops at the correct location. The control room operator's input has been received.	Critical Alarm List Inputs from the Control Room Operator Weather Condition Earthquake Alert Facilities Information Train Schedule
Drive Control System	Calculate the target current. Maintain the target current flowing through the coils required to achieve the train's target speed.	Target current command	The drive current does not correspond to the target current.	Inputs from the Train Operation Management System (Acceleration or Deceleration) The Drive Current
Safety Control System	Prohibit the train from exceeding the safe allowable speed limit. Prohibit door opening while the train is in motion or at an incorrect location.	Emergency brake command Door control enables Landing gear control enables	The train exceeds the safe allowable speed limit. The train is still in motion or stops at an incorrect location.	Train Speed Train Position Vehicle Equipment Failure Info Brake Status Door Status

Controller	Responsibilities	Control Action	Process Model	Feedback & Other Input
	Prohibit door closing while passengers are boarding or alighting. Prohibit wheel retraction during low-speed travel. Prevent wheel extension while the train is in an overspeed condition. Ensure that an emergency brake command from the Control Room Operator is transmitted to the Safety Control System.		Passengers boarding/alighting continue. The train's speed exceeds the levitation threshold.	Landing Gear Status Fire Status
Onboard Train Control System	Ensure vehicle deceleration. Ensure that boarding and alighting are fully complete and that no objects are caught in the doors. Ensure that the doors remain fully open during boarding and alighting. Ensure that the doors remain fully	Brake actuation Door actuation Landing gear actuation	The train needs deceleration. Something is caught in the doors. The doors open/close. The landing gears deploy/retract.	Wheel Brake Position Aerodynamic Brake Position Landing Gear Position Door Locked Status Fire/Smoke Status

Controller	Responsibilities	Control Action	Process Model	Feedback & Other Input
	closed during travel. Ensure vehicle support during low-speed operation. Ensure vehicle levitation during high-speed operation.			

Detailed Control Actions

This section provides detailed descriptions of the control actions defined in Figure 14. A control action is a set of instructions, commands, or requests issued by a controller to its subordinate controllers or controlled processes. Typically, each controller issues distinct control actions to multiple subordinate entities or processes. The definition format for these control actions is specified as follows:

- Control Action
  - Controller → Lower-level Controller/Controlled processes
  - Definition

Due to the specialized nature of the railway domain, the definitions of control actions incorporate several technical terms. To facilitate the reader's comprehension, Table 2 elucidates the specific meanings and contexts of these terms as utilized in this study.

Table 2. Meanings and Contexts of Technical Terms

Term	Definition / Description
Rescheduling	This is a process of adjusting the train timetable in response to disruptions to ensure safety and restore normal operations. These rescheduling measures include service cancellations, emergency stops, temporary speed restrictions, changes to arrival and departure sequences, platform reassignments, and rolling stock substitutions.
Run curve	A target velocity profile that seamlessly integrates the optimal travel speeds calculated across all segments. Run curve information represents the acceleration and deceleration trajectory of a train.

Term	Definition / Description
Safety-allowable speed pattern	A dynamically generated velocity constraint that defines the maximum allowable speed at any given position to ensure the safe operation of the train based on various safety-critical factors, including the distance to the preceding train, infrastructure constraints (curves and gradients), and temporary speed restrictions.

Control Room Operator Controls

- Emergency Brake Command
  - Control Room Operator → Train Operation Management System
  - In an emergency or when necessary, activate the target vehicle's emergency brakes remotely.

- Evacuation Door Open Request
  - Control Room Operator → Train Operation Management System
  - When an evacuation is needed, request that the target vehicle's door be opened remotely.

- Reschedule Request
  - Control Room Operator → Train Operation Management System
  - When train delays occur, trains are rescheduled to facilitate recovery and ensure operational safety.

Train Operation Management System Controls

- Acceleration/Deceleration Command
  - Train Operation Management System → Drive Control System
  - Instruct the train to accelerate or decelerate according to the run curve information.

- Emergency Brake Command
  - Train Operation Management System → Safety Control System
  - The emergency brake command, once received from the Operator, is relayed to the Safety Control System.

- Door Open/Close Request
  - Train Operation Management System → Safety Control System
  - Upon confirming that the train velocity has reached zero and that the vehicle is stationary at the designated position within the station, a request to open the passenger doors is issued. Furthermore, once the scheduled departure time is reached,

a request to close the doors is issued. The request to open the doors is also issued upon receipt of an evacuation door open request from the Control Room Operator.

- Landing Gear Deploy/Retract Request
  - Train Operation Management System → Safety Control System
  - When the train's velocity falls to 75 miles per hour, a request to deploy the wheels is issued. Conversely, when the velocity exceeds the threshold, a request to retract the wheels is issued.

Drive Control System Controls

- Target Current Command
  - Drive Control System → Propulsion Coils
  - Calculate the optimal coil current amplitude and frequency required to regulate propulsion and ensure strict compliance in accordance with the run curve information, and apply this current to coils.

Safety Control System Controls

- Emergency Brake Command
  - Safety Control System → Onboard Train Control System
  - Upon detecting that a train is traveling more than the safety-allowable speed or receiving an emergency brake command, issue an emergency brake command to the affected train.

- Door Control Enable
  - Safety Control System → Onboard Train Control System
  - Upon receipt of a Door Open/Close Request, verify whether the vehicle has reached a complete stop and is accurately located at the current position, and allow door control.

- Landing Gear Control Enable
  - Safety Control System → Onboard Train Control System
  - Upon receipt of a Landing Gear Deploy/Retract Request, evaluate the validity of the request based on the train's real-time velocity, and allow landing gear control.

Onboard Train Control System Controls

- Brake Actuation
  - Onboard Train Control System → Train vehicle
  - Upon receiving an emergency brake command, initiate the wheel-disc brakes and the aerodynamic brakes.

- Door Actuation
  - Onboard Train Control System → Train vehicle
  - Upon receipt of a door control enable, open or close the passenger doors.

- Landing Gear Actuation
  - Onboard Train Control System → Train vehicle
  - Upon receipt of a landing gear enable, deploy or retract the wheel assembly.

4.1.3 Identify Unsafe Control Actions

Unsafe Control Actions

In this section, we identify UCAs in the "without conductor" model. To comprehensively evaluate the model, we identify UCAs for each controller, focusing on states during train operation and station stops.

As noted in Section 2.3, there are four types of UCA. Since templates are provided for each type—including the context in which the UCA occurs and the way control actions are executed—we will use the templates shown in Table 3 in this analysis as well. Additionally, each UCA has been assigned a unique ID, which is necessary for linking it to the scenarios to be generated later. A corresponding hazard ID is assigned to the end of each UCA, making it possible to trace which hazards each UCA is associated with.

Table 3. UCA Templates

UCA Type	UCA Template
Type 1: Not providing causes hazard	Type 1: <Controller> does not provide <control action> when <context>
Type 2: Providing causes hazard	Type 2: <Controller> provides <control action> when <context>
Type 3: Too early, too late, out of order causes hazard	Type 3: <Controller> provides <control action> too later after <context>
Type 4: Stopped too soon, applied too long causes hazard	Type 4: <Controller> stops providing <control action> too soon before <context>

As a result of the analysis, 102 UCAs were identified. Table 4 shows a sample of the identified UCAs. All UCAs are listed in Appendix A.2.

Table 4. Samples of the Identified UCAs in the "Without Conductor" Model

Control Action	Type 1: Not Providing Causes Hazard	Type 2: Providing Causes Hazard	Type 3: Too early, too late, out of order	Type 4: Stopped too soon, applied too long
Controller: Control Room Operator				
Emergency Brake Command	(UCA-9) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-10) Control Room Operator does not provide an emergency brake command when abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	(UCA-11) Control Room Operator provides an emergency brake command when a following train is approaching. [H-2, H-5]	(UCA-12) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-13) Control Room Operator provides an emergency brake command too late after abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	(UCA-14) Control Room Operator stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]
Controller: Train Operation Management System				
Acceleration Command	(UCA-26) Train Operation Management System does not provide an acceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(UCA-27) Train Operation Management System provides an acceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5]	(UCA-31) Train Operation Management System provides an acceleration command too early before the train completely passes a speed restriction zone. [H-1, H-2, H-5]	(UCA-32) Train Operation Management System applied an acceleration command too long after the train reached the target speed. [H-1, H-2, H-5]

Control Action	Type 1: Not Providing Causes Hazard	Type 2: Providing Causes Hazard	Type 3: Too early, too late, out of order	Type 4: Stopped too soon, applied too long
		(UCA-28) Train Operation Management System provides an acceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5] (UCA-29) Train Operation Management System provides an acceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5] (UCA-30) Train Operation Management System provides an acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]		
Controller: Drive Control System				
Target Current Command	(UCA-62) Drive Control System does not provide a	(UCA-63) Drive Control System provides a target current command	(UCA-64) Drive Control System provides a target current	(UCA-65) Drive Control System stopped a target current

Control Action	Type 1: Not Providing Causes Hazard	Type 2: Providing Causes Hazard	Type 3: Too early, too late, out of order	Type 4: Stopped too soon, applied too long
	target current command when the running speed does not keep the target speed. [H-1, H-2, H-5]	when personnel are entering the guideway for emergency maintenance. [H-5]	command too early before the calculation of the current value and phase is complete. [H-1, H-2, H-5]	command too soon before the train's speed reached the target speed. [H-1, H-2, H-5]
Controller: Safety Control System				
Door Close Enable	(UCA-75) Safety Control System does not provide a door close enable when the door-close condition[4] is met. [H-4, H-5]	(UCA-76) Safety Control System provides a door close enable when the door-close condition[4] is not met. [H-4] (UCA-77) Safety Control System provides a door close enable when passenger evacuation is necessary. [H-3]	(UCA-78) Safety Control System provides a door close enable too early before confirming whether the door-close condition[4] is met. [H-4]	(UCA-79) Safety Control System applied a door close enable too long after the door-close condition[4] was no longer met. [H-4]
Controller: Onboard Train Control System				
Door Actuation	(UCA-93) Onboard Train Control System does not provide a door actuation when receiving a door open/close enable. [H-3, H-4] (UCA-94) Onboard Train Control System does not	(UCA-95) Onboard Train Control System provides a door actuation when passenger boarding or alighting is still in progress. [H-3, H-4] (UCA-96) Onboard Train Control System provides a door	(UCA-97) Onboard Train Control System provides a door actuation too early before receiving a door open/close enable. [H-3, H-4]	(UCA-98) Onboard Train Control System applied a door actuation too long after a passenger was caught in the doors. [H-3, H-4]

Control Action	Type 1: Not Providing Causes Hazard	Type 2: Providing Causes Hazard	Type 3: Too early, too late, out of order	Type 4: Stopped too soon, applied too long
	provide a door actuation when a passenger is caught in the door. [H-4]	actuation when the train is still in motion. [H-4]		

Note.

[1] An external disturbance includes fire, earthquake, terrorism, obstacles, damage to facilities, intruders, and blackout.

[2] Abnormal behavior includes vibration, noise, and odor.

[4] The door-close condition is when passenger boarding/alighting is completed, and nothing is caught in the door.

Safety Constraints

Safety constraints that prevent UCA can be easily identified using safety constraint templates corresponding to the UCA types shown in Table 5.

Table 5. Safety Constraint Template

UCA	Safety Constraint
Type 1: <Controller> does not provide <control action> when <context>	Type 1: <Controller> shall provide <control action> when <context>
Type 2: <Controller> provides <control action> when <context>	Type 2: <Controller> should not provide <control action> when <context>
Type 3: <Controller> provides <control action> too later after <context>	Type 3: <Controller> shall provide <control action> within TBD seconds after <context>
Type 4: <Controller> stops providing <control action> too soon before <context>	Type 4: <Controller> should not stop providing <control action> before <context>

Table 6 shows a subset of the safety constraints for each UCA identified in this analysis. For the complete list of safety constraints, see Appendix A.3.

Table 6. Samples of the Safety Constraints for the "Without Conductor" Model

UCA	Safety Constraint
(UCA-9) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-9) Control Room Operator shall provide an emergency brake command when an external disturbance[1] occurs. [UCA-9]
(UCA-12) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-12) Control Room Operator shall provide an emergency brake command within TBD seconds after an external disturbance[1] occurs. [UCA-12]
(UCA-30) Train Operation Management System provides an acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]	(SC-30) Train Operation Management System should not provide an acceleration command when the train is operating within a speed restriction zone. [UCA-30]
(UCA-63) Drive Control System provides a target current command when personnel are entering the guideway for emergency maintenance. [H-5]	(SC-63) Drive Control System should not provide a target current command when personnel are entering the guideway for emergency maintenance. [UCA-63]
(UCA-79) Safety Control System applied a door close enable too long after the door-close condition was no longer met. [H-4]	(SC-79) Safety Control System shall stop providing a door close enable after the door-close condition is no longer met. [UCA-79]
(UCA-98) Onboard Train Control System applied a door actuation too long after a passenger was caught in the doors. [H-3, H-4]	(SC-98) Onboard Train Control System shall stop providing a door actuation after a passenger was caught in the doors. [UCA-98]

4.1.4 Identify Loss Scenarios

High-level Scenario Generation

When generating hazard scenarios, we first create high-level scenarios following the new formal approach proposed by Thomas [22]. Thomas's approach enables the comprehensive, structured generation of scenarios by classifying them into the following four categories. This allows us to avoid scenario generation that relies on the analyst's intuition or whims, and makes it easy to prove that scenarios are generated without overlooking any critical points.

Class 1: The controller issues a UCA despite receiving correct feedback

Class 2: The controller issues a UCA because of receiving incorrect or inappropriate feedback

Class 3: The controller issues an appropriate control action, but it becomes a UCA for some reason while being transmitted to the controlled process

Class 4: The controller issues an appropriate control action, but the receiving control process behaves like a UCA for some reason

Table 7 shows the templates for generating high-level scenarios for the four classes [22].

Table 7. High-Level Scenario Archetype Table

	UCA Type 1: Not providing	UCA Type 2: Providing	UCA Type 3: Too early/too late, out of order	UCA Type 4: Stopped too soon/applied too long
Scenario Class 1: Unsafe Controller Behavior	<controller> does not provide <command> when <context> AND <controller> received feedback that indicates <context>	<controller> provides <command> when <context> AND <controller> received feedback that indicates <context>	<controller> provides <command> too early/late before/after <context> AND <controller> received feedback that indicates <context> on time/in order	<controller> stops/continues providing <command> too soon/long before/after <context> AND <controller> received feedback that indicates <context> on time
Scenario Class 2: Unsafe Feedback Path	Feedback received by <controller> does not adequately indicate <context> AND <context> is true	Feedback received by <controller> does not adequately indicate <context> AND <context> is true	Feedback received by <controller> does not adequately indicate <context> (too early/late) AND <context> is true	Feedback received by <controller> does not adequately indicate <context> (inappropriate duration) AND <context> is true
Scenario Class 3: Unsafe Control Path	<controller> does provide <command> when <context> AND <command> is not received by <controlled process> when <context>	<controller> does not provide <command> when <context> AND <controlled process> receives <command> when <context>	<controller> does not provide <command> <context> (not too early/late) AND <command> is received by <controlled process> <context> (too early/late)	<controller> provides <command> with appropriate duration AND <command> is received by <controlled process> with <context>

				(inappropriate duration)
Scenario Class 4: Unsafe Controlled Process	<command> is received by <controlled process> when <context> AND <controlled process> does not respond by <…>	<command> is not received by <controlled process> when <context> AND <controlled process> responds by <…>	<command> is not received by <controlled process> <context> (not too early/late) AND <controlled process> responds by <…> (too early/late)	<command> is received by <controlled process> with appropriate duration AND <controlled process> does not respond to <…> with <context> (inappropriate duration)

Using these templates, this study generates the following high-level UCA scenarios. A set of UCAs was selected to demonstrate that STPA can generate hazard scenarios for any controller by identifying at least one UCA for each. Furthermore, the contexts incorporated—such as external disturbances (e.g., fire or obstacles), evacuation guidance, and emergency maintenance—align with the conditions of past major railway accidents, thereby enabling a more practical and realistic analysis.

UCA Type 1: Not providing causes hazard

(UCA-9) Control Room Operator does not provide an emergency brake command when an external disturbance occurs. [H-2, H-3, H-5]				
	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-9)	Control Room Operator does not provide an emergency brake command when an external disturbance occurs. AND	Feedback received by the Control Room Operator does not adequately indicate that an external disturbance occurred. AND	Control Room Operator provides an emergency brake command when an external disturbance occurs. AND The emergency brake command is	The emergency brake command is received by the Train Operation Management System when an external disturbance occurs. AND

	Control Room Operator received feedback that indicates that an external disturbance occurred.	An external disturbance is true.	not received by the Train Operation Management System when an external disturbance occurs.	Train Operation Management System does not respond to the emergency brake command.

UCA Type 2: Providing causes hazard

(UCA-30) Train Operation Management System provides an acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]				
	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 2: Providing causes hazard (UCA-30)	Train Operation Management System provides an acceleration command when the train is operating within a speed restriction zone. AND Train Operation Management System received feedback that indicates the train is operating within a speed restriction zone.	Feedback received by the Train Operation Management System does not adequately indicate that the train is operating within a speed restriction zone. AND The fact that the train is operating within a speed restriction zone is true.	Train Operation Management System does not provide an acceleration command when the train is operating within a speed restriction zone. AND Drive Control System received an acceleration command when the train is operating within a speed restriction zone.	An acceleration command is not received by the Drive Control System when the train is operating within a speed restriction zone. AND Drive Control System responds to an acceleration command.

(UCA-63) Drive Control System provides a target current command when personnel are entering the guideway for emergency maintenance. [H-5]				
	Scenario Class 1:	Scenario Class 2:	Scenario Class 3:	Scenario Class 4:

	Unsafe Controller Behavior	Unsafe Feedback Path	Unsafe Control Path	Unsafe Controlled Process Behavior
UCA Type 2: Providing causes hazard (UCA-63)	Drive Control System provides a target current command when personnel are entering the guideway for emergency maintenance. AND Drive Control System received feedback that indicates personnel are entering the guideway for emergency maintenance.	Feedback received by the Drive Control System does not adequately indicate that personnel are entering the guideway for emergency maintenance. AND The fact that personnel are entering the guideway for emergency maintenance is true.	Drive Control System does not provide a target current command when personnel are entering the guideway for emergency maintenance. AND Propulsion Coils received a target current command when personnel are entering the guideway for emergency maintenance.	A target current command is not received by Propulsion Coils when personnel are entering the guideway for emergency maintenance. AND Propulsion Coils respond to a target current command.

UCA Type 3: Providing too early, too late, or out of order causes hazard

(UCA-12) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5]				
	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 3: Too early, too late, out of order causes hazard	Control Room Operator provides an emergency brake command too late after an external disturbance occurs. AND	Feedback received by Control Room Operator does not adequately indicate that an external disturbance occurs too late. AND	Control Room Operator does not provide an emergency brake command not too late. AND An emergency brake command is	An emergency brake command is not received by Train Operation Management System not too late. AND

(UCA-12)	Control Room Operator received feedback that indicates an external disturbance occurs on time.	The fact that an external disturbance occurs is true.	received by Train Operation Management System too late.	Train Operation Management System responds to an emergency brake command too late.

UCA Type 4: Stopped too soon, applied too long causes hazard

(UCA-79) Safety Control System applied a door-close enable too long after the door-close condition was no longer met. [H-4]				
	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 4: Stopped too soon, applied too long causes hazard (UCA-79)	Safety Control System continues providing a door close enable too long after the door-close condition is no longer met. AND Safety Control System received feedback that indicates the door-close condition was no longer met on time.	Feedback received by Safety Control System does not indicate that the door-close condition was no longer met. AND The fact that the door-close condition was no longer met is true.	Safety Control System provides a door close enable for an appropriate duration. AND A door close enable is received by Onboard Train Control System with an inappropriate duration.	A door close enable is received by Onboard Train Control System with an appropriate duration. AND Onboard Train Control System does not respond to a door close enable with an appropriate duration.

(UCA-98) Onboard Train Control System applied a door actuation too long after a passenger was caught in the doors. [H-3, H-4]				
	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 4: Stopped too soon, applied too long causes hazard (UCA-98)	Onboard Train Control System continues providing a door actuation too long after a passenger is caught in the door. AND Onboard Train Control System received feedback indicating that a passenger was caught in the door on time.	Feedback received by Onboard Train Control System does not adequately indicate that a passenger is caught in the door. AND The fact that a passenger is caught in the door is true.	Onboard Train Control System provides a door actuation when a passenger is caught in the door for an appropriate duration. AND A door actuation is received by Train Vehicle for an inappropriate duration.	A door actuation is received by Train Vehicle with an appropriate duration. AND Train Vehicle does not respond to a door actuation within an appropriate duration.

Refined Scenario Generation

After identifying the UCA and high-level scenarios in the previous section, the next step is to develop detailed scenarios. For each high-level scenario, we ask questions such as "Why does the control system behave this way?" and "Why might the process behave as if that UCA had been issued?" and examine them in detail. This detailed investigation examines the scope of responsibility, control algorithms, process models, feedback paths, and operating modes, considering both failure-causing and non-failure-causing factors.

This section presents 8 refined scenarios. In generating these scenarios, the focus is not on hazard scenarios caused by component failures, but rather on non-failure scenarios in which hazards arise from interactions between components, even when the individual components are not failing. Furthermore, hazard scenarios range from design changes that eliminate them to changes that rely on component attention, such as adding signage or protocols.

