Application of a Systems-Theoretic Approach to Risk Analysis of High-speed Rail Project Management in the US

by

Soshi Kawakami

M.E., Mechanical Engineering, Kyoto University, 2005
B.E., Mechanical Engineering, Kyoto University, 2003

Submitted to the Engineering Systems Division
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering Systems
at the
Massachusetts Institute of Technology

JUNE 2014

Signature of Author: _____
Engineering Systems Division
May 9, 2014

Certified by: _____
Nancy G. Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

Certified by: _____
Joseph M. Sussman
JR East Professor of Civil and Environmental Engineering and Engineering Systems
Thesis Supervisor

Accepted by: _____
Richard Larson
Mitsui Professor of Engineering Systems
Chair, ESD Education Committee

Application of a Systems-Theoretic Approach to Risk Analysis of High-speed Rail Project Management in the US

by

Soshi Kawakami

Submitted to the Engineering Systems Division
on May 9, 2014 in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering Systems

ABSTRACT

High-speed rail (HSR) is drawing attention as an environmentally-friendly transportation mode, and is expected to be a solution for sociotechnical transportation issues in many societies. Currently, its market has been rapidly expanding all over the world. In the US, the *Federal Railroad Administration* (FRA) released a strategic vision to develop new HSRs in 2008, specifically focusing on 10 corridors, including the Northeast Corridor (NEC) from Boston to Washington D.C. With such rapid growth, safety is a growing concern in HSR projects; in fact, there have been two HSR accidents over the past three years. In developing a new HSR system, it is crucial to conduct risk analysis based on lessons learned from these past accidents. Furthermore, for risk analysis of complex sociotechnical systems such as HSR systems, a holistic system-safety approach focusing not only on physical domains but also on institutional levels is essential. With these perspectives, this research proposes a new system-based safety risk analysis methodology for complex sociotechnical systems. This methodology is based on the system safety approach, called STAMP (*System-Theoretic Accident Model and Processes*). As a case study, the proposed HSR project in the NEC is analyzed by this methodology. This methodology includes steps of conducting STAMP-based accident analysis, developing a safety model of the HSR system in the NEC, and analyzing safety risks of it based on lessons learned from the analyzed accidents, with a specific focus on the institutional structure. As a result of this analysis, 58 NEC-specific risks are identified, and with them, weaknesses of safety-related regulations applied to the project are discussed. Additionally, this research introduces *System Dynamics* to analyze further detailed causal relations of the identified risks and discusses its potential usage for risk analysis. Thus, this thesis research concludes with specific recommendations about safety management in the project in the NEC, making a point that the proposed methodology can be valuable for the actual project processes as a "safety-guided institutional design" tool.

Thesis Supervisor: Nancy G. Leveson
Title: Professor of Aeronautics and Astronautics and Engineering Systems

Thesis Supervisor: Joseph M. Sussman
Title: JR East Professor of Civil and Environmental Engineering and Engineering Systems

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my thesis advisor, Professor Nancy G. Leveson, who has supported this thesis work and has kept me inspired with her novel, insightful, and immense views on safety and engineering systems. Her STAMP-based approach has drastically changed my view toward safety. Without her guidance and persistent help, I would not fulfill my academic goal at the MIT.

I would like to express my great appreciation to the other thesis advisor, Professor Joseph M. Sussman, who has kept me highly motivated throughout my thesis work with his patient and enthusiastic support whilst allowing me the room to work in my own way. His broad and deep knowledge about transportation has dramatically broadened my perspective on railway system and management, which I believe will drive my productivity in my future career as a railway system integrator in international fields.