UCA Type 1: Not providing causes hazard

UCA-9	Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. [H-2, H-3, H-5]
High-Level Scenario Class 1	Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. AND

	Control Room Operator received feedback that indicates that an external disturbance (fire) occurred.
Refined Scenario	The control room operator intentionally withholds braking to prevent the train from stopping in a tunnel, prioritizing mitigating smoke-related suffocation risks over the immediate fire hazard. However, the fire is spreading rapidly, so the passengers should be evacuated as soon as possible.
Recommendations	(R-1: Fire and Train Position Trade-off Evaluation) Implement a context-aware algorithm that evaluates the trade-off between fire/smoke and train position, such as in a tunnel, at a station, or outside. This algorithm enables operators to make contextual decisions and minimize fire-related damage.
	(R-2: Introducing Smoke Exhaust System) Install a system that automatically vents smoke when a fire is detected.
	(R-3: Vehicles made of non-combustible materials) Make vehicle interiors, seats, wiring, etc., with extremely high flame-retardant properties or non-combustible materials.
	(R-4: Introduction of Automatic Emergency Brake) In the event of a fire, the system automatically calculates the optimal stopping point based on the fire's severity and the train's current location, then brings the train to a stop.
	(R-5: Conducting Fire Response Drills) Conduct regular live-vehicle drills to ensure the control room operator can respond appropriately to any situation that may arise during a fire.

UCA Type 2: Providing causes hazard

UCA-30	Train Operation Management System provides acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]
High-Level Scenario Class 2	Feedback received by the Train Operation Management System does not adequately indicate that the train is operating within a speed restriction zone. AND It is true that the train is operating within a speed restriction zone.

Refined Scenario	While stationary at the station, the calibration of the initial position introduced a position offset of 10 meters in the direction of travel. As a result, the Train Operation Management System determines that the train has passed the speed limit zone even though the train is still in the zone and issues an acceleration command to return to normal operating speed.
Recommendations	(R-6: Logical Safety Margin for Speed Limit Zone): Incorporate a logical safety margin when defining the release point for temporary speed restrictions to mitigate the risks associated with position offsets. Specifically, the cancellation point of a speed limit zone shall be set at a predefined distance forward (downstream) of the actual geographic boundary.
	(R-7: Power Supply Limitation for Propulsion Coils) By setting an upper limit on the power supply to the propulsion coils, the system physically prevents the train from exceeding the temporary speed limit.
	(R-8: Emergency Braking in Case of Temporary Speed Exceedance) If the temporary speed limit is exceeded, the Safety Control System automatically activates the emergency brakes.
	(R-9: Abnormal Acceleration Detection) When abnormal acceleration is detected, a warning is issued to the control room operator.

UCA-63	Drive Control System provides a target current command when personnel enter the guideway for emergency maintenance. [H-5]
High-Level Scenario Class 1	Drive Control System provides a target current command when personnel enter the guideway for emergency maintenance. AND Drive Control System received feedback indicating that an emergency maintenance is required.
Refined Scenario	A lack of coil continuity in the SC Maglev can cause a sudden loss of levitation and propulsion, posing a hazard (derailment). To ensure operational safety, the Drive Control System performs periodic health checks via weak current injection. Although the operator issues a wide power-off command for emergency maintenance, the automatic continuity-check logic does not turn off. Consequently, the system

	provides a current reference even while personnel are present in the guideway.
Recommendations	(R-10: Maintenance Entry Interlock by Short-Circuit Grounding): Establish a safety interlock between the guideway access control and the Drive Control System to physically enforce a short-circuit grounding state before granting entry to personnel.
	(R-11: Health Check Using Ultra-Low Voltage) Perform coil health checks at ultra-low voltage, posing no risk to humans.
	(R-12: Introduction of Maintenance Mode) Modify the basic software design so that the health check logic cannot be activated while in maintenance mode.
	(R-13: Introduction of Warning Lights Inside the Guideway) Activate flashing lights and buzzers inside the guideway where current is flowing to warn workers.
	(R-14: Establishment of Guideway Entry Protocols) Establish protocols to confirm that the system is in a non-pressurized state before entering the guideway

UCA Type 3: Providing too early, too late, or out of order causes hazard

UCA-12	Control Room Operator provides an emergency brake command too late after an external disturbance (obstacle) occurs. [H-2, H-3, H-5]
High-Level Scenario Class 1	Control Room Operator provides an emergency brake command too late after an external disturbance (obstacle) occurs. AND Control Room Operator received feedback indicating that an external disturbance (obstacle) occurred on time.
Refined Scenario	The operator dismissed an initial obstacle alert within a tunnel, driven by a *belief* that tunnels are sealed, debris-free environments. This cognitive bias led to the prioritization of routine tasks over safety verification. Visual confirmation of concrete spalling via CCTV occurred only after a secondary, higher-priority alert, by which point the emergency braking was initiated too late to prevent breaching the safety braking margin.

Recommendations	(R-15: Immediate Suspension Protocols for Alert Responses): Establish operational protocols that mandate the immediate suspension of all ongoing tasks upon receipt of an alert, prioritizing situational assessment and the formulation of response measures.
	(R-16: Fully Enclosed Guideway) Design a fully enclosed guideway structure that physically prevents obstacles from entering.
	(R-17: Integrated Visualized Feedback regarding Obstacles) Provide immediate, visual feedback on the status of obstacles to the operator, going beyond mere warnings.
	(R-18: System-Level Interlock for Emergency Focus): Implement a system-level interlock that restricts access to non-essential functions when a high-priority alert is triggered, thereby compelling the operator to focus exclusively on the emergency.
	(R-19: Automatic Emergency Brake Upon Obstacle Detection): Implement automatic emergency brake for all trains by the Safety Control System immediately upon obstacle detection.

UCA Type 4: Stopped too soon, applied too long causes hazard

UCA-79	Safety Control System applied a door-close enable too long after the door-close condition was no longer met. [H-4]
High-Level Scenario Class 3	Safety Control System provides a door close enable for an appropriate duration. AND A door close enable is received by the Onboard Train Control System with an inappropriate duration.
Refined Scenario	The Safety Control System was located remotely and used a dedicated line to communicate with the Onboard Train Control System. However, due to the dedicated line's vulnerability, unauthorized access occurred, resulting in tampering with commands from the Safety Control System. Consequently, a door-close enable signal was continuously transmitted to the Onboard Train Control System even though the door-close conditions were not met.

Recommendations	(R-20: Encryption and Authentication Protocols) By applying encryption and authentication to the data itself, the system automatically discards any tampered data.
	(R-21: Enhanced Monitoring of Unauthorized Access) Implement logic that triggers an emergency stop of the train when a communication interruption or abnormal communication (e.g., repeated transmission of the same data) is detected.
	(R-22: Validation of Received Data by Onboard Train Control System) The Onboard Train Control System also verifies whether door-closing conditions are met; if not, it revokes permission to close the doors.
	(R-23: Implementation of Unauthorized Access Alerts) When unauthorized access is detected, a warning is sent to the control room operator.
	(R-24: Conducting Regular Penetration Tests) Regular penetration tests are conducted to verify that there are no vulnerabilities in the communication pathways.

UCA-98	Onboard Train Control System applied a door actuation too long after a passenger was caught in the doors. [H-3, H-4]
High-Level Scenario Class 1	Onboard Train Control System continues a door actuation (close) too long after a passenger is caught in the doors. AND Onboard Train Control System received feedback that indicates a passenger was caught in the doors on time.
Refined Scenario	Despite a physical obstruction in the doorway, the control system continued issuing door-closure commands because the automatic timeout function was activated. This feature, designed to prevent schedule disruptions from irregular boarding in unmanned railway operations, effectively overrode the obstruction sensors once the dwell-time threshold was reached.

Recommendations	(R-25: Safety-First Door Closure and Departure Logic): Never continue the door close command under any circumstances when something is caught in the doors, regardless of the train's delay status.
	(R-26: Eliminate the Automatic Timeout Function): Remove the automatic door closing function based on time. The risk of closing doors on passengers outweighs the operational stability. Door closure must always depend on safety verification, never solely on a timer.
	(R-27: Maximum Duration for Door Closing) Implement a function that automatically reopens the doors if they cannot close within a specified time limit.
	(R-28: Implementation of a Pinch Warning System) Alert station staff when an object is detected caught in the doors.
	(R-29: Pre-departure visual inspection protocol) Establish a protocol requiring station staff to visually confirm safety before departure.

4.2 Application of STPA to “With Conductor” Model

In this section, we perform an STPA analysis of the “with conductor” model, which adds a conductor to the control structure of the “without conductor” model.

4.2.1 Define the Purpose of the Analysis

The objectives of the analysis, such as the definition of loss, system-level hazards, and system-level safety constraints, are the same as those for the “without conductor” model. This is to ensure that the conditions are consistent when comparing the two models.

The Losses

- **L-1**: Injury or death to humans
- **L-2**: Physical Damage to the vehicle, guideway, or other equipment
- **L-3**: Loss of the transportation mission (Transport passengers to their destination)

System-Level Hazards

- **H-1:** The SC Maglev is in a state of overspeed. [L-1, L-2, L-3]
- **H-2:** Two or more SC Maglev trains exist in the same block section (state of not maintaining a safe margin from other trains). [L-1, L-2, L-3]
- **H-3:** The SC Maglev traps passengers, leaving no evacuation route. [L-1, L-2, L-3]
- **H-4:** The SC Maglev is not being stopped during passenger boarding or alighting. [L-1, L-3]
- **H-5**: The SC Maglev is colliding with an obstacle, the guideway, or another train [L-1, L-2, L-3]
- **H-6:** The SC Maglev significantly delays. [L-3]

System-Level Safety Constraints

- **SC-1:** The SC Maglev must be controlled in accordance with the run curve information. [H-1, H-2, H-5]
- **SC-2:** Only one SC Maglev must exist in a block section at a time. [H-2, H-3]
- **SC-3:** The SC Maglev must ensure an evacuation route is available. [H-3]
- **SC-4:** The SC Maglev must be stopped during passenger boarding and alighting. [H-4]
- **SC-5:** The SC Maglev must avoid any collision with an obstacle, the guideway, or another train. [H-5]
- **SC-6:** The SC Maglev must operate on time. [H-6]

4.2.2 Model the Control Structure

Control Structure for the "With Conductor" Model

The next step is to model the system's hierarchical control structure. Figure 15 shows the control structure of the "with conductor" model. As you can see, the "with conductor" model is derived from the "without conductor" model by adding a conductor to the control structure. The conductor is a component that interacts with both the Control Room Operator and the Onboard Train Control System. An enlarged version is included in Appendix B.1.

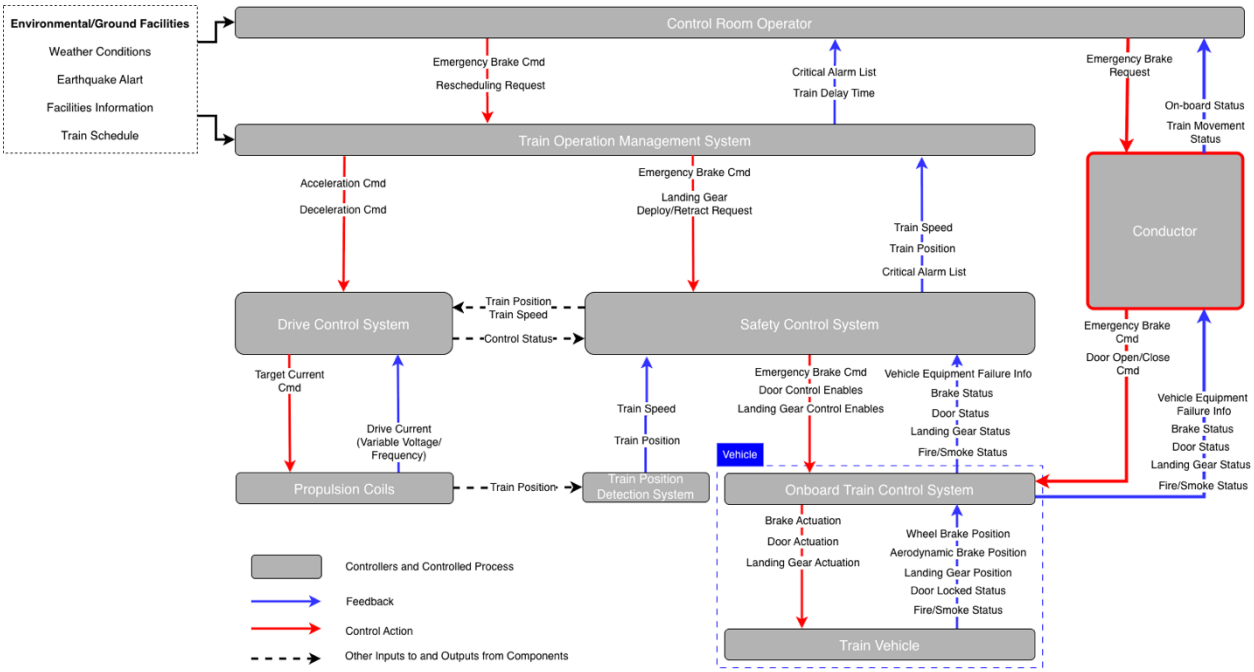


Figure 15. Control Structure for the "With Conductor" Model

Responsibilities, Control Actions, Process Model, and Feedback

This section provides detailed descriptions of the responsibilities, control actions, process model, and feedback defined in Table 8. The conductor collaborates with the control room operator to maintain safe operation. Upon receiving an emergency brake request from the control room operator, the conductor promptly initiates emergency braking procedures. In addition, the conductor is responsible for opening and closing the doors when the train stops at stations and during emergency evacuations. Regarding feedback, the conductor also reports on-board conditions and the status of train movement to the control room operator. To accurately grasp cabin conditions and running status, the conductor can receive feedback from the Onboard Train Control System on major failure flags, brake status, door status, landing gear status, and fire/smoke detection.

Table 8. Each Controller's Responsibilities, Control Action, Process Model, and Feedback/Other Input (the "With Conductor" Model)

Controller	Responsibility	Control Action	Process Models	Feedback &Other Inputs
Control Room Operator	Prevent the escalation of losses when external disturbances (e.g., earthquakes or fires) occur. Ensure the safe evacuation of passengers. Minimize train delays and ensure the prompt restoration of the schedule. Maximize the operational efficiency of rolling stock and crew.	Emergency brake command Reschedule request	External disturbances occur. The train is delayed The schedule is disturbed.	Critical Alarm List Train Delay Time On-board Status Train Movement Status Weather Condition Earthquake Alert Facilities Information Train Schedule
Conductor	Prevent the escalation of losses when external disturbances (e.g., earthquakes or fires) occur. Prevent the escalation of losses when abnormal behavior within the vehicle (e.g., abnormal vibration, noise, or odors) occurs. Ensure the safe evacuation of passengers. Provide opportunities for passengers to board and alight.	Emergency brake command Door open/close command	Abnormal behavior in the vehicle occurs. Passengers need evacuation. The train stops at the correct location. Something is caught in the doors.	Vehicle Equipment Failure Info Brake Status Door Status Landing Gear Status Fire Status

Controller	Responsibility	Control Action	Process Models	Feedback &Other Inputs
	Ensure that boarding and alighting are fully complete and that no objects are caught in the doors.			
Train Operation Management System	Maintain the train's target speed. Ensure that the train operates according to schedule. Maintain vehicle support and levitation in accordance with the train's speed. Ensure that commands from the Control Room Operator are transmitted to the Safety Control System.	Acceleration command Deceleration command Door open request Landing gear deploy/retract request	The train speed exceeds/falls below the target speed. The train speed exceeds/falls below the threshold. The train stops at the correct location. The control room operator's input has been received.	Train Speed Train Position Critical Alarm List Inputs from the Control Room Operator Weather Condition Earthquake Alert Facilities Information Train Schedule
Drive Control System	Maintain the target current flowing through the coils required to achieve the train's target speed.	Target current command	The drive current does not correspond to the target current.	Inputs from the Train Operation Management System (Acceleration and deceleration) The Drive Current

Controller	Responsibility	Control Action	Process Models	Feedback &Other Inputs
Safety Control System	Prohibit the train from exceeding the safe allowable speed limit. Prohibit door opening while the train is in motion or at an incorrect location. Prohibit door closing while passengers are boarding or alighting. Prohibit wheel retraction during low-speed travel. Prevent wheel extension while the train is in an overspeed condition.	Emergency brake command Door open/close enable Landing gear deploy/retract enable	The train exceeds the safe allowable speed limit. The train is still in motion or stops at an incorrect location. Passengers boarding and alighting continue. The train's speed exceeds the levitation threshold.	Train Speed Train Position Vehicle Equipment Failure Info Brake Status Door Status Landing Gear Status Fire Status
Onboard Train Control System	Ensure vehicle deceleration. Ensure that boarding and alighting are fully complete and that no objects are caught in the doors. Ensure that the doors remain fully open during boarding and alighting. Ensure that the doors remain fully closed during travel. Ensure vehicle support during low-speed operation.	Brake actuation Door actuation Landing gear actuation	The train needs deceleration. Something is caught in the doors. The doors open/close. The landing gears deploy/retract.	Wheel Brake Position Aerodynamic Brake Position Landing Gear Position Door Locked Status Fire/Smoke Status

Controller	Responsibility	Control Action	Process Models	Feedback &Other Inputs
	Ensure vehicle levitation during high-speed operation.			

Detailed Control Actions

This section provides detailed descriptions of the control actions defined in Figure 15. Note that if a control action is identical to one defined in the "without conductor" model, the label 'Identical' is appended to the end of the control action. On the other hand, the label 'New' is appended to the control action newly added in the "with conductor" model. These labels make it clear which control actions were added in the "with conductor" model. The definition format for these control actions is specified as follows:

- Control Action
  - Controller → Lower-level Controller/Controlled processes
  - Definition

Control Room Operator Controls

- Emergency Brake Command [Identical]
  - Control Room Operator → Train Operation Management System
  - In an emergency or when necessary, activate the target vehicle's emergency brakes remotely.

- Reschedule Request [Identical]
  - Control Room Operator → Train Operation Management System
  - When train delays occur, trains are rescheduled to facilitate recovery and ensure operational safety.
- Emergency Brake Request [New]
  - Control Room Operator → Conductor
  - For some reason, the emergency brake is not implemented. The control room operator requests that the conductor initiate the emergency brake.

Conductor Controls

- Emergency Brake Command [New]
  - Conductor → Onboard Train Control System
  - Upon receiving an emergency brake request from the operator, the conductor promptly initiates the emergency brake. Additionally, if the conductor detects an

external disturbance or abnormal behavior, the conductor initiates the emergency brake without waiting for the operator's instruction.

- Door Open/Close Command [New]
  - Conductor → Onboard Train Control System
  - When the train stops at the station, the conductor opens and closes the door to let passengers board and alight. Moreover, when something is caught in the door, the conductor manually opens and closes the door.

Train Operation Management System Controls

- Acceleration/Deceleration Command [Identical]
  - Train Operation Management System → Drive Control System
  - Instruct the train to accelerate or decelerate according to the run curve information.

- Emergency Brake Command [Identical]
  - Train Operation Management System → Safety Control System
  - The emergency brake command, once received from the Operator, is relayed to the Safety Control System.

- Landing Gear Deploy/Retract Request [Identical]
  - Train Operation Management System → Safety Control System
  - When the train's velocity falls to 75 miles per hour, a request to deploy the wheels is issued. Conversely, when the velocity exceeds the threshold, a request to retract the wheels is issued.

Drive Control System Controls

- Target Current Command [Identical]
  - Drive Control System → Propulsion Coils
  - Calculate the optimal coil current amplitude and frequency required to regulate propulsion and ensure strict compliance in accordance with the run curve information, and apply this current to coils.

Safety Control System Controls

- Emergency Brake Command [Identical]
  - Safety Control System → Onboard Train Control System
  - Upon detecting that a train is traveling more than the safety-allowable speed or receiving an emergency brake command, issue an emergency brake command to the affected train.

- Door Control Enables [Identical]
  - Safety Control System → Onboard Train Control System

- Upon receipt of a Door Open/Close Request, verify whether the vehicle has reached a complete stop and is accurately located at the current position, and allow door control.

- Landing Gear Control Enables [Identical]
  - Safety Control System → Onboard Train Control System
  - Upon receipt of a Landing Gear Deploy/Retract Request, evaluate the validity of the request based on the train's real-time velocity, and allow landing gear control.

Onboard Train Control System Controls

- Brake Actuation [Identical]
  - Onboard Train Control System → Train vehicle
  - Upon receiving an emergency brake command, initiate the wheel-disc brakes and the aerodynamic brakes.

- Door Actuation [Identical]
  - Onboard Train Control System → Train vehicle
  - Upon receipt of a door control enable, open or close the passenger doors.

- Landing Gear Actuation [Identical]
  - Onboard Train Control System → Train vehicle
  - Upon receipt of a landing gear enable, deploy or retract the wheel assembly.

4.2.3 Identify Unsafe Control Actions

Unsafe Control Actions

In this section, we identify UCAs in the "with conductor" model. As with the "without conductor" model, to comprehensively evaluate the model, we identify UCAs for each controller, focusing on states during train operation and station stops. As a result of the analysis, 108 UCAs were identified. Table 9 shows a sample of the identified UCAs. All UCAs are listed in Appendix B.2.

Table 9. Samples of the Identified UCAs in the "With Conductor" Model.