In my daily work, I have been blessed with friendly and cheerful fellow researchers: I thank Ryan J. Westrom, S. Joel Carlson, Iori Mori, Andrés F. Archila, Maite Peña-Alcaraz, Naomi Stein, Guineng Chen, Rebecca J. Heywood, Samuel Levy, Heather Jones, Evelien van der Hurk, and Aleksandr Prodan in Regional Transportation Planning and High-speed Rail Research Group for the stimulating discussions about transportation issues, and I thank Dajiang Suo, Seth Placke, Cameron Thornberry, Cody Harrison Fleming, John Douglas Helferich, John P. Thomas, Nicholas Connor Dunn, William Edward Young, Dan Montes, Adam David Williams, Kip Edward Johnson, Aubrey Lynn Samost, Jonas Bianchini Fulindi, Meaghan Marie Oneil, and Nicholas Chung in Systems Engineering Research Laboratory for giving insightful advice on my safety analysis.

Finally, I would like to express my heartfelt appreciation to my family: my parents Masakazu and Hitomi, my siblings Chihiro and Keishi, my wife Shizu, my daughter Sae, and my newborn son Hiroaki. In particular, I would like to show my best gratitude and love to Shizu, who gave birth to Hiroaki on October 10, 2013. Although the delivery unfortunately enforced her to go through a severe surgery, she always motivated me with sacrificing support and love even after the tough time. Shizu's inexhaustible support, Sae's cheerful smile, and Hiroaki's great birth gave me unmeasurable energy to accomplish this thesis. In acknowledgment of their contribution and love, I dedicate this thesis to Shizu, Sae, and Hiroaki.

Soshi Kawakami
Cambridge, Massachusetts
May 2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Appendix Figure

LIST OF ACRONYMS AND ABBREVIATIONS

APTA	American Public Transit Association
ARRA	American Recovery and Reinvestment Act
ATP	Automatic Train Protection
AWS	Automatic Warning System
BNSF	Burlington Northern and Santa Fe Railway
BR	British Railway
C3RS	Confidential Close Call Reporting System
CALPRIG	California Public Interest Research Group
CAST	Causal Analysis based on STAMP
CFR	Code of Federal Regulations
CHSRA	California High Speed Rail Authority
CMS RA	Common Safety Methods for Risk Assessment
COTS	Commercial Off The Shelf
CRSC	China Railway Signal & Communication Corporation
CRSDC	Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.
CSM	Common Safety Method
CTC	Centralized Train Control
CTSC	Capture, Transport and storage of CO2
DB	Deutsche Bundesbahn
DBM	Design/Build/Maintenance
DBOM	Design/Build/Operate/Maintenance
DOT	Department of Transportation
DVT	Driving Van Trailer
EIS	Environmental Impact Statement
EN	European Norm
ERA	European Railway Agency
EU	European Union
FAA	Federal Aviation Administration
FMEA	Failure Mode Effect Analysis
FMECA	Failure Mode and Effect Criticality Analysis
FRA	Federal Railroad Administration
FTA	Federal Transit Administration or Fault Tree Analysis
GAO	United States Government Accountability Office
GCC	Gauge Corner Cracking
GNER	Great North Eastern Railway
HSE	Health and Safety Executive
HSR	High -speed Rail
IEC	International Electrotechnical Commission

IM	Infrastructure Manager
ISO	International Organization for Standardization
ITA	Independent Technical Authority
MK4	Mark 4
MOR	Ministry of Railway
NDA	Non Descried Alarm
NEC	Northeast Corridor
NEC HSR	the new High Speed Rail (project) in the Northeast Corridor in the US
NECSA	NEC Systems Authority
NEPA	National Environmental Policy Act
NPRM	Notice of Proposed Regulation Making
OECD	Organization for Economic Co-operation and Development
ORR	Office of Rail Regulation
PPP	Public-private Partnership
PRA	Probabilistic Risk Assessment
PTC	Positive Train Control
QRA	Quantitative Risk Assessment
RCF	Rolling Contact Fatigue
RFF	French Rail Network
RFP	Request For Proposal
RGS	Rail Group Standard
ROW	Right-of –way
RSAC	Railroad Safety Advisory Committee
RSIA	Rail Safety Improvement Act
RSSD	Railtrack Safety and Standards Directorate
SCMAGLEV	Superconducting Magnetic Levitation System
SD	System Dynamics
SDP	Service Development Plan
SMS	Safety Management Systems
SNCF	National Society of French Railways
SPP	System Safety Program
SSMP	Safety and Security Management Plan
SSPP	System Safety Program Plan
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
TCC	Train Control Center
TNEM	The Northeast Maglev
TOC	Train Operating Company
UIC	International Union of Railways
UP	Union Pacific Railroad