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Controller: Control Room Operator				

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Emergency Brake Command	(UCA-111) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(UCA-112) Control Room Operator provides an emergency brake command when a following train is approaching. [H-2, H-5]	(UCA-113) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	(UCA-114) Control Room Operator stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]
Controller: Conductor				
Emergency Brake Command	(UCA-119) Conductor does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-120) Conductor does not provide an emergency brake command when abnormal behavior[2] occurs. [H-2, H-3, H-5]	(UCA-121) Conductor provides an emergency brake command when a fire is detected and the train is located inside a long tunnel. [H-3] (UCA-122) Conductor provides an emergency brake command when a following train is approaching. [H-2, H-5]	(UCA-123) Conductor provides an emergency brake too late after an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-124) Conductor provides an emergency brake command too late after abnormal behavior[2] occurs. [H-2, H-3, H-5]	(UCA-125) Conductor stopped an emergency brake command too soon before the train completely stopped. [H-5]
Door Open Command	(UCA-126) Conductor does not provide a door open command when passenger	(UCA-129) Conductor provides a door open command when the train is in motion. [H-4, H-5]	(UCA-132) Conductor provides a door open command too early before the train	(UCA-135) Conductor applied a door open command too long after the evacuation had been

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	evacuation is required. [H-3] (UCA-127) Conductor does not provide a door open command when a passenger is caught in the door. [H-4] (UCA-128) Conductor does not provide a door open command when the train arrives at the station. [H-6]	(UCA-130) Conductor provides a door open command when the train is not at the appropriate boarding/alighting position. [H-3, H-4] (UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	completely stops. [H-4] (UCA-133) Conductor provides a door open command too early before the train position is suitable for passenger evacuation. [H-3, H-5] (UCA-134) Conductor provides a door open command too early before the oncoming train protections have been completed. [H-3, H-5]	completed. [H-5] (UCA-136) Conductor applied a door open command too long after the departure time had passed. [H-6]
Door Close Command	(UCA-137) Conductor does not provide a door close command when the departure time arrives. [H-2, H-5] (UCA-138) Conductor does not provide a door close command when the evacuation has been completed. [H-6]	(UCA-139) Conductor provides a door close command when passengers are boarding or alighting. [H-4] (UCA-140) Conductor provides a door close command when passenger evacuation is required. [H-3]	(UCA-141) Conductor provides a door close command too late after the train starts moving. [H-4, H-5] (UCA-142) Conductor provides a door close command too late after the train can resume operation. [H-6]	(UCA-143) Conductor applied a door close command too long after a passenger was caught in the doors. [H-3, H-4]

Safety Constraints

Table 10 shows a subset of the safety constraints for each UCA identified in this analysis. For the complete list of safety constraints, see Appendix B.3.

Table 10. Samples of the Safety Constraints for the "Without Conductor" Model

UCA	Safety Constraint
(UCA-111) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-111) Control Room Operator shall provide an emergency brake command when an external disturbance[1] occurs. [UCA-111]
(UCA-124) Conductor provides an emergency brake command too late after abnormal behavior[2] occurs. [H-2, H-3, H-5]	(SC-124) Conductor shall provide an emergency brake command within TBD seconds after abnormal behavior[2] occurs. [UCA-124]
(UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	(SC-131) Conductor should not provide a door open command when a strong magnetic field is generated along the guideway. [UCA-131]
(UCA-143) Conductor applied a door close command too long after a passenger was caught in the doors. [H-3, H-4]	(SC-143) Conductor shall stop providing a door close command after a passenger was caught in the doors. [UCA-143]

4.2.4 Identify Loss Scenarios

In this section, we will generate hazard scenarios. In this study, we will focus on generating hazard scenarios involving the newly added conductor and the control room operator, who is closely associated with the conductor. This approach not only allows us to generate new scenarios that cannot be observed in the "without conductor" model but also enables us to analyze the types of hazards that humans may create in highly automated high-speed rail systems.

High-level Scenario

While the "without conductor" model generated high-level scenarios in accordance with the latest STPA analysis workflow and then refined them, the "with conductor" model omits generating high-level scenarios and proceeds directly to generating specific refined scenarios from the outset.

Refined Scenario

UCA Type 1: Not providing causes hazard

UCA-111	Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. [H-2, H-3, H-5]
High-Level Scenario Class 1	Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. AND Control Room Operator received feedback indicating that an external disturbance (fire) had occurred.
Refined Scenario	The control room operator received a system alert indicating a fire onboard. However, because no verbal report was received from the conductor, the control room operator concluded that the alert was a false alarm and consequently did not initiate an emergency brake command. The conductor was preoccupied with firefighting and passenger evacuation, unable to communicate with the operator.
Recommendations	(R-30: Comprehensive Feedback on Fire Conditions): Integrate multi-modal feedback, such as cabin temperature, smoke fill level, and cabin camera footage, rather than just feedback on the presence or absence of fire, allowing operators to comprehensively assess the fire situation.
	(R-31: Vehicles made of non-combustible materials) Make vehicle interiors, seats, wiring, etc., with extremely high flame-retardant properties or non-combustible materials. (Same as R-2)
	(R-32: Introduction of Automatic Emergency Brake) In the event of a fire, the system automatically calculates the optimal stopping point based on the fire's severity and the train's current location, then brings the train to a stop. (Same as R-4)
	(R-33: Installation of Firewalls) Install firewalls and fire-retardant structures in each vehicle to minimize fire damage.
	(R-34: Response Protocol Independent on Verbal Report): Establish a protocol for the operator to initiate or defer emergency braking based on a comprehensive assessment of multi-modal feedback, independent on conductor's reports.

UCA Type 2: Providing causes hazard

UCA-131	Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]
High-Level Scenario Class 2	Feedback received by the conductor does not adequately indicate that a strong magnetic field is generated along the guideway. AND It is true that the strong magnetic field is generated along the guideway.
Refined Scenario	To ensure passenger safety, the conductor opens the door to initiate an evacuation in the event of an onboard fire. Simultaneously, the operator has maintained the power to move the train out of the tunnel, aiming to prevent the fire from spreading further. Consequently, passengers are exposed to hazardous magnetic fields on the guideway because the conductor is unaware that the guideway remains energized due to inadequate feedback.
Recommendations	(R-35: Mandatory Door Lock Under Strong Guideway Magnetic Field) Interlock the door so that it cannot be opened while a strong magnetic field is present on the guideway, regardless of the conductor's manual operation.
	(R-36: Installation of Dedicated Access Lifts and Evacuation Corridors) Install evacuation corridors that are physically separated from the magnetic field area, along with dedicated access lifts connecting the vehicles to these corridors, to prevent passengers from physically entering the magnetic field area.
	(R-37: Establishment of Emergency Door Opening Procedures) Establish operational procedures requiring the conductor and the control room operator to mutually confirm that pressurization of the propulsion coils has been stopped before opening the doors.
	(R-38: Feedback regarding Magnetic Field on the Guideway) Provide clear visual indicators to notify the conductor of the magnetic field outside the car.

UCA Type 3: Providing too early, too late, or out of order causes hazard

UCA-124	Conductor provides an emergency brake command too late after abnormal behavior (sound) occurs. [H-2, H-3, H-5]
High-Level Scenario Class 1	Conductor provides an emergency brake too late after abnormal behavior (sound) occurs. AND Conductor received feedback indicating that abnormal behavior (sound) occurs on time.
Refined Scenario	The conductor detected an abnormal sound but hesitated to issue an emergency brake command because the noise level did not clearly indicate that an immediate stop was required. Additionally, the "blame culture" regarding schedule delays discouraged the conductor from taking proactive action. As a result, the conductor postponed their decision and contacted the operator for instructions. However, the sound was a precursor to the car's body cracking. The resulting time lag led to a catastrophic hazard.
Recommendations	(R-39: Protocol for Emergency Brakes upon Abnormal Sound) Establish a strict criterion for the immediate activation of emergency brakes upon the detection of abnormal sound.
	(R-40: Automatic Emergency Brakes via Integrated Acoustic Sensing) Integrate acoustic sensors into critical vehicle components, such as superconducting magnets, bogies, and doors, to automatically trigger emergency brakes when abnormal sound levels are detected.
	(R-41: Elimination of Cracks Through One-Piece Molding) Remove the source of cracks by eliminating seams in the vehicle body through one-piece molding.
	(R-42: Introduction of Damage-Tolerant Design) Assuming cracks will occur, this design maximizes the time before they reach a level that poses a hazard.
	(R-43: Setting Thresholds for Abnormal Sound) Set volume thresholds for abnormal sounds and install alarms for the control room operator and the conductor when the sound exceeds the thresholds.
	(R-44: Just Culture Cultivation for Proactive Safety) Cultivate an organizational culture that does not penalize "false alarms". Instead,

	redesign the personnel evaluation system to incentivize and reward proactive safety-oriented action.

UCA Type 4: Stopped too soon, applied too long causes hazard

UCA-143	Conductor applied a door close command too long after a passenger was caught in the doors. [H-3, H-4]
High-Level Scenario Class 2	Feedback received by the conductor does not adequately indicate that a passenger was caught in the door for an inappropriate duration. AND It is true that a passenger is caught in the door.
Refined Scenario	When passengers are caught in the door, the design allows not only automatic door opening by the Onboard Train Control System but also manual door opening by the conductor. This redundancy ensures human intervention is possible when the system cannot automatically control the doors. Unfortunately, the camera detection system was designed to make decisions based on historical data, even when cameras monitoring the door area could not process the latest images due to noise. As a result, both the Onboard Train Control System and the conductor received feedback indicating “no obstruction”. Even with redundancy in place, if decisions are made based on the same feedback, that redundancy does not contribute to safety if the feedback is inappropriate.
Recommendations	(R-45: Torque Limitation and Use of Cushioning Material) The torque is set to a level that a person can push back with their own strength, and cushioning rubber is used at the door's tip to reduce physical damage.
	(R-46: Maximum Duration for Door Closing) Implement a function that automatically reopens the doors if they cannot close within a specified time limit. (Same as R-27)
	(R-47: Multi-Modal Obstruction Detection) Implement an integration of non-contact sensors, such as optical light curtains or capacitive proximity sensors. This approach ensures sensor diversity, enabling the system to detect obstacles even if one sensor is not functioning well.

	(R-48: Response Protocol for “Unknown” Camera Feedback) Return “unknown” feedback if the latest camera image cannot be used. Upon receiving this feedback, the conductor conducts an on-site verification.

Chapter 5: Discussion

In this chapter, we compare the STPA analysis results for the “without conductor” and “with conductor” models and discuss the advantages and challenges of each. We also present recommendations to help eliminate and control the identified hazard scenarios.

First, in Section 5.1, we examine the changes in each controller's responsibilities resulting from the introduction of the conductor. Section 5.2 compares the number of identified UCAs by controller and extracts “model-specific UCAs” that are not shared between the two models. Section 5.3 qualitatively analyzes the reasons for increases or decreases in the number of UCAs and the causes of model-specific UCAs, clarifying the structural background behind their non-shared nature. In Section 5.4, based on the insights from this series of analyses, we comprehensively examine the system characteristics and operational challenges of both models. Finally, in Section 5.5, we identify the priority of the derived recommendations and present guidelines for decision-making in safety design.

5.1 The Change in the Responsibilities of Each Controller

In this section, we examine how the introduction of the conductor has altered each controller's responsibilities during the transition from the “without conductor” to the “with conductor” model. Table 11 compares the responsibilities of each controller in both models.

With the addition of the conductor, responsibility for “Prevent the escalation of losses when abnormal behavior within the vehicle (e.g., abnormal vibration, noise, or odors) occurs.” was fully transferred from the control room operator to the conductor (shown in red in the table). Furthermore, the responsibilities for “Prevent the escalation of losses when external disturbance (e.g., earthquakes or fires) occurs,” and “Ensure the safe evacuation of passengers” were shared between the control room operator and the conductor (shown in blue in the table).

Furthermore, the responsibility for “Provide opportunities for passengers to board and alight” was transferred from the Train Operation Management System to the conductor. Consequently, the responsibility for “Ensure that boarding and alighting are fully complete and that no objects are caught in the doors” is now shared between the Onboard Train Control System and the conductor.

On the other hand, responsibilities related to the control of trains and infrastructure—such as running control, current control through the coils, control of onboard equipment, and safety checks for these controls—remain unchanged even with the introduction of the conductor. Therefore, the responsibilities of the Drive Control System, Safety Control System, and Onboard Train Control System have not changed.

These changes in responsibility reflect a design philosophy aimed at ensuring safety by having "people" on-site directly assess and respond to urgent situations—rather than relying solely on remote control or automated systems—in response to risks arising from interactions with passengers during emergencies or station stops. This can be seen as an effort to carry forward the safety philosophy of "people safeguarding safety," which has been upheld by conventional railway systems, even within the highly automated SC Maglev system.

Table 11. Comparison of Controller Responsibilities in Both Models: Responsibilities in red indicate those fully transferred to the conductor, while those in blue indicate responsibilities shared with the conductor.

Controller	"Without Conductor" Model	"With Conductor" Model
Conductor		Prevent the escalation of losses when external disturbance (e.g., earthquakes or fires) occurs. Prevent the escalation of losses when abnormal behavior within the vehicle (e.g., abnormal vibration, noise, or odors) occurs. Ensure the safe evacuation of passengers. Provide opportunities for passengers to board and alight. Ensure that boarding and alighting are fully complete and that no objects are caught in the doors.
Control Room Operator	Prevent the escalation of losses when external disturbance (e.g., earthquakes or fires) occurs. Prevent the escalation of losses when abnormal behavior within the vehicle (e.g., abnormal vibration, noise, or odors) occurs. Ensure the safe evacuation of passengers. Minimize train delays and ensure the prompt restoration of the schedule.	Prevent the escalation of losses when external disturbance (e.g., earthquakes or fires) occurs. Ensure the safe evacuation of passengers. Minimize train delays and ensure the prompt restoration of the schedule. Maximize the operational efficiency of rolling stock and crew.

	Maximize the operational efficiency of rolling stock and crew.	
Train Operation Management System	Maintain the train's target speed. Ensure that the train operates according to schedule. Provide opportunities for passengers to board and alight. Maintain vehicle support and levitation appropriate to the train's speed. Ensure that commands from the Control Room Operator are transmitted to the Safety Control System.	Maintain the train's target speed. Ensure that the train operates according to schedule. Maintain vehicle support and levitation appropriate to the train's speed. Ensure that commands from the Control Room Operator are transmitted to the Safety Control System.
Drive Control System	Calculate the target current. Maintain the target current flowing through the coils required to achieve the train's target speed.	Calculate the target current. Maintain the target current flowing through the coils required to achieve the train's target speed.
Safety Control System	Prohibit the train from exceeding the safe allowable speed limit. Prohibit door opening while the train is in motion or at an incorrect location. Prohibit door closing while passengers are boarding or alighting. Prohibit wheel retraction during low-speed travel. Prevent wheel extension while the train is in an overspeed condition. Ensure that an emergency brake command from the Control Room Operator is transmitted to the Safety Control System.	Prohibit the train from exceeding the safe allowable speed limit. Prohibit door opening while the train is in motion or at an incorrect location. Prohibit door closing while passengers are boarding or alighting. Prohibit wheel retraction during low-speed travel. Prevent wheel extension while the train is in an overspeed condition. Ensure that an emergency brake command from the Control Room Operator is transmitted to the Safety Control System.

Onboard Train Control System	Ensure vehicle deceleration. Ensure that boarding and alighting are fully complete and that no objects are caught in the doors. Ensure that the doors remain fully open during boarding and alighting. Ensure that the doors remain fully closed during travel. Ensure vehicle support during low-speed operation. Ensure vehicle levitation during high-speed operation.	Ensure vehicle deceleration. Ensure that boarding and alighting are fully complete and that no objects are caught in the doors. Ensure that the doors remain fully open during boarding and alighting. Ensure that the doors remain fully closed during travel. Ensure vehicle support during low-speed operation. Ensure vehicle levitation during high-speed operation.

5.2 Changes in the Number of Identified UCAs by Controller and Extract "Model-Specific UCAs."

In this section, to analyze the changes in UCAs resulting from the introduction of the conductor, we compile UCAs by controller and examine the characteristics of the "model-specific UCAs".

Table 12. Number of each component UCA identified for each model. The numbers in parentheses indicate the number of UCAs common to both models.

Controller	"Without Conductor" Model	"With Conductor" Model
Control Room Operator	25 (12)	16 (12)
Conductor		25
Train Operation Management System	36 (26)	26 (26)
Drive Control System	4	4
Safety Control System	22	22

Onboard Train Control System	15	15
Total	102	108

As shown in Table 12, adding the conductor reduced the number of UCAs for the control room operator from 25 to 16. Of these, 12 were common to both models, 13 were specific to the "without conductor" model, and 4 were specific to the "with conductor" model. Similarly, the number of UCAs in the Train Operation Management System also decreased from 36 to 26, but both models shared all 26; consequently, 10 unique UCAs were identified only for the "without conductor" model. On the other hand, 25 new UCAs were identified for the conductor.

Furthermore, the fact that these quantitative changes are directly attributable to the "transfer and sharing of responsibilities" discussed in Section 5.1 is supported by the observation that no changes whatsoever were seen in the number or content of UCAs for other controllers where there were no changes in the scope of responsibility. For example, regarding the Drive Control System, Safety Control System, and Onboard Train Control System, there were no differences in their responsibilities before and after the introduction of the conductor. Consequently, the content of the identified UCAs was completely consistent between the two models, and no increase or decrease in their quantity was observed. This fact strongly suggests that the increases, decreases, and transformations in the UCAs identified in this analysis are not merely due to modeling errors or random sampling, but accurately reflect the reorganization of the control structure resulting from the introduction of the conductor as a new controller.

Here, particular attention must be paid to the specific UCAs that arose from the transfer of responsibility. As Table 13 clearly shows, the majority of UCAs recorded as specific are those in which "only the entity responsible has changed" due to the transfer of responsibility—that is, "Transferred UCAs". Since the nature of the control actions leading to hazards is essentially the same in both models, these must be distinguished from the "Model-Specific UCAs" in the strictest sense.

Specifically, of the 23 specific UCAs in the "without conductor" model, 19 are transferred UCAs that share their essence in both models. At the same time, only 4 are true model-specific UCAs that occur exclusively in that model. Similarly, of the 29 specific UCAs in the "with conductor" model, 22 were transferred UCAs, while only 7 were true model-specific UCAs that arose specifically due to the conductor's intervention. These results suggest that introducing the conductor does not fundamentally alter the system's hazards but primarily reorganizes the control structure, specifically regarding "who bears existing responsibilities."

Table 13. A list classifying UCAs not shared by both models as either "Transferred UCA" or "Model-Specific UCA."

Model	Controller	UCA	Transferred/Model-Specific UCA
Without Conductor	Control Room Operator	(UCA-10) Control Room Operator does not provide an emergency brake command when abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	Transferred
		(UCA-13) Control Room Operator provides an emergency brake command too late after abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	Transferred
		(UCA-15) Control Room Operator does not provide an evacuation door open request when passenger evacuation is required. [H-3]	Transferred
		(UCA-16) Control Room Operator provides an evacuation door open request when the train is in motion. [H-3, H-5]	Transferred
		(UCA-17) Control Room Operator provides an evacuation door open request when passengers are crowded together near the doors and causing chaos. [H-3, H-5]	Model-Specific
		(UCA-18) Control Room Operator provides an evacuation door open request too early before the train position is suitable for passenger evacuation. [H-3, H-5]	Transferred
		(UCA-19) Control Room Operator applied an evacuation door open request too long after the evacuation had been completed. [H-5]	Transferred
		(UCA-20) Control Room Operator does not provide an evacuation door close request when the evacuation is completed. [H-6]	Transferred
		(UCA-21) Control Room Operator provides an evacuation door close request when some passengers are still inside the vehicle. [H-3]	Model-Specific

Model	Controller	UCA	Transferred/Model-Specific UCA
		(UCA-22) Control Room Operator provides an evacuation door close request when passengers are evacuating. [H-3]	Model-Specific
		(UCA-23) Control Room Operator provides an evacuation door close request when the conductor is still outside the vehicle for evacuation. [H-4, H-5]	Model-Specific
		(UCA-24) Control Room Operator provides an evacuation door close request too late after the train can resume operation. [H-6]	Transferred
		(UCA-25) Control Room Operator applied an evacuation door close request too long after a passenger was caught in the door. [H-3, H-4]	Transferred
	Train Operation Management System	(UCA-43) Train Operation Management System does not provide a door open request when the train arrives at the station. [H-6]	Transferred
		(UCA-44) Train Operation Management System provides a door open request when the train is in motion. [H-4, H-5]	Transferred
		(UCA-45) Train Operation Management System provides a door open request when the train is not at the appropriate boarding/alighting position. [H-3, H-4]	Transferred
		(UCA-46) Train Operation Management System provides a door open request too early before the train completely stops. [H-4]	Transferred
		(UCA-47) Train Operation Management System applied a door open request too long after the departure time had passed. [H-6]	Transferred
		(UCA-48) Train Operation Management System does not provide a door close request when the departure time arrives. [H-2, H-5]	Transferred

Model	Controller	UCA	Transferred/Model-Specific UCA
		(UCA-49) Train Operation Management System provides a door close request when passengers are boarding or alighting. [H-4]	Transferred
		(UCA-50) Train Operation Management System provides a door close request when passenger evacuation is required. [H-3]	Transferred
		(UCA-51) Train Operation Management System provides a door close request too late after the train starts moving. [H-4, H-5]	Transferred
		(UCA-52) Train Operation Management System applied a door close request too long after a passenger was caught in the doors. [H-3, H-4]	Transferred
With Conductor	Control Room Operator	(UCA-115) Control Room Operator does not provide an emergency brake request to the Conductor when the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	Model-Specific
		(UCA-116) Control Room Operator provides an emergency brake request to the conductor instead of executing a direct remote activation when an emergency is occurring. [H-1, H-2, H-5]	Model-Specific
		(UCA-117) Control Room Operator provides an emergency brake request to the conductor too late after the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	Model-Specific
		(UCA-118) Control Room Operator stopped an emergency brake request to the conductor too soon before the conductor initiated a direct emergency brake. [H-1, H-2, H-5]	Model-Specific
	Conductor	(UCA-119) Conductor does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	Transferred

Model	Controller	UCA	Transferred/Model-Specific UCA
		(UCA-120) Conductor does not provide an emergency brake command when abnormal behavior[2] occurs. [H-2, H-3, H-5]	Transferred
		(UCA-121) Conductor provides an emergency brake command when a fire is detected and the train is located inside a long tunnel. [H-3]	Model-Specific
		(UCA-122) Conductor provides an emergency brake command when a following train is approaching. [H-2, H-5]	Transferred
		(UCA-123) Conductor provides an emergency brake too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	Transferred
		(UCA-124) Conductor provides an emergency brake command too late after abnormal behavior[2] occurs. [H-2, H-3, H-5]	Transferred
		(UCA-125) Conductor stopped an emergency brake command too soon before the train completely stopped. [H-5]	Transferred
		(UCA-126) Conductor does not provide a door open command when passenger evacuation is required. [H-3]	Transferred
		(UCA-127) Conductor does not provide a door open command when a passenger is caught in the door. [H-4]	Transferred
		(UCA-128) Conductor does not provide a door open command when the train arrives at the station. [H-6]	Transferred
		(UCA-129) Conductor provides a door open command when the train is in motion. [H-4, H-5]	Transferred
		(UCA-130) Conductor provides a door open command when the train is not at the	Transferred

Model	Controller	UCA	Transferred/Model-Specific UCA
		appropriate boarding/alighting position. [H-3, H-4]	
		(UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	Model-Specific
		(UCA-132) Conductor provides a door open command too early before the train completely stops. [H-4]	Transferred
		(UCA-133) Conductor provides a door open command too early before the train position is suitable for passenger evacuation. [H-3, H-5]	Transferred
		(UCA-134) Conductor provides a door open command too early before oncoming train protections have not been completed. [H-3, H-5]	Model-Specific
		(UCA-135) Conductor applied a door open command too long after the evacuation had been completed. [H-5]	Transferred
		(UCA-136) Conductor applied a door open command too long after the departure time had passed. [H-6]	Transferred
		(UCA-137) Conductor does not provide a door close command when the departure time arrives. [H-2, H-5]	Transferred
		(UCA-138) Conductor does not provide a door close command when the evacuation has been completed. [H-6]	Transferred
		(UCA-139) Conductor provides a door close command when passengers are boarding or alighting. [H-4]	Transferred
		(UCA-140) Conductor provides a door close command when passenger evacuation is required. [H-3]	Transferred

Model	Controller	UCA	Transferred/Model-Specific UCA
		(UCA-141) Conductor provides a door close command too late after the train starts moving. [H-4, H-5]	Transferred
		(UCA-142) Conductor provides a door close command too late after the train can resume operation. [H-6]	Transferred
		(UCA-143) Conductor applied a door close command too long after a passenger was caught in the doors. [H-3, H-4]	Transferred

5.3 Why the Model-Specific UCAs Occur in the Specific Model

This section focuses on the "Model-Specific UCAs" identified in the previous section. We examine the structural causal factors that explain why they occur only in specific model configurations, as shown in Table 14.