CHAPTER 1. INTRODUCTION

1.1 Motivation and Purpose

- **Rapid market growth**

Today, high-speed rail (HSR) is drawing attention as an environmentally-friendly transportation mode, and is expected to be a solution for sociotechnical[1] transportation issues in many societies by providing capacity increase and economic benefit for key corridors. HSR systems are rapidly expanding all over the world; specifically, 15 countries are operating commercial HSRs in the world as of May 2014, and the total global HSR network size is estimated to double in the next 10 years [1]. With such rapid growth and widespread use, safety of these systems is a growing concern.

- **HSR accidents**

It is widely believed that railways, including HSRs, are safe systems due to their technological maturity. However, there are still many railway accidents every year all around the world. Although HSRs have had only three fatal accidents in their 50-year history, two of them occurred over the past three years as HSR systems in operation have grown. Specifically, in 2011, a collision of two high speed trains occurred in Wenzhou, China, killing 40 passengers (*Wenzhou train collision*). A flaw in the signal systems and several managerial problems were behind the tragedy [2]. In 2013, a disastrous derailment occurred in Santiago de Compostela, Spain, killing 79 passengers (*Santiago de Compostela derailment*) [3]. The high-speed train was running on a track designed for conventional trains at about 190 km/h, which was 110 km/h-higher than the regulated speed for the curve. The details of the causes for this accident are still under investigation as of May 2014. These accidents have reminded HSR planners and operators of the importance and difficulty of continuously managing safety for a large-scale system such as HSR.

- **Importance of system-based perspectives**

This thesis research focuses on how to manage safety risks of a complex system such as HSR in its development as well as operating processes. Specifically, emerging HSR projects in the US are discussed as a case study. This work will show that one of the keys to successful risk management is how lessons learned from these past accidents are effectively reflected to future management. However, this process is challenging due to the complexity of railway systems, which include not only a technical physical domain

[1] In "sociotechnical" system, technology plays a central role as does the social context within which the system is operating [122].

but also institutional domains such as labor management, regulation, and coordination among diverse entities and stakeholders involved in the operation. In fact, the *Santiago de Compostela derailment* was not prevented in spite of the fact that there were many past railway accidents that had similar types of operational flaws as crucial accident causes to those of the *Santiago de Compostela derailment*, such as the *Amagasaki rail crash* in Japan in 2005 and *Valencia Metro derailment* in Spain in 2006.
The problem of system complexity can be clearly seen in the Chinese HSR accident. There were systematic flaws in the Chinese rail industry such as inappropriate safety policy/regulation, the lack of safety education and training, and missing safety culture [4][5]. As shown in this thesis, in order to acquire true lessons from accidents, it is crucial to analyze complex causal factors leading to accidents from a system-based perspective, not to try only to find a single root cause. "System" in this context consists of not only a physical level such as rolling stock, signal systems, or another infrastructure, but also corporate-management levels such as operation planning/control and safety training, and institutional levels such as the industrial structure (see Section 1.3) and safety-related interactions of entities involved in the industry; e.g., the *International Union of Railways* (UIC) more specifically defines a HSR as a complex system that is comprised of 10 different elements [6]. Another example of inadequate awareness of system complexity can be seen in CNN's editorial in July 2013 claiming about the Spanish HSR accident that, "The good news is that the United States, whose rail system already has a strong safety record, is becoming safer thanks to investments being made by public and private entities. The *Federal Railroad Administration* mandated last year that by 2015 all intercity tracks be equipped with train control systems [PTC, explained in Section 1.2] that would prevent crashes such as this week's accident in Spain [7]." This reasoning is defective in that the author focuses on only one component of the total system, which is one function of the signal system. For instance, there is a possibility that the regulation of the signal system might have a fatal flaw, or knowledge of the workers about the function or risk of the signal system might not be sufficient. Even if the US authority uses a high-performance signal system, these problems could drive the US rail industry to an unsafe state.