5.3.1 Limitations of Remote Control in the "Without Conductor" Model

All the "Model-Specific UCAs" identified in the "without conductor" model are concentrated within the context of "emergency passenger evacuation guidance." In this model, the control room operator bears full responsibility for evacuation guidance; however, this role is subject to physical and psychological constraints inherent to remote control.

First, the "control dilemma" faced by the control room operator is the primary causal factor of these model-specific UCAs. In urgent situations such as a fire, while a rapid start to evacuation is required, if hundreds of panicked passengers are rushing toward the doors, carelessly opening them risks causing serious secondary damage, such as a crowded collapse or passengers falling onto the tracks. For the control room operator located remotely, the means to influence on-site crowd psychology are extremely limited. This conflict between "speed" and "safety" distorts the control room operator's decision-making and induces UCAs.

Furthermore, the incompleteness of feedback poses a serious risk. Surveillance via onboard cameras inevitably has physical blind spots, and there are limits to confirming the complete evacuation of passengers remotely. Moreover, when doors are temporarily closed for minor adjustments to the stopping position, it is conceivable that the control room operator may neglect to recognize subtle changes in the on-site situation. These are typical examples of how insufficient feedback leads to the development of an inappropriate process model, resulting in UCA.

In the “with conductor” model, the conductor can directly defuse confusion and use their five senses to gain a detailed understanding of the evacuation situation; therefore, UCAs caused by remote control can be mitigated.

5.3.2 Side Effects of Redundancy and Risks of Isolation in the “With Conductor” Model

On the other hand, the “Model-Specific UCAs” identified in the “with conductor” model stem from the interaction between the control room operator and the conductor, as well as the asymmetry of information for the conductor.

The first factor is the “dilution of responsibility” that results from adding human redundancy to the system. In the case of the control room operator’s specific UCA, instances were observed in which the control room operator overestimated that the conductor would proactively handle emergency braking procedures, which the control room operator should have handled themselves. This demonstrates that the presence of a backup diminishes a sense of personal responsibility, leading to an inappropriate process model. Furthermore, in situations where responsibility is shared, a psychological bias to defer emergency decisions to others can delay actions necessary to ensure safety.

The second factor is the state of “information asymmetry”. In special environments, such as during high-speed operation or in long tunnels, the conductor, isolated inside the vehicle, finds it extremely difficult to accurately determine their current position or the external situation solely through their senses. Consequently, there is a risk that the conductor will perform unsafe control actions, such as opening doors at an unsafe time, based on a mistaken belief that they have “already reached a safe stopping position.”

Furthermore, “speculation” regarding the status of other controllers is also a significant factor. Unconfirmed expectations—such as the assumption that the control room operator has already completed power disconnection or safety measures—can trigger unsafe control actions by the conductor. This suggests that deficiencies in “coordination” between the control room operator and the conductor can create new hazards.

Table 14. Model-Specific UCAs for each model and the Main Causal Factor

Model	Controller	UCA	Main Causal Factor
Without Conductor	Control Room Operator	(UCA-17) Control Room Operator provides an evacuation door open request when passengers are crowded together near the doors and causing chaos. [H-3, H-5]	Remote Control

Model	Controller	UCA	Main Causal Factor
		(UCA-21) Control Room Operator provides an evacuation door close request when some passengers are still inside the vehicle. [H-3]	Remote Control
		(UCA-22) Control Room Operator provides an evacuation door close request when passengers are evacuating. [H-3]	Remote Control
		(UCA-23) Control Room Operator provides an evacuation door close request when the conductor is still outside the vehicle for evacuation. [H-4, H-5]	Remote Control
With Conductor	Control Room Operator	(UCA-115) Control Room Operator does not provide an emergency brake request to the Conductor when the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	Coordination
		(UCA-116) Control Room Operator provides an emergency brake request to the conductor instead of executing a direct remote activation when an emergency is occurring. [H-1, H-2, H-5]	Coordination
		(UCA-117) Control Room Operator provides an emergency brake request to the conductor too late after the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	Coordination
		(UCA-118) Control Room Operator stopped an emergency brake request to the conductor too soon before the conductor initiated a direct emergency brake. [H-1, H-2, H-5]	Coordination
		(UCA-121) Conductor provides an emergency brake command when a fire is detected and the train is located inside a long tunnel. [H-3]	Information Asymmetry Speculation
		(UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	Information Asymmetry

Model	Controller	UCA	Main Causal Factor
			Speculation
		(UCA-134) Conductor provides a door open command too early before oncoming train protections have not been completed. [H-3, H-5]	Information Asymmetry Speculation

5.4 Characteristics and Challenges of Each Model

Based on the quantitative and qualitative analyses presented in the preceding sections, this section summarizes the characteristics of both models within the SC Maglev system. From a systems engineering perspective, we examine the strengths and challenges of each model—factors that serve as key indicators for evaluating trade-offs when determining the system's design and requirements.

5.4.1 Without Conductor Model

As shown in Table 15, the primary advantage of the "without conductor" model is decision-making consistency, achieved through a simplified control structure.

In this model, the absence of a redundant controller—namely, the conductor—centralizes the responsibility for responding to external disturbances and abnormal behavior solely with the control room operator. Consequently, structural inconsistencies in judgment and coordination delays among multiple controllers are eliminated, enabling the control room operator to make rapid, consistent decisions. Furthermore, a key strength of this model is that all necessary feedback for decision-making is consolidated with the control room operator, thereby enabling decisions to be made based on a multifaceted assessment of the current situation.

Conversely, to manage all aspects of an emergency response remotely, the control room operator must solely process a massive volume of information transmitted from vehicles and trackside equipment, resulting in an extremely high cognitive workload. It presents significant technical challenges to fully detect subtle signs of anomalies, such as "unusual noises" or "strange odors," which are typically perceptible to the human senses. Because it is difficult to define specific digital thresholds for such qualitative information to enable automated detection, there is a risk that critical contextual details may be lost during the sensing process. Furthermore, being physically isolated from the actual scene and compelled to make critical decisions under extreme pressure—based solely on fragmented information received through a digital interface—can contribute to a distorted control room operator's process model of the situation.

Table 15. Advantages and Challenges of the "Without Conductor" Model

	Advantages	Challenges
Without conductor model	• Consistency in Decision-Making The operator can manage feedback in a centralized manner and make decisions. • Reduction of Human Error Prevention of miscommunication and operational errors between humans due to emergency disruptions. • Simple Control Structure Clear responsibility for emergency situations and reduction of development costs.	• Increased Cognitive Load The operator must make rapid decisions with enormous feedback. • Dependency on Sensors The operator does not receive clear feedback on abnormal behavior, such as vibration, sound, or odor, because the operator is remote and relies on sensors.

5.4.2 With Conductor Model

The "with conductor" model is grounded in a design philosophy aimed at enhancing the capacity to respond to emergencies—specifically those that automated systems and remote monitoring cannot fully cover—through the physical presence of "people" in the field. This aligns with the safety philosophy inherent in traditional railway systems: the principle that "humans safeguard safety." However, analytical results suggest that adding the conductor does not necessarily translate directly into an improvement in the system's intrinsic safety.

The primary advantage of this model lies in its utilization of the five senses on-site as shown in Table 16. By immediately perceiving—through their senses—subtle precursors to anomalies (such as unusual vibrations, noises, or odors) that are difficult to detect via remote monitoring, the conductor can take preventive control actions that forestall the manifestation of hazards or the escalation of losses. Furthermore, the conductor serves as a backup for the control room operator and automated control systems, providing a means for manual intervention in the event of communication failures or the loss of remote-control capabilities. This enhances both the system's availability and reliability.

Moreover, in the "without conductor" model, all operational control relies on remote commands from the control room or the systems. Consequently, security risks, such as unauthorized access or cyberattacks, are inevitable on the communication channels used to transmit commands. Since a complete disruption of the communication channels would result in

the loss of system functionality, it is extremely difficult to structurally eliminate vulnerabilities stemming from the communication network in this model. In contrast, in the “with conductor” model, the presence of a conductor enables physical intervention. Specifically, it is feasible to establish a dedicated control path physically isolated from external networks, allowing the conductor to directly operate physical control mechanisms such as door locks and brakes. Maintaining a “closed control system” with no external connections is a major advantage of the “with conductor” model from a security risk perspective.

Conversely, in highly automated, ultra-high-speed systems such as the SC Maglev, the conductor is isolated from the actual operating environment. In an environment where speeds exceed 300 miles per hour, visual detection of obstacles and precise location determination are impossible; consequently, the conductor is compelled to make decisions within a limited information space. Making judgments based solely on fragmentary on-site information—without a comprehensive understanding of the vehicle's or wayside equipment's operational status—can lead to UCAs rooted in erroneous assumptions. Furthermore, the overlap of responsibilities between the control room operator and the conductor fosters inappropriate mutual expectations—specifically, the assumption that "the other party must be handling this"—which delays decision-making during emergencies and leads to UCAs.

This model enhances redundancy by enabling the conductor to manually operate the train in the event of a failure in the remote-control system. However, it can be argued that information asymmetry, decision-making based on inferences and assumptions, and increased system complexity collectively compromise safety. As indicated by the quantitative analysis (Section 5.2), the number of newly induced UCAs (29 instances) exceeded the number of UCAs eliminated through the introduction of the conductor (23 instances). Moreover, many of the UCAs that appeared to have been eliminated were merely "Transferred UCAs", meaning the overall number of UCAs within the system has not necessarily decreased.

Table 16. Advantages and Challenges of the “With Conductor” Model

	Advantages	Challenges
With Conductor Model	• Ensuring Physical Redundancy Even in cases where a system fails or a communication network is blocked, the conductor can independently control emergency brakes and door open/close. • Five Senses On-Site	• Information Asymmetry The conductor is forced to make decisions with less information than the operator due to an isolated vehicle space and cognitive limitations led by ultra-high-speed running conditions. • Inappropriate Inference or Assumption

	The conductor can directly detect emergency signals on-site. • Cybersecurity Resilience By establishing a closed control loop with no external connections, the model mitigates security risks such as cyberattacks.	The conductor makes decisions based on subjective inferences or assumptions. • Ambiguous Responsibility The act of shifting responsibility back and forth between operators and conductors. • Complex Control Structure By ensuring the safety of manual operations by conductors, coordination becomes complex and poses a new risk.

5.5 Prioritization of Recommendations

Through this analysis, several valuable recommendations were developed to prevent hazards and losses. Ideally, all recommendations should be implemented within the system; however, due to constraints such as cost and development schedules, implementing every recommendation is difficult. Therefore, in this section, the recommendations for each model are categorized based on the prioritization of safety measures defined in MIL-STD-882E.

5.5.1 Overview of MIL-STD-882E

MIL-STD-882E (Standard Practice for System Safety) is a standard practice for system safety programs established by the U.S. Department of Defense [23]. This standard provides a systematic approach for identifying and classifying hazards and reducing their associated risks to an acceptable level throughout the entire system lifecycle—encompassing design, development, testing, operation, and disposal.

Within this system safety program, an "Order of Precedence" for safety measures is defined to serve as a guideline for mitigating risks effectively within the constraints of limited cost and schedule resources. The five priorities are below:

A. Eliminate hazards through design selection. Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether.

B. Reduce risk through design alteration. If adopting an alternative design change or material to eliminate the hazard is not feasible, consider design changes that reduce the severity and/or the probability of the mishap potential caused by the hazard(s).

C. Incorporate engineered features or devices. If mitigation of the risk through design alteration is not feasible, reduce the severity or the probability of the mishap potential caused by the hazard(s) using engineered features or devices. In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap.

D. Provide warning devices. If engineered features and devices are not feasible or do not adequately lower the severity or probability of the mishap potential caused by the hazard, include detection and warning systems to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.

E. Incorporate signage, procedures, training, and PPE. Where design alternatives, design changes, and engineered features and devices are not feasible and warning devices cannot adequately mitigate the severity or probability of the mishap potential caused by the hazard, incorporate signage, procedures, training, and PPE. Signage includes placards, labels, signs and other visual graphics. Procedures and training should include appropriate warnings and cautions. Procedures may prescribe the use of PPE. For hazards assigned Catastrophic or Critical mishap severity categories, the use of signage, procedures, training, and PPE as the only risk reduction method should be avoided.

This prioritization is based on the robustness of the countermeasures and their reliance on human factors; it is assumed that the higher a measure ranks in this hierarchy, the more effectively it can eliminate risk.

5.5.2 Prioritization of Recommendations for the "Without Conductor" Model

Table 17 shows the results of classifying the recommendations for the UCA of the "without conductor" model—derived through STPA as described in the previous section—according to the "Order of Precedence" of safety measures specified in MIL-STD-882E.

Table 17. Classifications of the recommendations for the "Without Conductor" Model according to the "Order of Precedence."

(UCA-9) Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. [H-2, H-3, H-5]	
High-Level Scenario Class 1	Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. AND Control Room Operator received feedback that indicates that an external disturbance (fire) occurred.

Order	Recommendation Title
A	R-3: Vehicles made of Non-Combustible Materials
B	R-2: Introducing Smoke Exhaust System
C	R-4: Introduction of Automatic Emergency Brake
D	R-1: Fire and Train Position Trade-off Evaluation
E	R-5: Conducting Fire Response Drills
(UCA-30) Train Operation Management System provides acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]	
High-Level Scenario Class 2	Feedback received by the Train Operation Management System does not adequately indicate that the train is operating within a speed restriction zone. AND It is true that the train is operating within a speed restriction zone.
Order	Recommendation Title
A	R-7: Power Supply Limitation for Propulsion Coils
B	R-6: Logical Safety Margin for Speed Limit Zone
C	R-8: Emergency Braking in Case of Temporary Speed Exceedance
D	R-9: Abnormal Acceleration Detection
(UCA-63) Drive Control System provides a target current command when personnel enter the guideway for emergency maintenance. [H-5]	
High-Level Scenario Class 1	Drive Control System provides a target current command when personnel enter the guideway for emergency maintenance. AND Drive Control System received feedback indicating that an emergency maintenance is required.
Order	Recommendation Title
B	R-12: Introduction of Maintenance Mode
C	R-10: Maintenance Entry Interlock by Short-Circuit Grounding

	R-11: Health Check Using Ultra-Low Voltage
D	R-13: Introduction of Warning Lights Inside the Guideway
E	R-14: Establishment of Guideway Entry Protocols
(UCA-12) Control Room Operator provides an emergency brake command too late after an external disturbance (obstacle) occurs. [H-2, H-3, H-5]	
High-Level Scenario Class 1	Control Room Operator provides an emergency brake command too late after an external disturbance (obstacle) occurs. AND Control Room Operator received feedback indicating that an external disturbance (obstacle) occurred on time.
Order	Recommendation Title
A	R-16: Fully Enclosed Guideway
C	R-18: System-Level Interlock for Emergency Focus R-19: Automatic Emergency Brake Upon Obstacle Detection
D	R-17: Integrated Visualized Feedback regarding Obstacles
E	R-15: Immediate Suspension Protocols for Alert Responses
(UCA-79) Safety Control System applied a door-close enable too long after the door-close condition was no longer met. [H-4]	
High-Level Scenario Class 3	Safety Control System provides a door close enable for an appropriate duration. AND A door close enable is received by the Onboard Train Control System with an inappropriate duration.
Order	Recommendation Title
B	R-20: Encryption and Authentication Protocols R-21: Enhanced Monitoring of Unauthorized Access
C	R-22: Validation of Received Data by Onboard Train Control System
D	R-23: Implementation of Unauthorized Access Alerts

E	R-24: Conducting Regular Penetration Tests
(UCA-98) Onboard Train Control System applied a door actuation too long after a passenger was caught in the doors. [H-3, H-4]	
High-Level Scenario Class 1	Onboard Train Control System continues a door actuation (close) too long after a passenger is caught in the doors. AND Onboard Train Control System received feedback that indicates a passenger was caught in the doors on time.
Order	Recommendation Title
A	R-26: Eliminate the Automatic Timeout Function
B	R-25: Safety-First Door Closure and Departure Logic
C	R-27: Maximum Duration for Door Closing
D	R-28: Implementation of a Pinch Warning System
E	R-29: Pre-departure visual inspection protocol

5.5.3 Prioritization of Recommendations for the "With Conductor" Model

Table 18 presents the classification results, based on MIL-STD-882E, for the STPA recommendations for each UCA derived from the "with conductor" model.

The total number of recommendations identified in this model's analysis is relatively limited compared to that of the "without conductor" model. This is because the analysis focused on the transformation of the control structure resulting from the introduction of the conductor, placing particular emphasis on the interfaces among the three parties involved: the control room operator, the Onboard Train Control System, and the conductor. Consequently, this disparity in quantity does not reflect the relative superiority or inferiority of the models themselves; rather, it reflects an analysis focused specifically on safety within the newly established control paths and feedback loops.

Table 18. Classifications of the recommendations for the "With Conductor" Model according to the "Order of Precedence."

(UCA-111) Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. [H-2, H-3, H-5]

High-Level Scenario Class 1	Control Room Operator does not provide an emergency brake command when an external disturbance (fire) occurs. AND Control Room Operator received feedback indicating that an external disturbance (fire) had occurred.
Order	Recommendation Title
A	R-31: Vehicles made of non-combustible materials (Same as R-2)
B	R-33: Installation of Firewalls
C	R-32: Introduction of Automatic Emergency Brake (Same as R-4)
D	R-30: Comprehensive Feedback on Fire Conditions
E	R-34: Response Protocol Independent on Verbal Report
(UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	
High-Level Scenario Class 2	Feedback received by the conductor does not adequately indicate that a strong magnetic field is generated along the guideway. AND It is true that the strong magnetic field is generated along the guideway.
Order	Recommendation Title
A	R-36: Installation of Dedicated Access Lifts and Evacuation Corridors
C	R-35: Mandatory Door Lock Under Strong Guideway Magnetic Field
D	R-38: Feedback regarding Magnetic Field on the Guideway
E	R-37: Establishment of Emergency Door Opening Procedures
(UCA-124) Conductor provides an emergency brake command too late after abnormal behavior (sound) occurs. [H-2, H-3, H-5]	
High-Level Scenario Class 1	Conductor provides an emergency brake too late after abnormal behavior (sound) occurs. AND

	Conductor received feedback indicating that abnormal behavior (sound) occurs on time.
Order	Recommendation Title
A	R-41: Elimination of Cracks Through One-Piece Molding
B	R-42: Introduction of Damage-Tolerant Design
C	R-40: Automatic Emergency Brakes via Integrated Acoustic Sensing
D	R-43: Setting Thresholds for Abnormal Sound
E	R-39: Protocol for Emergency Brakes upon Abnormal Sound R-44: Just Culture Cultivation for Proactive Safety
(UCA-143) Conductor applied a door close command too long after a passenger was caught in the doors. [H-3, H-4]	
High-Level Scenario Class 2	Feedback received by the conductor does not adequately indicate that a passenger was caught in the door for an inappropriate duration. AND It is true that a passenger is caught in the door.
Order	Recommendation Title
B	R-45: Torque Limitation and Use of Cushioning Material
C	R-46: Maximum Duration for Door Closing. (Same as R-27)
D	R-47: Multi-Modal Obstruction Detection
E	R-48: Response Protocol for “Unknown” Camera Feedback

Chapter 6: Conclusion

In this study, we applied STPA—a next-generation hazard analysis method—to the SC Maglev system, the world's fastest, highly automated ground transportation system, and conducted a comprehensive analysis of how differences in control structure, particularly the presence or absence of a conductor, affect the system's overall safety. In this chapter, we summarize the key findings and discuss the significance of this study and future research directions.

6.1 Key Findings

First, we demonstrated that STPA is an exceptionally robust hazard analysis method within today's increasingly complex transportation systems. Whereas FTA and FMEA—which have been the primary focus of conventional railway hazard analyses—have mainly focused on physical deficiencies such as hardware failures and component lifespans, STPA has successfully identified and comprehensively assessed non-failure scenarios attributable to software design flaws, human-system interactions, and organizational factors. For example, a scenario in which a control room operator fails to apply the emergency brake despite a fire breaking out in a train car can occur due to the control room operator's misperception or misjudgment, even if the fire detectors and brake systems are functioning properly. Such non-failure scenarios were overlooked by conventional hazard analysis methods, making it difficult to implement effective countermeasures; however, by applying STPA, we were able to identify them comprehensively. This demonstrated the effectiveness of evaluating the safety of the entire SC Maglev system—including not only physical components but also non-hardware elements such as humans and systems—during the early stages of development.