Additionally, in applying system-based lessons learned from past accidents to HSR projects in the US, it is essential to understand the difference of the "systems" between the US and countries that had the accidents because different HSR corridors have different institutional structures [8][9]. System attributes of HSRs depend on how these system elements such as technologies, organizations, people, and regulations are integrated and how they interact, coping with local rules, culture, and nationality.

- **Purpose and structure of this thesis**

The purpose of this research is thus to propose a system-based safety risk analysis methodology based on lessons learned from past accidents for complex, large-scale, sociotechnical systems such as HSR systems. The method used in this work is based on the STAMP (*System-Theoretic Accident Model and Processes*) theory proposed by Leveson [10][11]. One of the key ideas in this theory is that *safety is an emergent property*, which means that safety could be threatened by any lack of enforcement of safety constraints among system components in the entire system as well as by a single component error [11][12]. The details about this theory and methodology are explained in Chapter 2. As a case study, the new HSR project in the northeast corridor in the US (NEC HSR) is then analyzed by the proposed methodology. The proposed methodology includes steps of analyzing past accidents and acquiring system-based lessons (described in Chapter 3), developing a safety model of the NEC HSR (described in Chapter 4), and analyzing safety risks of the NEC HSR based on the lessons learned (described in Chapter 5); for the NEC HSR, it is crucial to incorporate past lessons and system-based perspectives in light of the US's limited experience in HSR operation and its unique complex institutional structure and regulation. The final goal of this research is to provide specific suggestions about safety management in the NEC HSR for project planners, based on the analysis results (Chapter 6). As a research background, the current situation of HSR development in the US is described in Section 1.2. Also, the main focus of this case study is the institutional level of the system; i.e., the risks related to detailed specifications about rolling stock or signal systems, or detailed operational processes or maintenance methods are not discussed. In Section 1.3, the interpretation of "institutional level" in this research is described in detail.

1.2 Background 1: High-speed rail and Rail Safety in the US

A HSR system is defined as a "specially built line for operation at 250km/h or more, or specially upgraded line for operation at 200km/h or more" according to UIC [13]. The first operation of HSR started in Japan in 1964, and subsequent HSR development occurred in Europe in the 1980's and 1990's. Today, typical maximum operation speed has reached around 320 km/h (200 mile/h), and this mature system with environmental-friendly features, compares favorably to air and highway transportation, and has been increasingly adopted in other areas to improve intercity connectivity and to accommodate future increases in transportation demand, with economic benefit expected in the surrounding regions.

The US is one of the countries that have a HSR in operation.[2] *Acela Express* is the only HSR in the US and is operated on the NEC from Boston to Washington D.C. In 2009, as required by the *American Recovery and Reinvestment Act* (ARRA), which was signed by President Barack Obama, the *Federal Railroad Administration* (FRA) released a strategic vision to develop new HSRs, specifically focusing on 10 corridors shown in Figure 1-1, including the NEC. While some of the plans such as in Ohio and Florida have already been abandoned [14][15], the California corridor is scheduled to start its construction in 2014 [16]. Another promising project is the renewal of the NEC, for which FRA is now implementing an environmental assessment, called a Tier 1 *Environmental Impact Statement* (EIS) in accordance with NEPA (The *National Environmental Policy Act*, 1969), and *Service Development Plan* (SDP) to define alternatives for rail service improvements, evaluate their impact on the existing network and operations, and assess costs and benefits of the proposed plan [13][14]. While more than half of the US citizens are presumed to have an interest in using new HSRs according to a survey conducted by *American Public Transit Association* (APTA) in 2012 [19], their projects are, in fact, struggling with significant financial challenges in their planning processes.