The core achievement of this study lies in identifying model-specific hazard factors associated with the introduction of a conductor through a safety trade-off analysis. The traditional safety philosophy in railways—the notion that "people ensure safety"—has relied on on-site personnel using their five senses to detect anomalies and respond flexibly. However, quantitative comparisons revealed that the "with conductor" model identified 108 UCAs, whereas the "without conductor" model identified 102. While the introduction of the conductor offers advantages such as on-site anomaly detection using the five senses and smoother evacuation guidance, it was revealed that in the SC Maglev system—which operates at ultra-high speeds exceeding 300 miles per hour and relies on advanced automated control—new risks may arise between the conductor, who is isolated inside the train, and the control room operator. These risks include information asymmetry, coordination failures, and diffusion of responsibility.

It is important to note here that the system's redundancy and safety must be evaluated separately. Adding a conductor to the control structure certainly improves redundancy during manual intervention in the event of communication failures and similar situations. However, as the quantitative analysis results indicate, adding a conductor simultaneously introduces new UCAs,

suggesting that the system's overall safety does not necessarily improve. The observation that increased redundancy may increase system complexity and introduce new vulnerabilities through inappropriate interactions between components is a critical issue not only for the SC Maglev system but also for the safety design of future autonomous driving systems.

Based on the above analysis, this study proposes a multi-layered safety design plan that complies with the priority levels specified in MIL-STD-882E. We have successfully proposed a wide range of measures, ranging from design changes that eliminate hazards and risks at their root cause to the integration of physical interlocks, rather than merely superficial measures such as modifying signs or protocols that rely on human subjective judgment or on-site intuition.

6.2 Future Work

First, expanding the scope of analysis and conducting a detailed deep dive into each control system. Since this study focused on comparing control structures based on the presence or absence of a conductor, the scope was primarily limited to the conductor, control room operator, and Onboard Train Control System. However, the safety of the SC Maglev system is fundamentally sustained by the sophisticated coordination among subsystems that manage high-level automated control, such as the Train Operation Management System, the Safety Control System, and the Drive Control System. Future work should involve applying a detailed STPA to these automated control subsystems to identify non-failure scenarios across the entire system in a more comprehensive and multi-layered manner.

Second, performing a multi-faceted verification of the feasibility and validity of the proposed recommendations. Although the recommendations in this study were logically derived to prevent hazards, their implementation requires careful evaluation of their consistency with existing system architectures, development costs, and the potential for new trade-offs arising from increased system complexity. Since the SC Maglev is a large-scale system characterized by complex interactions among diverse subsystems, it is essential to establish a process for refining these recommendations through collaboration with experts across technical domains, ultimately translating them into practical design requirements and operational protocols.

Appendices

Appendix A.1: Enlarged Control Structure for the “Without Conductor” Model

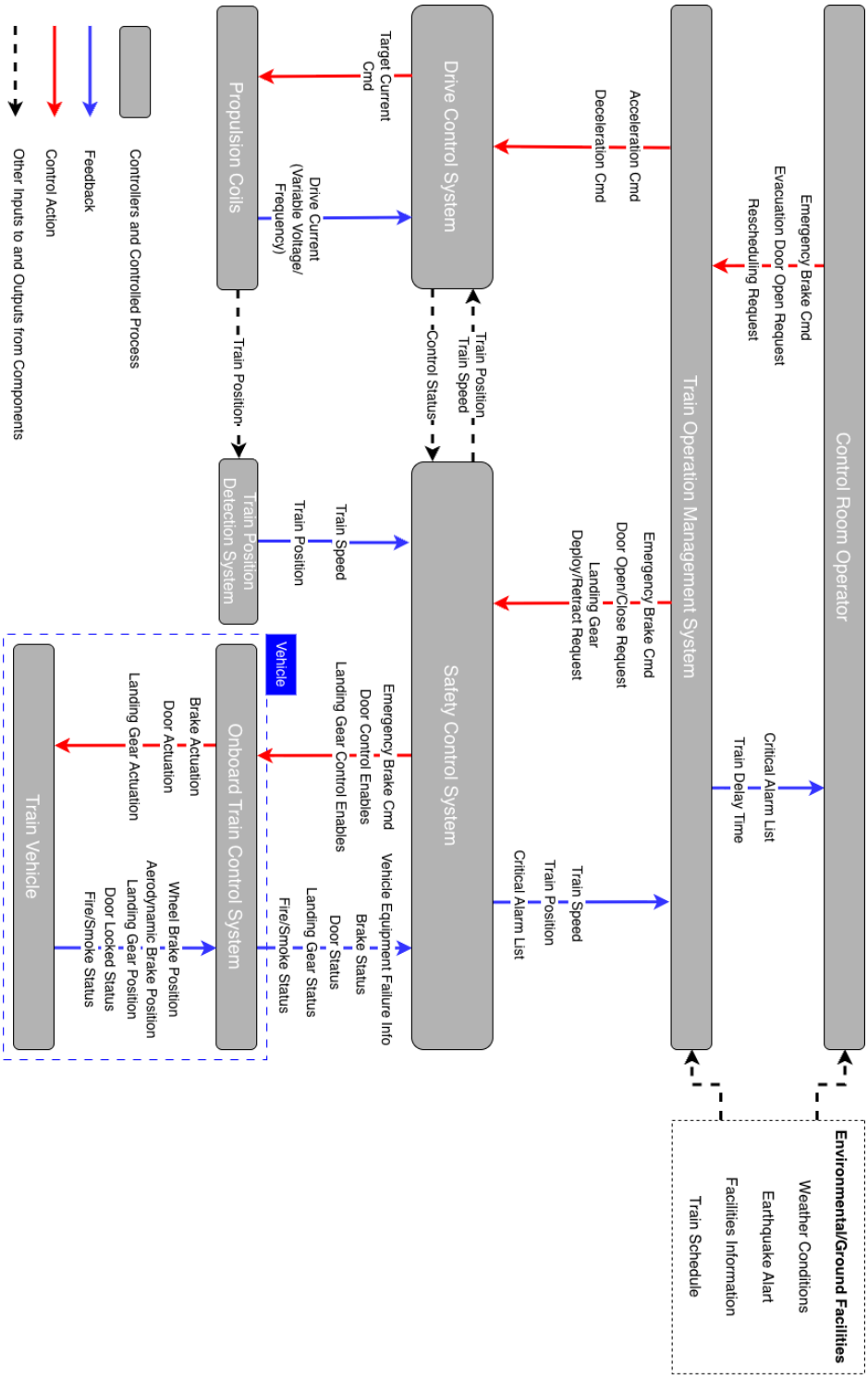


Figure 16. Enlarged Control Structure for the “Without Conductor” Model

Appendix A.2: All UCAs Identified in the "Without Conductor" Model

Table 19. All UCAs Identified in the "Without Conductor" Model

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Controller: Control Room Operator				
Reschedule Request	(UCA-1) Control Room Operator does not provide a reschedule request when a suddenly sick person requires an emergency stop at the next station. [H-3] (UCA-2) Control Room Operator does not provide a reschedule request when the arrival track at the next station must be changed. [H-2, H-5, H-6] (UCA-3) Control Room Operator does not provide a reschedule request when a temporary speed restriction setting is required. [H-1, H-2, H-5]	(UCA-4) Control Room Operator provides a reschedule request when the tracks are closed. [H-5, H-6] (UCA-5) Control Room Operator provides a reschedule request when maintenance work is being carried out. [H-5]	(UCA-6) Control Room Operator provides a reschedule request too early before the official request is finalized in the operation center. [H-1, H-2, H-3, H-4, H-5, H-6] (UCA-7) Control Room Operator provides a reschedule request too early before the route configuration is complete. [H-1, H-2, H-5]	(UCA-8) Control Room Operator stopped a reschedule request too soon before the requests were reflected in the train schedule. [H-1, H-2, H-3, H-4, H-5, H-6]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Emergency Brake Command	(UCA-9) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-10) Control Room Operator does not provide an emergency brake command when abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	(UCA-11) Control Room Operator provides an emergency brake command when a following train is approaching. [H-2, H-5]	(UCA-12) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-13) Control Room Operator provides an emergency brake command too late after abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	(UCA-14) Control Room Operator stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]
Evacuation Door Open Request	(UCA-15) Control Room Operator does not provide an evacuation door open request when passenger evacuation is required. [H-3]	(UCA-16) Control Room Operator provides an evacuation door open request when the train is in motion. [H-3, H-5] (UCA-17) Control Room Operator provides an evacuation door open request when passengers are crowded together near the doors and	(UCA-18) Control Room Operator provides an evacuation door open request too early before the train position is suitable for passenger evacuation. [H-3, H-5]	(UCA-19) Control Room Operator applied an evacuation door open request too long after the evacuation had been completed. [H-6]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
		causing chaos. [H-3, H-5]		
Evacuation Door Close Request	(UCA-20) Control Room Operator does not provide an evacuation door close request when the evacuation is completed. [H-6]	(UCA-21) Control Room Operator provides an evacuation door close request when some passengers are still inside the vehicle. [H-3] (UCA-22) Control Room Operator provides an evacuation door close request when passengers are evacuating. [H-3] (UCA-23) Control Room Operator provides an evacuation door close request when the conductor is still outside the vehicle for evacuation. [H-4, H-5]	(UCA-24) Control Room Operator provides an evacuation door close request too late after the train can resume operation. [H-6]	(UCA-25) Control Room Operator applied an evacuation door close request too long after a passenger was caught in the door. [H-3, H-4]
Controller: Train Operation Management System				
Acceleration Command	(UCA-26) Train Operation Management System does not provide an acceleration command when the distance to	(UCA-27) Train Operation Management System provides an acceleration command when the running speed exceeds the target	(UCA-31) Train Operation Management System provides an acceleration command too early before the train completely	(UCA-32) Train Operation Management System applied an acceleration command too long after the train reached the

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	the following train falls below the safe margin. [H-2, H-5]	speed on a run curve. [H-1, H-2, H-5] (UCA-28) Train Operation Management System provides an acceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5] (UCA-29) Train Operation Management System provides acceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5] (UCA-30) Train Operation Management System provides an acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]	passes a speed restriction zone. [H-1, H-2, H-5]	target speed. [H-1, H-2, H-5]
Deceleration Command	(UCA-33) Train Operation Management	(UCA-36) Train Operation Management	(UCA-37) Train Operation Management	(UCA-38) Train Operation Management

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	System does not provide a deceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5] (UCA-34) Train Operation Management System does not provide a deceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5] (UCA-35) Train Operation Management System does not provide a deceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5]	System provides a deceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	System provides a deceleration command too late after the train enters a speed restriction zone. [H-1, H-2, H-5]	System stopped a deceleration command too soon before the train reached the target speed. [H-1, H-2, H-5]
Emergency Brake Command	(UCA-39) Train Operation Management System does not provide an emergency	(UCA-40) Train Operation Management System provides an emergency brake command	(UCA-41) Train Operation Management System provides an emergency brake command	(UCA-42) Train Operation Management System stopped an emergency brake command

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	brake command when an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	when a following train is approaching. [H-5]	too late after an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	too soon before the train stopped completely. [H-1, H-2, H-3, H-5]
Door Open Request	(UCA-43) Train Operation Management System does not provide a door open request when the train arrives at the station. [H-6]	(UCA-44) Train Operation Management System provides a door open request when the train is in motion. [H-4, H-5] (UCA-45) Train Operation Management System provides a door open request when the train is not at the appropriate boarding/alighting position. [H-3, H-4]	(UCA-46) Train Operation Management System provides a door open request too early before the train completely stops. [H-4]	(UCA-47) Train Operation Management System applied a door open request too long after the departure time had passed. [H-6]
Door Close Request	(UCA-48) Train Operation Management System does not provide a door close request when the departure time arrives. [H-2, H-5]	(UCA-49) Train Operation Management System provides a door close request when passengers are boarding or alighting. [H-4] (UCA-50) Train Operation Management System provides a	(UCA-51) Train Operation Management System provides a door close request too late after the train starts moving. [H-4, H-5]	(UCA-52) Train Operation Management System applied a door close request too long after a passenger was caught in the doors. [H-3, H-4]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
		door close request when passenger evacuation is required. [H-3]		
Landing Gear Deploy Request	(UCA-53) Train Operation Management System does not provide a landing gear deploy request when the train enters the wheel running mode. [H-5]	(UCA-54) Train Operation Management System provides a landing gear deploy request when the train is in the levitation running mode. [H-2, H-5]	(UCA-55) Train Operation Management System provides a landing gear deploy request too late after the train's speed falls below 75 miles per hour (the threshold for the wheel running mode). [H-5]	(UCA-56) Train Operation Management System stopped a landing gear deploy request too soon before the landing gear was fully deployed. [H-5]
Landing Gear Retract Request	(UCA-57) Train Operation Management System does not provide a landing gear retract request when the train is in levitation running mode. [H-2, H-5]	(UCA-58) Train Operation Management System provides a landing gear retract request when the train is in wheel running mode. [H-5] (UCA-59) Train Operation Management System provides a landing gear retract request when the train stops at the station. [H-3, H-4, H-5]	(UCA-60) Train Operation Management System provides a landing gear retract request too late after the train's speed exceeds 75 miles per hour (the threshold for the levitation running mode). [H-5]	(UCA-61) Train Operation Management System stopped a landing gear retract request too soon before the landing gear was fully retracted. [H-5]
Controller: Drive Control System				

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Target Current Command	(UCA-62) Drive Control System does not provide a target current command when the running speed does not keep the target speed. [H-1, H-2, H-5]	(UCA-63) Drive Control System provides a target current command when personnel are entering the guideway for emergency maintenance. [H-5]	(UCA-64) Drive Control System provides a target current command too early before the calculation of the current value and phase is complete. [H-1, H-2, H-5]	(UCA-65) Drive Control System stopped a target current command too soon before the train's speed reached the target speed. [H-1, H-2, H-5]
Controller: Safety Control System				
Emergency Brake Command	(UCA-66) Safety Control System does not provide an emergency brake command when traveling above the safe allowable speed limit. [H-1, H-2, H-5] (UCA-67) Safety Control System does not provide an emergency brake command when an emergency brake command is initiated by Control Room Operator [H-1, H-2, H-3, H-5]	(UCA-68) Safety Control System provides an emergency brake command when a following train is approaching. [H-5]	(UCA-69) Safety Control System provides an emergency brake command too late after the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(UCA-70) Safety Control System stopped an emergency brake command too soon before the train completely stopped. [H-2, H-5]
Door Open Enable	(UCA-71) Safety Control	(UCA-72) Safety Control System	(UCA-73) Safety Control	(UCA-74) Safety Control

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	System does not provide a door open enable when the door-open condition[3] is met and passenger evacuation is necessary. [H-3]	provides a door open enable when the door-open condition[3] is not met. [H-4]	System provides a door open enable too early before confirming whether the door-open condition[3] is met. [H-4]	System applied a door open enable too long after the door-open condition[3] was no longer met. [H-4]
Door Close Enable	(UCA-75) Safety Control System does not provide a door close enable when the door-close condition[4] is met. [H-4, H-5]	(UCA-76) Safety Control System provides a door close enable when the door-close condition[4] is not met. [H-4] (UCA-77) Safety Control System provides a door close enable when passenger evacuation is necessary. [H-3]	(UCA-78) Safety Control System provides a door close enable too early before confirming whether the door-close condition[4] is met. [H-4]	(UCA-79) Safety Control System applied a door close enable too long after the door-close condition[4] was no longer met. [H-4]
Landing Gear Deploy Enable	(UCA-80) Safety Control System does not provide a landing gear deploy enable when the wheel-running condition[5] is met. [H-5]	(UCA-81) Safety Control System provides a landing gear deploy enable when the wheel-running condition[5] is not met. [H-5]	(UCA-82) Safety Control System provides a landing gear deploy enable too early before confirming whether the wheel-running condition[5] is met. [H-5]	(UCA-83) Safety Control System applied a landing gear deploy enable too long after the wheel-running condition[5] was no longer met. [H-5]
Landing Gear Retract Enable	(UCA-84) Safety Control System does	(UCA-85) Safety Control System provides a landing	(UCA-86) Safety Control System provides	(UCA-87) Safety Control System applied

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	not provide a landing gear retract enable when the levitation-running condition[6] is met. [H-2, H-5]	gear retract enable when the levitation-running condition[6] is not met. [H-5]	a landing gear retract enable too early before confirming whether the levitation-running condition[6] is met. [H-5]	a landing gear retract enable too long after the levitation-running condition[5] was no longer met. [H-5]
Controller: Onboard Train Control System				
Brake Actuation	(UCA-88) Onboard Train Control System does not provide a brake actuation when the regenerative brake is insufficient. [H-1, H-2, H-5] (UCA-89) Onboard Train Control System does not provide a brake actuation when an emergency brake command has been received. [H-1, H-2, H-5]	(UCA-90) Onboard Train Control System provides a brake actuation when the train is operating on an icy guideway. [H-1, H-2, H-5]	(UCA-91) Onboard Train Control System provides a brake actuation too late after an emergency brake command has been received. [H-1, H-2, H-5]	(UCA-92) Onboard Train Control System stopped a brake actuation too soon before the train completely stopped. [H-1, H-5]
Door Actuation	(UCA-93) Onboard Train Control System does not provide a door actuation when receiving a door open/close	(UCA-95) Onboard Train Control System provides a door actuation when passenger boarding or alighting is still in	(UCA-97) Onboard Train Control System provides a door actuation too early before receiving a door open/close	(UCA-98) Onboard Train Control System applied a door actuation too long after a passenger was caught in the

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	enable. [H-3, H-4] (UCA-94) Onboard Train Control System does not provide a door actuation when a passenger is caught in the door. [H-4]	progress. [H-3, H-4] (UCA-96) Onboard Train Control System provides a door actuation when the train is still in motion. [H-4]	enable. [H-3, H-4]	doors. [H-3, H-4]
Landing Gear Actuation	(UCA-99) Onboard Train Control System does not provide a landing gear actuation when receiving a landing gear deploy/retract enable. [H-5]	(UCA-100) Onboard Train Control System provides a landing gear actuation when the train's speed is not in the threshold range. [H-5]	(UCA-101) Onboard Train Control System provides a landing gear actuation too late after receiving a landing gear deploy/retract enable. [H-5]	(UCA-102) Onboard Train Control System stopped a landing gear actuation too soon before the landing gear touched the ground. [H-5]

Note.

[1] An external disturbance includes fire, earthquake, terrorism, obstacles, damage to facilities, intruders, and blackout.

[2] Abnormal behavior includes vibration, noise, and odor.

[3] The door-open condition is when the train completely stops and is at the appropriate position.

[4] The door-close condition is when passenger boarding/alighting is completed, and nothing is caught in the door.

[5] The wheel-running condition is when the train speed falls below 75 miles per hour.

[6] The levitation-running condition is when the train speed exceeds 75 miles per hour.