[2] The definition of HSR in the US is different from that of UIC. HSRs are categorized into three groups (HSR Express, HSR Regional, and Emerging HSR) according to operational speed and typical distance between major cities that the HSR line connects [20].

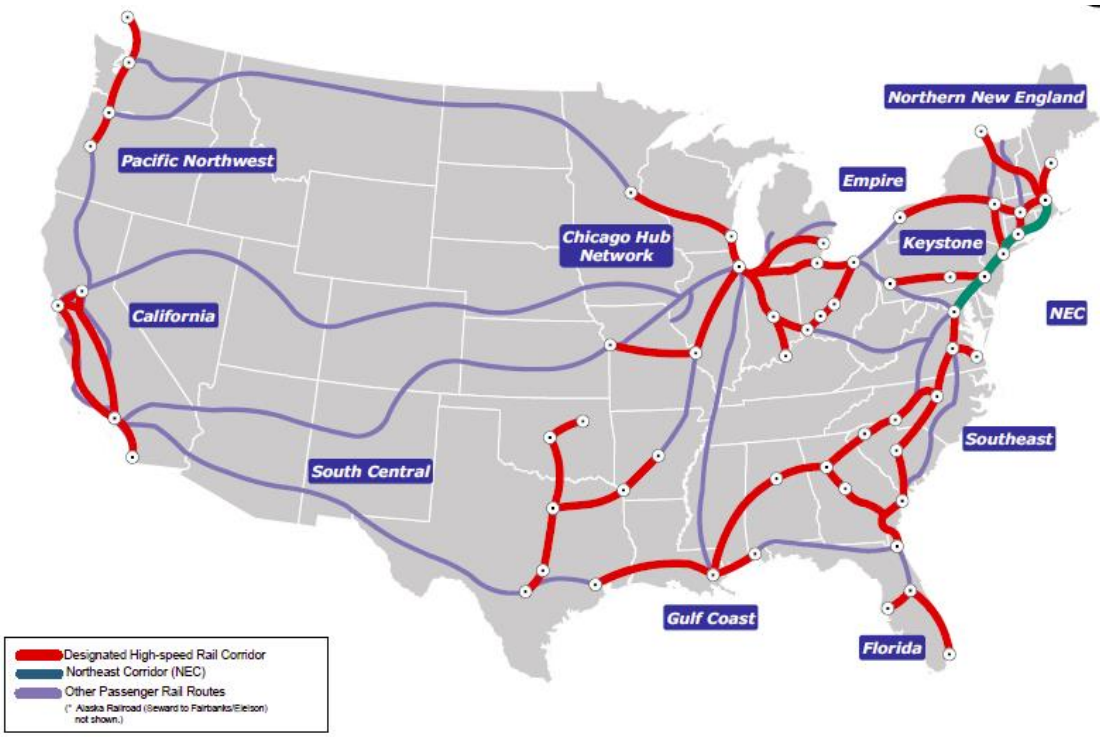

Figure 1-1 Designated HSR corridors and the NEC [20]

Overall, rail safety in the US has been gradually improving since 1980, as shown in Figure 1-2. The accident rate defined as the train accident rate per million train miles dropped by approximately 50 percent from 2004 to 2012. Despite the significant reduction in the accident rate, on average almost 300 people were injured and about ten people were killed in train accidents each year, from 2003 to 2012 [21]. The *Rail Safety Improvement Act in 2008* (RSIA) was enacted as a response to several rail accidents in the 2000s. The RSIA forces FRA to develop new safety regulations about rail safety such as implementation of a new signal system called *Positive Train Control* (PTC).