Appendix A.3: All Safety Constraints for the "Without Conductor" Model

Table 20. All Safety Constraints for the "Without Conductor" Model

UCA	Safety Constraint
(UCA-1) Control Room Operator does not provide a reschedule request when a suddenly sick person requires an emergency stop at the next station. [H-3]	(SC-1) Control Room Operator shall provide a reschedule request when a suddenly sick person requires an emergency stop at the next station. [UCA-1]
(UCA-2) Control Room Operator does not provide a reschedule request when the arrival track at the next station must be changed. [H-2, H-5, H-6]	(SC-2) Control Room Operator shall provide a reschedule request when the arrival track at the next station must be changed. [UCA-2]
(UCA-3) Control Room Operator does not provide a reschedule request when a temporary speed restriction setting is required. [H-1, H-2, H-5]	(SC-3) Control Room Operator shall provide a reschedule request when a temporary speed restriction setting is required. [UCA-3]
(UCA-4) Control Room Operator provides a reschedule request when the tracks are closed. [H-5, H-6]	(SC-4) Control Room Operator should not provide a reschedule request when the tracks are closed. [UCA-4]
(UCA-5) Control Room Operator provides a reschedule request when maintenance work is being carried out. [H-5]	(SC-5) Control Room Operator should not provide a reschedule request when maintenance work is being carried out. [UCA-5]
(UCA-6) Control Room Operator provides a reschedule request too early before the official request is finalized in the operation center. [H-1, H-2, H-3, H-4, H-5, H-6]	(SC-6) Control Room Operator shall provide a reschedule request within TBD seconds after the official request is finalized in the operation center. [UCA-6]
(UCA-7) Control Room Operator provides a reschedule request too early before the route configuration is complete. [H-1, H-2, H-5]	(SC-7) Control Room Operator shall provide a reschedule request within TBD seconds after the route configuration is complete. [UCA-7]
(UCA-8) Control Room Operator stopped a reschedule request too soon before the requests were reflected in the train schedule. [H-1, H-2, H-3, H-4, H-5, H-6]	(SC-8) Control Room Operator should not stop providing a reschedule request before the requests were reflected in the train schedule. [UCA-8]
(UCA-9) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-9) Control Room Operator shall provide an emergency brake command when an external disturbance[1] occurs. [UCA-9]
(UCA-10) Control Room Operator does not provide an emergency brake command when abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	(SC-10) Control Room Operator shall provide an emergency brake command when abnormal behavior[2] occurs inside the vehicle. [UCA-10]
(UCA-11) Control Room Operator provides an emergency brake command when a following train is approaching. [H-2, H-5]	(SC-11) Control Room Operator should not provide an emergency brake command when a following train is approaching. [UCA-11]

UCA	Safety Constraint
(UCA-12) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-12) Control Room Operator shall provide an emergency brake command within TBD seconds after an external disturbance[1] occurs. [UCA-12]
(UCA-13) Control Room Operator provides an emergency brake command too late after abnormal behavior[2] occurs inside the vehicle. [H-2, H-3, H-5]	(SC-13) Control Room Operator shall provide an emergency brake command within TBD seconds after abnormal behavior[2] occurs inside the vehicle. [UCA-13]
(UCA-14) Control Room Operator stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]	(SC-14) Control Room Operator should not stop providing an emergency brake command before the train stopped completely. [UCA-14]
(UCA-15) Control Room Operator does not provide an evacuation door open request when passenger evacuation is required. [H-3]	(SC-15) Control Room Operator shall provide an evacuation door open request when passenger evacuation is required. [UCA-15]
(UCA-16) Control Room Operator provides an evacuation door open request when the train is in motion. [H-3, H-5]	(SC-16) Control Room Operator should not provide an evacuation door open request when the train is in motion. [UCA-16]
(UCA-17) Control Room Operator provides an evacuation door open request when passengers are crowded together near the doors and causing chaos. [H-3, H-5]	(SC-17) Control Room Operator should not provide an evacuation door open request when passengers are crowded together near the doors and causing chaos. [UCA-17]
(UCA-18) Control Room Operator provides an evacuation door open request too early before the train position is suitable for passenger evacuation. [H-3, H-5]	(SC-18) Control Room Operator shall provide an evacuation door open request within TBD seconds after the train position is suitable for passenger evacuation. [UCA-18]
(UCA-19) Control Room Operator applied an evacuation door open request too long after the evacuation had been completed. [H-6]	(SC-19) Control Room Operator shall stop providing an evacuation door open request after the evacuation had been completed. [UCA-19]
(UCA-20) Control Room Operator does not provide an evacuation door close request when the evacuation is completed. [H-6]	(SC-20) Control Room Operator shall provide an evacuation door close request when the evacuation is completed. [UCA-20]
(UCA-21) Control Room Operator provides an evacuation door close request when some passengers are still inside the vehicle. [H-3]	(SC-21) Control Room Operator should not provide an evacuation door close request when some passengers are still inside the vehicle. [UCA-21]
(UCA-22) Control Room Operator provides an evacuation door close request when passengers are evacuating. [H-3]	(SC-22) Control Room Operator should not provide an evacuation door close request when passengers are evacuating. [UCA-22]
(UCA-23) Control Room Operator provides an evacuation door close request when the conductor is still outside the vehicle for evacuation. [H-4, H-5]	(SC-23) Control Room Operator should not provide an evacuation door close request when the conductor is still outside the vehicle for evacuation. [UCA-23]

UCA	Safety Constraint
(UCA-24) Control Room Operator provides an evacuation door close request too late after the train can resume operation. [H-6]	(SC-24) Control Room Operator shall provide an evacuation door close request within TBD seconds after the train can resume operation. [UCA-24]
(UCA-25) Control Room Operator applied an evacuation door close request too long after a passenger was caught in the door. [H-3, H-4]	(SC-25) Control Room Operator shall stop providing an evacuation door close request after a passenger was caught in the door. [UCA-25]
(UCA-26) Train Operation Management System does not provide an acceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(SC-26) Train Operation Management System shall provide an acceleration command when the distance to the following train falls below the safe margin. [UCA-26]
(UCA-27) Train Operation Management System provides an acceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5]	(SC-27) Train Operation Management System should not provide an acceleration command when the running speed exceeds the target speed on a run curve. [UCA-27]
(UCA-28) Train Operation Management System provides an acceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(SC-28) Train Operation Management System should not provide an acceleration command when the running speed exceeds the safe allowable speed limit. [UCA-28]
(UCA-29) Train Operation Management System provides acceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5]	(SC-29) Train Operation Management System should not provide acceleration command when the distance to the preceding train falls below the safe margin. [UCA-29]
(UCA-30) Train Operation Management System provides acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]	(SC-30) Train Operation Management System should not provide acceleration command when the train is operating within a speed restriction zone. [UCA-30]
(UCA-31) Train Operation Management System provides an acceleration command too early before the train completely passes a speed restriction zone. [H-1, H-2, H-5]	(SC-31) Train Operation Management System shall provide an acceleration command within TBD seconds after the train completely passes a speed restriction zone. [UCA-31]
(UCA-32) Train Operation Management System applied an acceleration command too long after the train reached the target speed. [H-1, H-2, H-5]	(SC-32) Train Operation Management System shall stop providing an acceleration command after the train reached the target speed. [UCA-32]
(UCA-33) Train Operation Management System does not provide a deceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(SC-33) Train Operation Management System shall provide a deceleration command when the running speed exceeds the safe allowable speed limit. [UCA-33]
(UCA-34) Train Operation Management System does not provide a deceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5]	(SC-34) Train Operation Management System shall provide a deceleration command when the running speed exceeds the target speed on a run curve. [UCA-34]

UCA	Safety Constraint
(UCA-35) Train Operation Management System does not provide a deceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5]	(SC-35) Train Operation Management System shall provide a deceleration command when the distance to the preceding train falls below the safe margin. [UCA-35]
(UCA-36) Train Operation Management System provides a deceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(SC-36) Train Operation Management System should not provide deceleration command when the distance to the following train falls below the safe margin. [UCA-36]
(UCA-37) Train Operation Management System provides a deceleration command too late after the train enters a speed restriction zone. [H-1, H-2, H-5]	(SC-37) Train Operation Management System shall provide a deceleration command within TBD seconds after the train enters a speed restriction zone. [UCA-37]
(UCA-38) Train Operation Management System stopped a deceleration command too soon before the train reached the target speed. [H-1, H-2, H-5]	(SC-38) Train Operation Management System should not stop providing a deceleration command before the train reached the target speed. [UCA-38]
(UCA-39) Train Operation Management System does not provide an emergency brake command when an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	(SC-39) Train Operation Management System shall provide an emergency brake command when an emergency brake command is received from Control Room Operator. [UCA-39]
(UCA-40) Train Operation Management System provides an emergency brake command when a following train is approaching. [H-5]	(SC-40) Train Operation Management System should not provide an emergency brake command when a following train is approaching. [UCA-40]
(UCA-41) Train Operation Management System provides an emergency brake command too late after an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	(SC-41) Train Operation Management System shall provide an emergency brake command within TBD seconds after an emergency brake command is received from Control Room Operator. [UCA-41]
(UCA-42) Train Operation Management System stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]	(SC-42) Train Operation Management System should not stop providing an emergency brake command before the train stopped completely. [UCA-42]
(UCA-43) Train Operation Management System does not provide a door open request when the train arrives at the station. [H-6]	(SC-43) Train Operation Management System shall provide a door open request when the train arrives at the station. [UCA-43]
(UCA-44) Train Operation Management System provides a door open request when the train is in motion. [H-4, H-5]	(SC-44) Train Operation Management System should not provide a door open request when the train is in motion. [UCA-44]
(UCA-45) Train Operation Management System provides a door open request when the train is not at the appropriate boarding/alighting position. [H-3, H-4]	(SC-45) Train Operation Management System should not provide a door open request when the train is not at the appropriate boarding/alighting position. [UCA-45]

UCA	Safety Constraint
(UCA-46) Train Operation Management System provides a door open request too early before the train completely stops. [H-4]	(SC-46) Train Operation Management System shall provide a door open request within TBD seconds after the train completely stops. [UCA-46]
(UCA-47) Train Operation Management System applied a door open request too long after the departure time had passed. [H-6]	(SC-47) Train Operation Management System should stop providing a door open request after the departure time had passed. [UCA-47]
(UCA-48) Train Operation Management System does not provide a door close request when the departure time arrives. [H-2, H-5]	(SC-48) Train Operation Management System shall provide a door close request when the departure time arrives. [UCA-48]
(UCA-49) Train Operation Management System provides a door close request when passengers are boarding or alighting. [H-4]	(SC-49) Train Operation Management System should not provide a door close request when passengers are boarding or alighting. [UCA-49]
(UCA-50) Train Operation Management System provides a door close request when passenger evacuation is required. [H-3]	(SC-50) Train Operation Management System should not provide a door close request when passenger evacuation is required. [UCA-50]
(UCA-51) Train Operation Management System provides a door close request too late after the train starts moving. [H-4, H-5]	(SC-51) Train Operation Management System shall provide a door close request within TBD seconds before the train starts moving. [UCA-51]
(UCA-52) Train Operation Management System applied a door close request too long after a passenger was caught in the doors. [H-3, H-4]	(SC-52) Train Operation Management System should stop providing a door close request after a passenger was caught in the doors. [UCA-52]
(UCA-53) Train Operation Management System does not provide a landing gear deploy request when the train enters the wheel running mode. [H-5]	(SC-53) Train Operation Management System shall provide a landing gear deploy request when the train enters the wheel running mode. [UCA-53]
(UCA-54) Train Operation Management System provides a landing gear deploy request when the train is in the levitation running mode. [H-2, H-5]	(SC-54) Train Operation Management System should not provide a landing gear deploy request when the train is in the levitation running mode. [UCA-54]
(UCA-55) Train Operation Management System provides a landing gear deploy request too late after the train's speed falls below 75 miles per hour (the threshold for the wheel running mode). [H-5]	(SC-55) Train Operation Management System shall provide a landing gear deploy request within TB seconds after the train's speed falls below 75 miles per hour (the threshold for the wheel running mode). [UCA-55]
(UCA-56) Train Operation Management System stopped a landing gear deploy request too soon before the landing gear was fully deployed. [H-5]	(SC-56) Train Operation Management System should not stop providing a landing gear deploy request before the landing gear was fully deployed. [UCA-56]
(UCA-57) Train Operation Management System does not provide a landing gear retract	(SC-57) Train Operation Management System shall provide a landing gear retract request

UCA	Safety Constraint
request when the train is in levitation running mode. [H-2, H-5]	when the train is in levitation running mode. [UCA-57]
(UCA-58) Train Operation Management System provides a landing gear retract request when the train is in wheel running mode. [H-5]	(SC-58) Train Operation Management System should not provide a landing gear retract request when the train is in wheel running mode. [UCA-58]
(UCA-59) Train Operation Management System provides a landing gear retract request when the train stops at the station. [H-3, H-4, H-5]	(SC-59) Train Operation Management System should not provide a landing gear retract request when the train stops at the station. [UCA-59]
(UCA-60) Train Operation Management System provides a landing gear retract request too late after the train's speed exceeds 75 miles per hour (the threshold for the levitation running mode). [H-5]	(SC-60) Train Operation Management System shall provide a landing gear retract request within TBD seconds after the train's speed exceeds 75 miles per hour (the threshold for the levitation running mode). [UCA-60]
(UCA-61) Train Operation Management System stopped a landing gear retract request too soon before the landing gear was fully retracted. [H-5]	(SC-61) Train Operation Management System stopped a landing gear retract request too soon before the landing gear was fully retracted. [UCA-61]
(UCA-62) Drive Control System does not provide a target current command when the running speed does not keep the target speed. [H-1, H-2, H-5]	(SC-62) Drive Control System shall provide a target current command when the running speed does not keep the target speed. [UCA-62]
(UCA-63) Drive Control System provides a target current command when personnel are entering the guideway for emergency maintenance. [H-5]	(SC-63) Drive Control System should not provide a target current command when personnel are entering the guideway for emergency maintenance. [UCA-63]
(UCA-64) Drive Control System provides a target current command too early before the calculation of the current value and phase is complete. [H-1, H-2, H-5]	(SC-64) Drive Control System shall provide a target current command within TBD seconds after the calculation of the current value and phase is complete. [UCA-64]
(UCA-65) Drive Control System stopped a target current command too soon before the train's speed reached the target speed. [H-1, H-2, H-5]	(SC-65) Drive Control System should not stop providing a target current command before the train's speed reached the target speed. [UCA-65]
(UCA-66) Safety Control System does not provide an emergency brake command when traveling above the safe allowable speed limit. [H-1, H-2, H-5]	(SC-66) Safety Control System shall provide an emergency brake command when traveling above the safe allowable speed limit. [UCA-66]
(UCA-67) Safety Control System does not provide an emergency brake command when an emergency brake command is initiated by Control Room Operator [H-1, H-2, H-3, H-5]	(SC-67) Safety Control System shall provide an emergency brake command when an emergency brake command is initiated by Control Room Operator [UCA-67]

UCA	Safety Constraint
(UCA-68) Safety Control System provides an emergency brake command when a following train is approaching. [H-5]	(SC-68) Safety Control System should not provide an emergency brake command when a following train is approaching. [UCA-68]
(UCA-69) Safety Control System provides an emergency brake command too late after the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(SC-69) Safety Control System shall provides an emergency brake command within TBD seconds after the running speed exceeds the safe allowable speed limit. [UCA-69]
(UCA-70) Safety Control System stopped an emergency brake command too soon before the train completely stopped. [H-2, H-5]	(SC-70) Safety Control System should not stop providing an emergency brake command before the train completely stopped. [UCA-70]
(UCA-71) Safety Control System does not provide a door open enable when the door-open condition[3] is met and passenger evacuation is necessary. [H-3]	(SC-71) Safety Control System shall provide a door open enable when the door-open condition[3] is met and passenger evacuation is necessary. [UCA-71]
(UCA-72) Safety Control System provides a door open enable when the door-open condition[3] is not met. [H-4]	(SC-72) Safety Control System should not provide a door open enable when the door-open condition[3] is not met. [UCA-72]
(UCA-73) Safety Control System provides a door open enable too early before confirming whether the door-open condition[3] is met. [H-4]	(SC-73) Safety Control System shall provide a door open enable within TBD seconds after confirming whether the door-open condition[3] is met. [UCA-73]
(UCA-74) Safety Control System applied a door open enable too long after the door-open condition[3] was no longer met. [H-4]	(SC-74) Safety Control System shall stop providing a door open enable after the door-open condition[3] was no longer met. [UCA-74]
(UCA-75) Safety Control System does not provide a door close enable when the door-close condition[4] is met. [H-4, H-5]	(SC-75) Safety Control System shall provide a door close enable when the door-close condition[4] is met. [UCA-75]
(UCA-76) Safety Control System provides a door close enable when the door-close condition[4] is not met. [H-4]	(SC-76) Safety Control System should not provide a door close enable when the door-close condition[4] is not met. [UCA-76]
(UCA-77) Safety Control System provides a door close enable when passenger evacuation is necessary. [H-3]	(SC-77) Safety Control System should not provide a door close enable when passenger evacuation is necessary. [UCA-77]
(UCA-78) Safety Control System provides a door close enable too early before confirming whether the door-close condition[4] is met. [H-4]	(SC-78) Safety Control System shall provide a door close enable within TBD seconds after confirming whether the door-close condition[4] is met. [UCA-78]
(UCA-79) Safety Control System applied a door close enable too long after the door-close condition[4] was no longer met. [H-4]	(SC-79) Safety Control System shall stop providing a door close enable after the door-close condition[4] was no longer met. [UCA-79]
(UCA-80) Safety Control System does not provide a landing gear deploy enable when the wheel-running condition[5] is met. [H-5]	(SC-80) Safety Control System shall provide a landing gear deploy enable when the wheel-running condition[5] is met. [UCA-80]

UCA	Safety Constraint
(UCA-81) Safety Control System provides a landing gear deploy enable when the wheel-running condition[5] is not met. [H-5]	(SC-81) Safety Control System should not provide a landing gear deploy enable when the wheel-running condition[5] is not met. [UCA-81]
(UCA-82) Safety Control System provides a landing gear deploy enable too early before confirming whether the wheel-running condition[5] is met. [H-5]	(SC-82) Safety Control System shall provide a landing gear deploy enable within TBD seconds after confirming whether the wheel-running condition[5] is met. [UCA-82]
(UCA-83) Safety Control System applied a landing gear deploy enable too long after the wheel-running condition[5] was no longer met. [H-5]	(SC-83) Safety Control System shall stop providing a landing gear deploy enable after the wheel-running condition[5] was no longer met. [UCA-83]
(UCA-84) Safety Control System does not provide a landing gear retract enable when the levitation-running condition[6] is met. [H-2, H-5]	(SC-84) Safety Control System shall provide a landing gear retract enable when the levitation-running condition[6] is met. [UCA-84]
(UCA-85) Safety Control System provides a landing gear retract enable when the levitation-running condition[6] is not met. [H-5]	(SC-85) Safety Control System should not provide a landing gear retract enable when the levitation-running condition[6] is not met. [UCA-85]
(UCA-86) Safety Control System provides a landing gear retract enable too early before confirming whether the levitation-running condition[6] is met. [H-5]	(SC-86) Safety Control System shall provide a landing gear retract enable within TBD seconds after confirming whether the levitation-running condition[6] is met. [UCA-86]
(UCA-87) Safety Control System applied a landing gear retract enable too long after the levitation-running condition[5] was no longer met. [H-5]	(SC-87) Safety Control System shall stop providing a landing gear retract enable after the levitation-running condition[5] was no longer met. [UCA-87]
(UCA-88) Onboard Train Control System does not provide a brake actuation when the regenerative brake is insufficient. [H-1, H-2, H-5]	(SC-88) Onboard Train Control System shall provide a brake actuation when the regenerative brake is insufficient. [UCA-88]
(UCA-89) Onboard Train Control System does not provide a brake actuation when an emergency brake command has been received. [H-1, H-2, H-5]	(SC-89) Onboard Train Control System shall provide a brake actuation when an emergency brake command has been received. [UCA-89]
(UCA-90) Onboard Train Control System provides a brake actuation when the train is operating on an icy guideway. [H-1, H-2, H-5]	(SC-90) Onboard Train Control System should not provide a brake actuation when the train is operating on an icy guideway. [UCA-90]
(UCA-91) Onboard Train Control System provides a brake actuation too late after an emergency brake command has been received. [H-1, H-2, H-5]	(SC-91) Onboard Train Control System shall provide a brake actuation within TBD seconds after an emergency brake command has been received. [UCA-91]

UCA	Safety Constraint
(UCA-92) Onboard Train Control System stopped a brake actuation too soon before the train completely stopped. [H-1, H-5]	(SC-92) Onboard Train Control System should not stop providing a brake actuation before the train completely stopped. [UCA-92]
(UCA-93) Onboard Train Control System does not provide a door actuation when receiving a door open/close enable. [H-3, H-4]	(SC-93) Onboard Train Control System shall provide a door actuation when receiving a door open/close enable. [UCA-93]
(UCA-94) Onboard Train Control System does not provide a door actuation when a passenger is caught in the door. [H-4]	(SC-94) Onboard Train Control System shall provide a door actuation when a passenger is caught in the door. [UCA-94]
(UCA-95) Onboard Train Control System provides a door actuation when passenger boarding or alighting is still in progress. [H-3, H-4]	(SC-95) Onboard Train Control System should not provide a door actuation when passenger boarding or alighting is still in progress. [UCA-95]
(UCA-96) Onboard Train Control System provides a door actuation when the train is still in motion. [H-4]	(SC-96) Onboard Train Control System should not provide a door actuation when the train is still in motion. [UCA-96]
(UCA-97) Onboard Train Control System provides a door actuation too early before receiving a door open/close enable. [H-3, H-4]	(SC-97) Onboard Train Control System shall provide a door actuation within TBD seconds after receiving a door open/close enable. [UCA-97]
(UCA-98) Onboard Train Control System applied a door actuation too long after a passenger was caught in the doors. [H-3, H-4]	(SC-98) Onboard Train Control System shall stop providing a door actuation after a passenger was caught in the doors. [UCA-98]
(UCA-99) Onboard Train Control System does not provide a landing gear actuation when receiving a landing gear deploy/retract enable. [H-5]	(SC-99) Onboard Train Control System shall provide a landing gear actuation when receiving a landing gear deploy/retract enable. [UCA-99]
(UCA-100) Onboard Train Control System provides a landing gear actuation when the train's speed is not in the threshold range. [H-5]	(SC-100) Onboard Train Control System should not provide a landing gear actuation when the train's speed is not in the threshold range. [UCA-100]
(UCA-101) Onboard Train Control System provides a landing gear actuation too late after receiving a landing gear deploy/retract enable. [H-5]	(SC-101) Onboard Train Control System shall provide a landing gear actuation within TBD seconds after receiving a landing gear deploy/retract enable. [UCA-101]
(UCA-102) Onboard Train Control System stopped a landing gear actuation too soon before the landing gear touched the ground. [H-5]	(SC-102) Onboard Train Control System should not stop providing a landing gear actuation before the landing gear touched the ground. [UCA-102]

Note.

[1] An external disturbance includes fire, earthquake, terrorism, obstacles, damage to facilities, intruders, and blackout.

[2] Abnormal behavior includes vibration, noise, and odor.

[3] The door-open condition is when the train completely stops and is at the appropriate position.

[4] The door-close condition is when passenger boarding/alighting is completed, and nothing is caught in the door.

[5] The wheel-running condition is when the train speed falls below 75 miles per hour.

[6] The levitation-running condition is when the train speed exceeds 75 miles per hour.

Appendix B.1: Enlarged Control Structure for the “With Conductor” Model

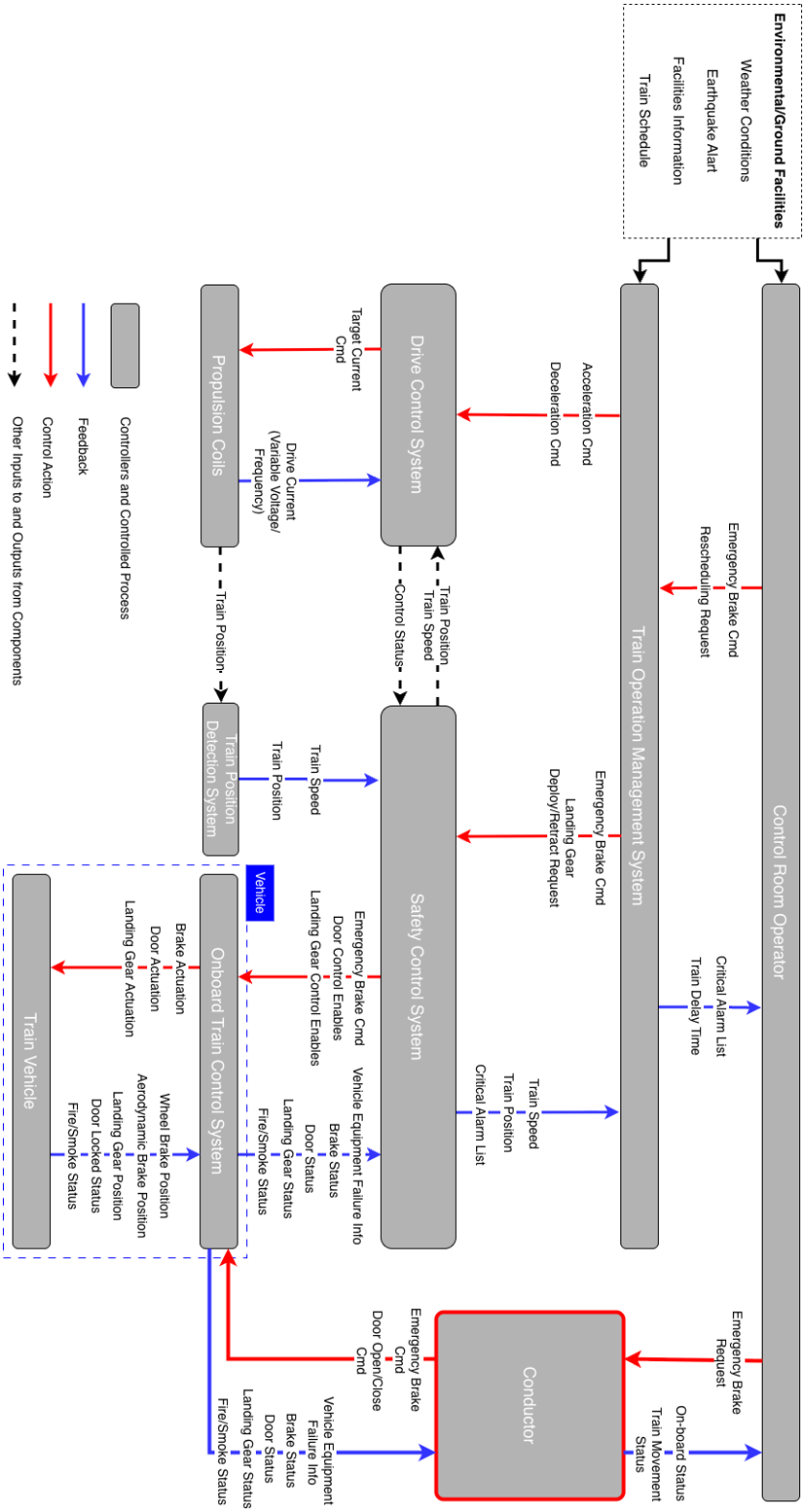


Figure 17. Enlarged Control Structure for the “With Conductor” Model

Appendix B.2: All UCAs Identified in the "With Conductor" Model

Table 21. All UCAs Identified in the "With Conductor" Model

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Controller: Control Room Operator				
Reschedule Request	(UCA-103) Control Room Operator does not provide a reschedule request when a suddenly sick person requires an emergency stop at the next station. [H-3] (UCA-104) Control Room Operator does not provide a reschedule request when the arrival track at the next station must be changed. [H-2, H-5] (UCA-105) Control Room Operator does not provide a reschedule request when a temporary speed restriction setting is required. [H-1, H-2, H-5]	(UCA-106) Control Room Operator provides a reschedule request when the tracks are closed. [H-5, H-6] (UCA-107) Control Room Operator provides a reschedule request when maintenance work is being carried out. [H-5]	(UCA-108) Control Room Operator provides a reschedule request too early before the official request is finalized in the operation center. [H-1, H-2, H-3, H-4, H-5] (UCA-109) Control Room Operator provides a reschedule request too early before the route configuration is complete. [H-1, H-2, H-5]	(UCA-110) Control Room Operator stopped a reschedule request too soon before the requests were reflected in the train schedule. [H-1, H-2, H-3, H-4, H-5]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Emergency Brake Command	(UCA-111) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(UCA-112) Control Room Operator provides an emergency brake command when a following train is approaching. [H-2, H-5]	(UCA-113) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	(UCA-114) Control Room Operator stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]
Emergency Brake Request	(UCA-115) Control Room Operator does not provide an emergency brake request to the Conductor when the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	(UCA-116) Control Room Operator provides an emergency brake request to the conductor instead of executing a direct remote activation when an emergency is occurring. [H-1, H-2, H-5]	(UCA-117) Control Room Operator provides an emergency brake request to the conductor too late after the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	(UCA-118) Control Room Operator stopped an emergency brake request to the conductor too soon before the conductor initiated a direct emergency brake. [H-1, H-2, H-5]
Controller: Conductor				
Emergency Brake Command	(UCA-119) Conductor does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(UCA-121) Conductor provides an emergency brake command when a fire is detected and the train is located inside a long tunnel. [H-3] (UCA-122) Conductor	(UCA-123) Conductor provides an emergency brake too late after an external disturbance[1] occurs. [H-2, H-3, H-5] (UCA-124) Conductor	(UCA-125) Conductor stopped an emergency brake command too soon before the train completely stopped. [H-5]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	(UCA-120) Conductor does not provide an emergency brake command when abnormal behavior[2] occurs. [H-2, H-3, H-5]	provides an emergency brake command when a following train is approaching. [H-2, H-5]	provides an emergency brake command too late after abnormal behavior[2] occurs. [H-2, H-3, H-5]	
Door Open Command	(UCA-126) Conductor does not provide a door open command when passenger evacuation is required. [H-3] (UCA-127) Conductor does not provide a door open command when a passenger is caught in the door. [H-4] (UCA-128) Conductor does not provide a door open command when the train arrives at the station. [H-6]	(UCA-129) Conductor provides a door open command when the train is in motion. [H-4, H-5] (UCA-130) Conductor provides a door open command when the train is not at the appropriate boarding/alighting position. [H-3, H-4] (UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	(UCA-132) Conductor provides a door open command too early before the train completely stops. [H-4] (UCA-133) Conductor provides a door open command too early before the train position is suitable for passenger evacuation. [H-3, H-5] (UCA-134) Conductor provides a door open command too early before oncoming train protections have not been completed. [H-3, H-5]	(UCA-135) Conductor applied a door open command too long after the evacuation had been completed. [H-5] (UCA-136) Conductor applied a door open command too long after the departure time had passed. [H-6]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Door Close Command	(UCA-137) Conductor does not provide a door close command when the departure time arrives. [H-2, H-5] (UCA-138) Conductor does not provide a door close command when the evacuation has been completed. [H-6]	(UCA-139) Conductor provides a door close command when passengers are boarding or alighting. [H-4] (UCA-140) Conductor provides a door close command when passenger evacuation is required. [H-3]	(UCA-141) Conductor provides a door close command too late after the train starts moving. [H-4, H-5] (UCA-142) Conductor provides a door close command too late after the train can resume operation. [H-6]	(UCA-143) Conductor applied a door close command too long after a passenger was caught in the doors. [H-3, H-4]
Controller: Train Operation Management System				
Acceleration Command	(UCA-144) Train Operation Management System does not provide an acceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(UCA-145) Train Operation Management System provides an acceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5] (UCA-146) Train Operation Management System provides an acceleration command when the running speed exceeds the safe allowable speed	(UCA-149) Train Operation Management System provides an acceleration command too early before the train completely passes a speed restriction zone. [H-1, H-2, H-5]	(UCA-150) Train Operation Management System applied an acceleration command too long after the train reached the target speed. [H-1, H-2, H-5]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
		limit. [H-1, H-2, H-5] (UCA-147) Train Operation Management System provides acceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5] (UCA-148) Train Operation Management System provides acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]		
Deceleration Command	(UCA-151) Train Operation Management System does not provide a deceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5] (UCA-152) Train Operation	(UCA-154) Train Operation Management System provides a deceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(UCA-155) Train Operation Management System provides a deceleration command too late after the train enters a speed restriction zone. [H-1, H-2, H-5]	(UCA-156) Train Operation Management System stopped a deceleration command too soon before the train reached the target speed. [H-1, H-2, H-5]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	Management System does not provide a deceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5] (UCA-153) Train Operation Management System does not provide a deceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5]			
Emergency Brake Command	(UCA-157) Train Operation Management System does not provide an emergency brake command when an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	(UCA-158) Train Operation Management System provides an emergency brake command when a following train is approaching. [H-5]	(UCA-159) Train Operation Management System provides an emergency brake command too late after an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	(UCA-160) Train Operation Management System stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]
Landing Gear Deploy Request	(UCA-161) Train Operation Management System does	(UCA-162) Train Operation Management System provides a	(UCA-163) Train Operation Management System provides	(UCA-164) Train Operation Management System stopped

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	not provide a landing gear deploy request when the train enters wheel running mode. [H-5]	landing gear deploy request when the train is in levitation running mode. [H-2, H-5]	a landing gear deploy request too late after the train's speed falls below 75 miles per hour (the threshold for the wheel running mode). [H-5]	a landing gear deploy request too soon before the landing gear was fully deployed. [H-5]
Landing Gear Retract Request	(UCA-165) Train Operation Management System does not provide a landing gear retract request when the train is in levitation running mode. [H-2, H-5]	(UCA-166) Train Operation Management System provides a landing gear retract request when the train is in wheel running mode. [H-5] (UCA-167) Train Operation Management System provides a landing gear retract request when the train stops at the station. [H-3, H-4, H-5]	(UCA-168) Train Operation Management System provides a landing gear retract request too late after the train's speed exceeds 75 miles per hour (the threshold for the levitation running mode). [H-5]	(UCA-169) Train Operation Management System stopped a landing gear retract request too soon before the landing gear was fully retracted. [H-5]
Controller: Drive Control System				
Target Current Command	(UCA-170) Drive Control System does not provide a target current command when the running speed does not keep the target	(UCA-171) Drive Control System provides a target current command when personnel are entering the guideway for emergency	(UCA-172) Drive Control System provides a target current command too early before the calculation of the current value and phase is	(UCA-173) Drive Control System stopped a target current command too soon before the train's speed reached the

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	speed. [H-1, H-2, H-5]	maintenance. [H-5]	complete. [H-1, H-2, H-5]	target speed. [H-1, H-2, H-5]
Controller: Safety Control System				
Emergency Brake Command	(UCA-174) Safety Control System does not provide an emergency brake command when traveling above the safe allowable speed limit. [H-1, H-2, H-5] (UCA-175) Safety Control System does not provide an emergency brake command when an emergency brake command is initiated by Control Room Operator [H-1, H-2, H-3, H-5]	(UCA-176) Safety Control System provides an emergency brake command when a following train is approaching. [H-5]	(UCA-177) Safety Control System provides an emergency brake command too late after the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(UCA-178) Safety Control System stopped an emergency brake command too soon before the train completely stopped. [H-2, H-5]
Door Open Enable	(UCA-179) Safety Control System does not provide a door open enable when the door-open condition[3] is met and passenger evacuation is	(UCA-180) Safety Control System provides a door open enable when the door-open condition[3] is not met. [H-4]	(UCA-181) Safety Control System provides a door open enable too early before confirming whether the door-open condition[3] is met. [H-4]	(UCA-182) Safety Control System applied a door open enable too long after the door-open condition[3] was no longer met. [H-4]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	necessary. [H-3]			
Door Close Enable	(UCA-183) Safety Control System does not provide a door close enable when the door-close condition[4] is met. [H-4, H-5]	(UCA-184) Safety Control System provides a door close enable when the door-close condition[4] is not met. [H-4] (UCA-185) Safety Control System provides a door close enable when passenger evacuation is necessary. [H-3]	(UCA-186) Safety Control System provides a door close enable too early before confirming whether the door-close condition[4] is met. [H-4]	(UCA-187) Safety Control System applied a door close enable too long after the door-close condition[4] was no longer met. [H-4]
Landing Gear Deploy Enable	(UCA-188) Safety Control System does not provide a landing gear deploy enable when the wheel-running condition[5] is met. [H-5]	(UCA-189) Safety Control System provides a landing gear deploy enable when the wheel-running condition[5] is not met. [H-5]	(UCA-190) Safety Control System provides a landing gear deploy enable too early before confirming whether the wheel-running condition[5] is met. [H-5]	(UCA-191) Safety Control System applied a landing gear deploy enable too long after the wheel-running condition[5] was no longer met. [H-5]
Landing Gear Retract Enable	(UCA-192) Safety Control System does not provide a landing gear retract enable when the levitation-running condition[6] is met. [H-2, H-5]	(UCA-193) Safety Control System provides a landing gear retract enable when the levitation-running condition[6] is not met. [H-5]	(UCA-194) Safety Control System provides a landing gear retract enable too early before confirming whether the levitation-running condition[6] is met. [H-5]	(UCA-195) Safety Control System applied a landing gear retract enable too long after the levitation-running condition[5] was no longer met. [H-5]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Onboard Train Control System				
Brake Actuation	(UCA-196) Onboard Train Control System does not provide a brake actuation when the regenerative brake is insufficient. [H-1, H-2, H-5] (UCA-197) Onboard Train Control System does not provide a brake actuation when an emergency brake command has been received. [H-1, H-2, H-5]	(UCA-198) Onboard Train Control System provides a brake actuation when the train is operating on an icy guideway. [H-1, H-2, H-5]	(UCA-199) Onboard Train Control System provides a brake actuation too late after an emergency brake command has been received. [H-1, H-2, H-5]	(UCA-200) Onboard Train Control System stopped a brake actuation too soon before the train completely stopped. [H-1, H-5]
Door Actuation	(UCA-201) Onboard Train Control System does not provide a door actuation when receiving a door open/close enable. [H-3, H-4] (UCA-202) Onboard Train Control System does not provide a door actuation when	(UCA-203) Onboard Train Control System provides a door actuation when passenger boarding or alighting is still in progress. [H-3, H-4] (UCA-204) Onboard Train Control System provides a door actuation when	(UCA-205) Onboard Train Control System provides a door actuation too early before receiving a door open/close enable. [H-3, H-4]	(UCA-206) Onboard Train Control System applied a door actuation too long after the rescue of a passenger caught in the doors was complete. [H-3, H-4]

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
	a passenger is caught in the door. [H-4]	the train is still in motion. [H-4]		
Landing Gear Actuation	(UCA-207) Onboard Train Control System does not provide a landing gear actuation when receiving a landing gear deploy/retract enable. [H-5]	(UCA-208) Onboard Train Control System provides a landing gear actuation when the train's speed is not in the threshold range. [H-5]	(UCA-209) Onboard Train Control System provides a landing gear actuation too late after receiving a landing gear deploy/retract enable. [H-5]	(UCA-210) Onboard Train Control System stopped a landing gear actuation too soon before the landing gear touched the ground. [H-5]

Appendix B.3: All Safety Constraints for the "With Conductor" Model

Table 22. All Safety Constraints for the "With Conductor" Model

UCA	Safety Constraint
(UCA-103) Control Room Operator does not provide a reschedule request when a suddenly sick person requires an emergency stop at the next station. [H-3]	(SC-103) Control Room Operator shall provide a reschedule request when a suddenly sick person requires an emergency stop at the next station. [UCA-103]
(UCA-104) Control Room Operator does not provide a reschedule request when the arrival track at the next station must be changed. [H-2, H-5]	(SC-104) Control Room Operator shall provide a reschedule request when the arrival track at the next station must be changed. [UCA-104]
(UCA-105) Control Room Operator does not provide a reschedule request when a temporary speed restriction setting is required. [H-1, H-2, H-5]	(SC-105) Control Room Operator shall provide a reschedule request when a temporary speed restriction setting is required. [UCA-105]
(UCA-106) Control Room Operator provides a reschedule request when the tracks are closed. [H-5, H-6]	(SC-106) Control Room Operator should not provide a reschedule request when the tracks are closed. [UCA-106]
(UCA-107) Control Room Operator provides a reschedule request when maintenance work is being carried out. [H-5]	(SC-107) Control Room Operator should not provide a reschedule request when maintenance work is being carried out. [UCA-107]
(UCA-108) Control Room Operator provides a reschedule request too early before the official request is finalized in the operation center. [H-1, H-2, H-3, H-4, H-5]	(SC-108) Control Room Operator shall provide a reschedule request within TBD seconds after the official request is finalized in the operation center. [UCA-108]
(UCA-109) Control Room Operator provides a reschedule request too early before the route configuration is complete. [H-1, H-2, H-5]	(SC-109) Control Room Operator shall provide a reschedule request within TBD seconds after the route configuration is complete. [UCA-109]
(UCA-110) Control Room Operator stopped a reschedule request too soon before the requests were reflected in the train schedule. [H-1, H-2, H-3, H-4, H-5]	(SC-110) Control Room Operator should not stop providing a reschedule request before the requests were reflected in the train schedule. [UCA-110]

UCA	Safety Constraint
(UCA-111) Control Room Operator does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-111) Control Room Operator shall provide an emergency brake command when an external disturbance[1] occurs. [UCA-111]
(UCA-112) Control Room Operator provides an emergency brake command when a following train is approaching. [H-2, H-5]	(SC-112) Control Room Operator should not provide an emergency brake command when a following train is approaching. [UCA-112]
(UCA-113) Control Room Operator provides an emergency brake command too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-113) Control Room Operator shall provide an emergency brake command within TBD seconds after an external disturbance[1] occurs. [UCA-113]
(UCA-114) Control Room Operator stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]	(SC-114) Control Room Operator should not stop providing an emergency brake command before the train stopped completely. [UCA-114]
(UCA-115) Control Room Operator does not provide an emergency brake request to the Conductor when the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	(SC-115) Control Room Operator shall provide an emergency brake request to the Conductor when the operator cannot issue the direct remote emergency brake command. [UCA-115]
(UCA-116) Control Room Operator provides an emergency brake request to the conductor instead of executing a direct remote activation when an emergency is occurring. [H-1, H-2, H-5]	(SC-116) Control Room Operator should not provide an emergency brake request to the conductor instead of executing a direct remote activation when an emergency is occurring. [UCA-116]
(UCA-117) Control Room Operator provides an emergency brake request to the conductor too late after the operator cannot issue the direct remote emergency brake command. [H-1, H-2, H-5]	(SC-117) Control Room Operator shall provide an emergency brake request to the conductor within TBD seconds after the operator cannot issue the direct remote emergency brake command. [UCA-117]
(UCA-118) Control Room Operator stopped an emergency brake request to the conductor too soon before the conductor initiated a direct emergency brake. [H-1, H-2, H-5]	(SC-118) Control Room Operator should not stop providing an emergency brake request to the conductor before the conductor initiated a direct emergency brake. [UCA-118]

UCA	Safety Constraint
(UCA-119) Conductor does not provide an emergency brake command when an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-119) Conductor shall provide an emergency brake command when an external disturbance[1] occurs. [UCA-119]
(UCA-120) Conductor does not provide an emergency brake command when abnormal behavior[2] occurs. [H-2, H-3, H-5]	(SC-120) Conductor shall provide an emergency brake command when abnormal behavior[2] occurs. [UCA-120]
(UCA-121) Conductor provides an emergency brake command when a fire is detected and the train is located inside a long tunnel. [H-3]	(SC-121) Conductor should not provide an emergency brake command when a fire is detected, and the train is located inside a long tunnel. [UCA-121]
(UCA-122) Conductor provides an emergency brake command when a following train is approaching. [H-2, H-5]	(SC-122) Conductor should not provide an emergency brake command when a following train is approaching. [UCA-122]
(UCA-123) Conductor provides an emergency brake too late after an external disturbance[1] occurs. [H-2, H-3, H-5]	(SC-123) Conductor shall provide an emergency brake within TBD seconds after an external disturbance[1] occurs. [UCA-123]
(UCA-124) Conductor provides an emergency brake command too late after abnormal behavior[2] occurs. [H-2, H-3, H-5]	(SC-124) Conductor shall provide an emergency brake command within TBD seconds after abnormal behavior[2] occurs. [UCA-124]
(UCA-125) Conductor stopped an emergency brake command too soon before the train completely stopped. [H-5]	(SC-125) Conductor should not stop providing an emergency brake command before the train completely stopped. [UCA-125]
(UCA-126) Conductor does not provide a door open command when passenger evacuation is required. [H-3]	(SC-126) Conductor shall provide a door open command when passenger evacuation is required. [UCA-126]
(UCA-127) Conductor does not provide a door open command when a passenger is caught in the door. [H-4]	(SC-127) Conductor shall provide a door open command when a passenger is caught in the door. [UCA-127]
(UCA-128) Conductor does not provide a door open command when the train arrives at the station. [H-6]	(SC-128) Conductor shall provide a door open command when the train arrives at the station. [UCA-128]

UCA	Safety Constraint
(UCA-129) Conductor provides a door open command when the train is in motion. [H-4, H-5]	(SC-129) Conductor should not provide a door open command when the train is in motion. [UCA-129]
(UCA-130) Conductor provides a door open command when the train is not at the appropriate boarding/alighting position. [H-3, H-4]	(SC-130) Conductor should not provide a door open command when the train is not at the appropriate boarding/alighting position. [UCA-130]
(UCA-131) Conductor provides a door open command when a strong magnetic field is generated along the guideway. [H-3]	(SC-131) Conductor should not provide a door open command when a strong magnetic field is generated along the guideway. [UCA-131]
(UCA-132) Conductor provides a door open command too early before the train completely stops. [H-4]	(SC-132) Conductor shall provide a door open command within TBD seconds after the train completely stops. [UCA-132]
(UCA-133) Conductor provides a door open command too early before the train position is suitable for passenger evacuation. [H-3, H-5]	(SC-133) Conductor shall provide a door open command within TBD seconds after the train position is suitable for passenger evacuation. [UCA-133]
(UCA-134) Conductor provides a door open command too early before oncoming train protections have not been completed. [H-3, H-5]	(SC-134) Conductor shall provide a door open command within TBD seconds after oncoming train protections have not been completed. [UCA-134]
(UCA-135) Conductor applied a door open command too long after the evacuation had been completed. [H-5]	(SC-135) Conductor shall stop providing a door open command after the evacuation had been completed. [UCA-135]
(UCA-136) Conductor applied a door open command too long after the departure time had passed. [H-6]	(SC-136) Conductor shall stop providing a door open command after the departure time had passed. [UCA-136]
(UCA-137) Conductor does not provide a door close command when the departure time arrives. [H-2, H-5]	(SC-137) Conductor shall provide a door close command when the departure time arrives. [UCA-137]
(UCA-138) Conductor does not provide a door close command when the evacuation has been completed. [H-6]	(SC-138) Conductor shall provide a door close command when the evacuation has been completed. [UCA-138]

UCA	Safety Constraint
(UCA-139) Conductor provides a door close command when passengers are boarding or alighting. [H-4]	(SC-139) Conductor should not provide a door close command when passengers are boarding or alighting. [UCA-139]
(UCA-140) Conductor provides a door close command when passenger evacuation is required. [H-3]	(SC-140) Conductor should not provide a door close command when passenger evacuation is required. [UCA-140]
(UCA-141) Conductor provides a door close command too late after the train starts moving. [H-4, H-5]	(SC-141) Conductor shall provide a door close command within TBD seconds after the train starts moving. [UCA-141]
(UCA-142) Conductor provides a door close command too late after the train can resume operation. [H-6]	(SC-142) Conductor shall provide a door close command within TBD seconds after the train can resume operation. [UCA-142]
(UCA-143) Conductor applied a door close command too long after a passenger is caught in the doors. [H-3, H-4]	(SC-143) Conductor shall stop providing a door close command after a passenger is caught in the doors. [UCA-143]
(UCA-144) Train Operation Management System does not provide an acceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(SC-144) Train Operation Management System shall provide an acceleration command when the distance to the following train falls below the safe margin. [UCA-144]
(UCA-145) Train Operation Management System provides an acceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5]	(SC-145) Train Operation Management System should not provide an acceleration command when the running speed exceeds the target speed on a run curve. [UCA-145]
(UCA-146) Train Operation Management System provides an acceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(SC-146) Train Operation Management System should not provide an acceleration command when the running speed exceeds the safe allowable speed limit. [UCA-146]
(UCA-147) Train Operation Management System provides acceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5]	(SC-147) Train Operation Management System should not provide acceleration command when the distance to the preceding train falls below the safe margin. [UCA-147]
(UCA-148) Train Operation Management System provides acceleration command when the train is operating within a speed restriction zone. [H-1, H-2, H-5]	(SC-148) Train Operation Management System should not provide acceleration command when the train is operating within a speed restriction zone. [UCA-148]

UCA	Safety Constraint
(UCA-149) Train Operation Management System provides an acceleration command too early before the train completely passes a speed restriction zone. [H-1, H-2, H-5]	(SC-149) Train Operation Management System shall provide an acceleration command within TBD seconds after the train completely passes a speed restriction zone. [UCA-149]
(UCA-150) Train Operation Management System applied an acceleration command too long after the train reaches the target speed. [H-1, H-2, H-5]	(SC-150) Train Operation Management System shall stop providing an acceleration command after the train reaches the target speed. [UCA-150]
(UCA-151) Train Operation Management System does not provide a deceleration command when the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(SC-151) Train Operation Management System shall provide a deceleration command when the running speed exceeds the safe allowable speed limit. [UCA-151]
(UCA-152) Train Operation Management System does not provide a deceleration command when the running speed exceeds the target speed on a run curve. [H-1, H-2, H-5]	(SC-152) Train Operation Management System shall provide a deceleration command when the running speed exceeds the target speed on a run curve. [UCA-152]
(UCA-153) Train Operation Management System does not provide a deceleration command when the distance to the preceding train falls below the safe margin. [H-1, H-2, H-5]	(SC-153) Train Operation Management System shall provide a deceleration command when the distance to the preceding train falls below the safe margin. [UCA-153]
(UCA-154) Train Operation Management System provides a deceleration command when the distance to the following train falls below the safe margin. [H-2, H-5]	(SC-154) Train Operation Management System should not provide deceleration command when the distance to the following train falls below the safe margin. [UCA-154]
(UCA-155) Train Operation Management System provides a deceleration command too late after the train enters a speed restriction zone. [H-1, H-2, H-5]	(SC-155) Train Operation Management System shall provide a deceleration command within TBD seconds after the train enters a speed restriction zone. [UCA-155]
(UCA-156) Train Operation Management System stopped a deceleration command too soon before the train reached the target speed. [H-1, H-2, H-5]	(SC-156) Train Operation Management System should not stop providing a deceleration command before the train reached the target speed. [UCA-156]
(UCA-157) Train Operation Management System does not provide an emergency brake	(SC-157) Train Operation Management System shall provide an emergency brake

UCA	Safety Constraint
command when an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	command when an emergency brake command is received from Control Room Operator. [UCA-157]
(UCA-158) Train Operation Management System provides an emergency brake command when a following train is approaching. [H-5]	(SC-158) Train Operation Management System should not provide an emergency brake command when a following train is approaching. [UCA-158]
(UCA-159) Train Operation Management System provides an emergency brake command too late after an emergency brake command is received from Control Room Operator. [H-1, H-2, H-3, H-5]	(SC-159) Train Operation Management System shall provide an emergency brake command within TBD seconds after an emergency brake command is received from Control Room Operator. [UCA-159]
(UCA-160) Train Operation Management System stopped an emergency brake command too soon before the train stopped completely. [H-1, H-2, H-3, H-5]	(SC-160) Train Operation Management System should not stop providing an emergency brake command before the train stopped completely. [UCA-160]
(UCA-161) Train Operation Management System does not provide a landing gear deploy request when the train enters wheel running mode. [H-5]	(SC-161) Train Operation Management System shall provide a landing gear deploy request when the train enters the wheel running mode. [UCA-161]
(UCA-162) Train Operation Management System provides a landing gear deploy request when the train is in levitation running mode. [H-2, H-5]	(SC-162) Train Operation Management System should not provide a landing gear deploy request when the train is in the levitation running mode. [UCA-162]
(UCA-163) Train Operation Management System provides a landing gear deploy request too late after the train's speed falls below 75 miles per hour (the threshold for the wheel running mode). [H-5]	(SC-163) Train Operation Management System shall provide a landing gear deploy request within TB seconds after the train's speed falls below 75 miles per hour (the threshold for the wheel running mode). [UCA-163]
(UCA-164) Train Operation Management System stopped a landing gear deploy request too soon before the landing gear was fully deployed. [H-5]	(SC-164) Train Operation Management System should not stop providing a landing gear deploy request before the landing gear was fully deployed. [UCA-164]
(UCA-165) Train Operation Management System does not provide a landing gear retract	(SC-165) Train Operation Management System shall provide a landing gear retract

UCA	Safety Constraint
request when the train is in levitation running mode. [H-2, H-5]	request when the train is in levitation running mode. [UCA-165]
(UCA-166) Train Operation Management System provides a landing gear retract request when the train is in wheel running mode. [H-5]	(SC-166) Train Operation Management System should not provide a landing gear retract request when the train is in wheel running mode. [UCA-166]
(UCA-167) Train Operation Management System provides a landing gear retract request when the train stops at the station. [H-3, H-4, H-5]	(SC-167) Train Operation Management System should not provide a landing gear retract request when the train stops at the station. [UCA-167]
(UCA-168) Train Operation Management System provides a landing gear retract request too late after the train's speed exceeds 75 miles per hour (the threshold for the levitation running mode). [H-5]	(SC-168) Train Operation Management System shall provide a landing gear retract request within TBD seconds after the train's speed exceeds 75 miles per hour (the threshold for the levitation running mode). [UCA-168]
(UCA-169) Train Operation Management System stopped a landing gear retract request too soon before the landing gear was fully retracted. [H-5]	(SC-169) Train Operation Management System stopped a landing gear retract request too soon before the landing gear was fully retracted. [UCA-169]
(UCA-170) Drive Control System does not provide a target current command when the running speed does not keep the target speed. [H-1, H-2, H-5]	(SC-170) Drive Control System shall provide a target current command when the running speed does not keep the target speed. [UCA-170]
(UCA-171) Drive Control System provides a target current command when personnel are entering the guideway for emergency maintenance. [H-5]	(SC-171) Drive Control System should not provide a target current command when personnel are entering the guideway for emergency maintenance. [UCA-171]
(UCA-172) Drive Control System provides a target current command too early before the calculation of the current value and phase is complete. [H-1, H-2, H-5]	(SC-172) Drive Control System shall provide a target current command within TBD seconds after the calculation of the current value and phase is complete. [UCA-172]
(UCA-173) Drive Control System stopped a target current command too soon before the train's speed reached the target speed. [H-1, H-2, H-5]	(SC-173) Drive Control System should not stop providing a target current command before the train's speed reached the target speed. [UCA-173]

UCA	Safety Constraint
(UCA-174) Safety Control System does not provide an emergency brake command when traveling above the safe allowable speed limit. [H-1, H-2, H-5]	(SC-174) Safety Control System shall provide an emergency brake command when traveling above the safe allowable speed limit. [UCA-174]
(UCA-175) Safety Control System does not provide an emergency brake command when an emergency brake command is initiated by Control Room Operator [H-1, H-2, H-3, H-5]	(SC-175) Safety Control System shall provide an emergency brake command when an emergency brake command is initiated by Control Room Operator [UCA-175]
(UCA-176) Safety Control System provides an emergency brake command when a following train is approaching. [H-5]	(SC-176) Safety Control System should not provide an emergency brake command when a following train is approaching. [UCA-176]
(UCA-177) Safety Control System provides an emergency brake command too late after the running speed exceeds the safe allowable speed limit. [H-1, H-2, H-5]	(SC-177) Safety Control System shall provide an emergency brake command within TBD seconds after the running speed exceeds the safe allowable speed limit. [UCA-177]
(UCA-178) Safety Control System stopped an emergency brake command too soon before the train completely stopped. [H-2, H-5]	(SC-178) Safety Control System should not stop providing an emergency brake command before the train completely stopped. [UCA-178]
(UCA-179) Safety Control System does not provide a door open enable when the door-open condition[3] is met and passenger evacuation is necessary. [H-3]	(SC-179) Safety Control System shall provide a door open enable when the door-open condition[3] is met and passenger evacuation is necessary. [UCA-179]
(UCA-180) Safety Control System provides a door open enable when the door-open condition[3] is not met. [H-4]	(SC-180) Safety Control System should not provide a door open enable when the door-open condition[3] is not met. [UCA-180]
(UCA-181) Safety Control System provides a door open enable too early before confirming whether the door-open condition[3] is met. [H-4]	(SC-181) Safety Control System shall provide a door open enable within TBD seconds after confirming whether the door-open condition[3] is met. [UCA-181]
(UCA-182) Safety Control System applied a door open enable too long after the door-open condition[3] was no longer met. [H-4]	(SC-182) Safety Control System shall stop providing a door open enable after the door-open condition[3] was no longer met. [UCA-182]

UCA	Safety Constraint
(UCA-183) Safety Control System does not provide a door close enable when the door-close condition[4] is met. [H-4, H-5]	(SC-183) Safety Control System shall provide a door close enable when the door-close condition[4] is met. [UCA-183]
(UCA-184) Safety Control System provides a door close enable when the door-close condition[4] is not met. [H-4]	(SC-184) Safety Control System should not provide a door close enable when the door-close condition[4] is not met. [UCA-184]
(UCA-185) Safety Control System provides a door close enable when passenger evacuation is necessary. [H-3]	(SC-185) Safety Control System should not provide a door close enable when passenger evacuation is necessary. [UCA-185]
(UCA-186) Safety Control System provides a door close enable too early before confirming whether the door-close condition[4] is met. [H-4]	(SC-186) Safety Control System shall provide a door close enable within TBD seconds after confirming whether the door-close condition[4] is met. [UCA-186]
(UCA-187) Safety Control System applied a door close enable too long after the door-close condition[4] was no longer met. [H-4]	(SC-187) Safety Control System shall stop providing a door close enable after the door-close condition[4] was no longer met. [UCA-187]
(UCA-188) Safety Control System does not provide a landing gear deploy enable when the wheel-running condition[5] is met. [H-5]	(SC-188) Safety Control System shall provide a landing gear deploy enable when the wheel-running condition[5] is met. [UCA-188]
(UCA-189) Safety Control System provides a landing gear deploy enable when the wheel-running condition[5] is not met. [H-5]	(SC-189) Safety Control System should not provide a landing gear deploy enable when the wheel-running condition[5] is not met. [UCA-189]
(UCA-190) Safety Control System provides a landing gear deploy enable too early before confirming whether the wheel-running condition[5] is met. [H-5]	(SC-190) Safety Control System shall provide a landing gear deploy enable within TBD seconds after confirming whether the wheel-running condition[5] is met. [UCA-190]
(UCA-191) Safety Control System applied a landing gear deploy enable too long after the wheel-running condition[5] was no longer met. [H-5]	(SC-191) Safety Control System shall stop providing a landing gear deploy enable after the wheel-running condition[5] was no longer met. [UCA-191]

UCA	Safety Constraint
(UCA-192) Safety Control System does not provide a landing gear retract enable when the levitation-running condition[6] is met. [H-2, H-5]	(SC-192) Safety Control System shall provide a landing gear retract enable when the levitation-running condition[6] is met. [UCA-192]
(UCA-193) Safety Control System provides a landing gear retract enable when the levitation-running condition[6] is not met. [H-5]	(SC-193) Safety Control System should not provide a landing gear retract enable when the levitation-running condition[6] is not met. [UCA-193]
(UCA-194) Safety Control System provides a landing gear retract enable too early before confirming whether the levitation-running condition[6] is met. [H-5]	(SC-194) Safety Control System shall provide a landing gear retract enable within TBD seconds after confirming whether the levitation-running condition[6] is met. [UCA-194]
(UCA-195) Safety Control System applied a landing gear retract enable too long after the levitation-running condition[6] was no longer met. [H-5]	(SC-195) Safety Control System shall stop providing a landing gear retract enable after the levitation-running condition[6] was no longer met. [UCA-195]
(UCA-196) Onboard Train Control System does not provide a brake actuation when the regenerative brake is insufficient. [H-1, H-2, H-5]	(SC-196) Onboard Train Control System shall provide a brake actuation when the regenerative brake is insufficient. [UCA-196]
(UCA-197) Onboard Train Control System does not provide a brake actuation when an emergency brake command has been received. [H-1, H-2, H-5]	(SC-197) Onboard Train Control System shall provide a brake actuation when an emergency brake command has been received. [UCA-197]
(UCA-198) Onboard Train Control System provides a brake actuation when the train is operating on an icy guideway. [H-1, H-2, H-5]	(SC-198) Onboard Train Control System should not provide a brake actuation when the train is operating on an icy guideway. [UCA-198]
(UCA-199) Onboard Train Control System provides a brake actuation too late after an emergency brake command has been received. [H-1, H-2, H-5]	(SC-199) Onboard Train Control System shall provide a brake actuation within TBD seconds after an emergency brake command has been received. [UCA-199]
(UCA-200) Onboard Train Control System stopped a brake actuation too soon before the train completely stopped. [H-1, H-5]	(SC-200) Onboard Train Control System should not stop providing a brake actuation

UCA	Safety Constraint
	before the train completely stopped. [UCA-200]
(UCA-201) Onboard Train Control System does not provide a door actuation when receiving a door open/close enable. [H-3, H-4]	(SC-201) Onboard Train Control System shall provide a door actuation when receiving a door open/close enable. [UCA-201]
(UCA-202) Onboard Train Control System does not provide a door actuation when a passenger is caught in the door. [H-4]	(SC-202) Onboard Train Control System shall provide a door actuation when a passenger is caught in the door. [UCA-202]
(UCA-203) Onboard Train Control System provides a door actuation when passenger boarding or alighting is still in progress. [H-3, H-4]	(SC-203) Onboard Train Control System should not provide a door actuation when passenger boarding or alighting is still in progress. [UCA-203]
(UCA-204) Onboard Train Control System provides a door actuation when the train is still in motion. [H-4]	(SC-204) Onboard Train Control System should not provide a door actuation when the train is still in motion. [UCA-204]
(UCA-205) Onboard Train Control System provides a door actuation too early before receiving a door open/close enable. [H-3, H-4]	(SC-205) Onboard Train Control System shall provide a door actuation within TBD seconds after receiving a door open/close enable. [UCA-205]
(UCA-206) Onboard Train Control System applied a door actuation too long after the rescue of a passenger caught in the doors was complete. [H-3, H-4]	(SC-206) Onboard Train Control System shall stop providing a door actuation after the rescue of a passenger caught in the doors was complete. [UCA-206]
(UCA-207) Onboard Train Control System does not provide a landing gear actuation when receiving a landing gear deploy/retract enable. [H-5]	(SC-207) Onboard Train Control System shall provide a landing gear actuation when receiving a landing gear deploy/retract enable. [UCA-207]
(UCA-208) Onboard Train Control System provides a landing gear actuation when the train's speed is not in the threshold range. [H-5]	(SC-208) Onboard Train Control System should not provide a landing gear actuation when the train's speed is not in the threshold range. [UCA-208]
(UCA-209) Onboard Train Control System provides a landing gear actuation too late after receiving a landing gear deploy/retract enable. [H-5]	(SC-209) Onboard Train Control System shall provide a landing gear actuation within TBD seconds after receiving a landing gear deploy/retract enable. [UCA-209]

UCA	Safety Constraint
(UCA-210) Onboard Train Control System stopped a landing gear actuation too soon before the landing gear touched the ground. [H-5]	(SC-210) Onboard Train Control System should not stop providing a landing gear actuation before the landing gear touched the ground. [UCA-210]

References

[1] Central Japan Railway Company, “Fact sheets 2025.” May 2025. [Online]. Available: https://global.jr-central.co.jp/en/company/ir/factsheets/

[2] Central Japan Railway Company, “Annual Report 2025.” 2025. [Online]. Available: https://global.jr-central.co.jp/en/company/ir/annualreport/

[3] Central Japan Railway Company, “Passenger Volume Report 2026.” [Online]. Available: https://global.jr-central.co.jp/en/company/ir/passenger-volume/

[4] Y. Fukushima, T. Nishikawa, and Y. Kano, “High probability of successive occurrence of Nankai megathrust earthquakes,” *Sci. Rep.*, vol. 13, no. 1, p. 63, Jan. 2023, doi: 10.1038/s41598-022-26455-w.

[5] Central Japan Railway Company, “THE REVIEW of Superconducting Maglev.” [Online]. Available: https://global.jr-central.co.jp/en/company/_pdf/superconducting_maglev.pdf

[6] N. G. Leveson, *Engineering a safer world: systems thinking applied to safety*. in Engineering systems. Cambridge (Mass.): MIT press, 2011.

[7] H. W. Heinrich, *Industrial accident prevention; a scientific approach,* 1st ed. New York: McGraw-Hill book company, inc., 1931.

[8] H. W. Heinrich, “The origin of accidents,” in *Transactions, 1928*, 1928, pp. 127-131.

[9] J. T. Reason, *Human Error*. Cambridge [England]: Cambridge University Press, 1990.

[10] J. Reason, “Human error: models and management,” vol. 320, no. 7237, pp. 768–770, Mar. 2000, doi: 10.1136/bmj.320.7237.768.

[11] N. Leveson, “A new accident model for engineering safer systems,” *Saf. Sci.*, vol. 42, no. 4, pp. 237–270, Apr. 2004, doi: 10.1016/S0925-7535(03)00047-X.

[12] U.S. Military, “Procedures for Performing a Failure Mode, Effects and Criticality Analysis,” Department of Defense, MIL-P-1629, 1949.

[13] Vesely, W. E., Goldberg, F. F., Roberts, N. H., and Haasl, D. F., “Fault Tree Handbook,” U.S. Nuclear Regulatory Commission, Washington, DC, USA, NUREG-0492, 1981.

[14] Leveson, Nancy G. and Thomas, John P., “STPA Handbook,” Massachusetts Institute of Technology, Cambridge, MA, USA, 2018. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_Handbook.pdf

[15] R. Cabosky, “Application of Hierarchy to STPA: A Human Factors Study on Vehicle Automation,” Master’s thesis, Massachusetts Institute of Technology, Cambridge, MA, 2020.

[16] R. Bowers and Thomas, John P., “SAFETY IMPLICATIONS OF AUTONOMOUS VEHICLES – SYSTEM THEORETIC PROCESS ANALYSIS APPLIED TO A NEURAL NETWORK-CONTROLLED AIRCRAFT,” presented at the 54th Annual International Symposium of the Society of Flight Test Engineers, Patuxent River, MD, USA, 2023.

[17] B. R. Abrecht, “SYSTEMS THEORETIC PROCESS ANALYSIS APPLIED TO AN OFFSHORE SUPPLY VESSEL DYNAMIC POSITIONING SYSTEM,” Master’s thesis, Massachusetts Institute of Technology, Cambridge, MA, 2016.

[18] W. Suzuki, “Safety Analysis and Design Improvement for Semi-Automatic Train Operation (STO) in High-Speed Rail Using STPA,” Master’s thesis, Massachusetts Institute of Technology, Cambridge, MA, 2025.

[19] Oshima, Hiroshi, “Overview of Superconducting Maglev Technology (in Japanese),” 日本機会学会誌, vol. 120, no. 1179, pp. 25–28, 2017.

[20] Takayama, Masayuki, Usami, Kazuo, Sanjo, Kazuhiro, Kasuya, Naohiro, and Miyairi, Komei, “Drive Control System for Yamanashi Maglev Test Line (in Japanese),” *Hitachi Hyoron*, vol. 79, no. 2, pp. 47–52, 1997.

[21] Superconducting Magnetic Levitation Railway Practical Technology Evaluation Committee, “Practical Technology Evaluation of Superconducting Magnetic Levitation Railway (in Japanese),” Document 2, 2009.

[22] John P. Thomas, “Developing STPA Scenarios,” MIT STAMP workshop, 2024. [Online]. Available: https://psas.scripts.mit.edu/home/wp- content/uploads/2024/STPA-Scenarios-New-Approach.pdf

[23] United States Department of Defense, “MIL-STD-882E: Department of Defense Standard Practice: System Safety,” Department of Defense, United States of America, MIL-STD-882E, May 2012.