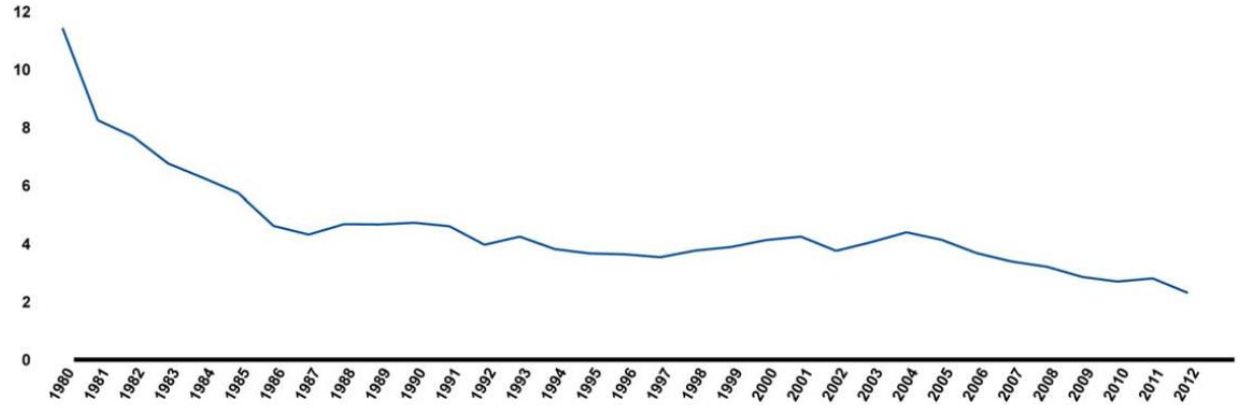

Figure 1-2 Train accident rate (per million train miles)

The rail industry in the US has been recently going through drastic changes in its safety management. For example, FRA issued the *High-speed Rail Safety Strategy* in 2009 [22]. This Safety Strategy laid out the challenges to be tackled for future HSR operation such as a high-quality signal system, new safety standard development, and rules for emergency operation. One of the aims of this strategy is to achieve uniformly safe service, regardless of operational speed. For this purpose, passenger services are categorized into several "tiers" according to their operational speeds, and different strategies or rules are planned to be applied to each tier [22]. In order to discuss HSR safety in the US, it is necessary to take into account the following three issues, which are also mentioned in the *HSR Safety Strategy*. These trends imply that safety management in the US HSR industry could become drastically different from that of any other region in the world.

- **Safety Standard on Crashworthiness**

  FRA announced in June 2013 that safety regulation about crashworthiness for passenger trains will be mitigated [23]. Without this mitigation, rolling stock for HSRs would have to have sufficient crashworthiness for front collision with freight trains. If the current regulation about crashworthiness were applied to new HSR trains, it would be difficult to directly apply international-quality HSR technologies from international suppliers such as Bombardier, Alston, Siemens, and Japanese manufacturers to HSRs in the US. Therefore, these suppliers and Amtrak, which is the current operator of *Acela Express* and one of the possible operators of the new HSR in the NEC, were strongly against the application of the current crashworthiness to HSRs. In the announcement, FRA referred to international-quality HSRs as "performance-based, service proven technology." The details of the new standards have not yet been clarified to the public as of May 2014. The NPRM (N*otice of Proposed Regulation Making*) that includes this revision is scheduled to be released soon.

- **Requirement for the Installment of Positive Train Control (PTC)**

  The RSIA in 2008 requires PTC technology to be installed on most of the US railroad network by December 15, 2015. This system uses GPS navigation to trace train movements, and the train receives information about its location and a safe zone to run (see Figure1-3). It is said that, with this system, the train can automatically stop or slow to prevent train-to-train collisions and derailments caused by excessive speed. Although the deadline of the installment might be extended, PTC is supposed to be installed in all of the new HSRs in the US [24].

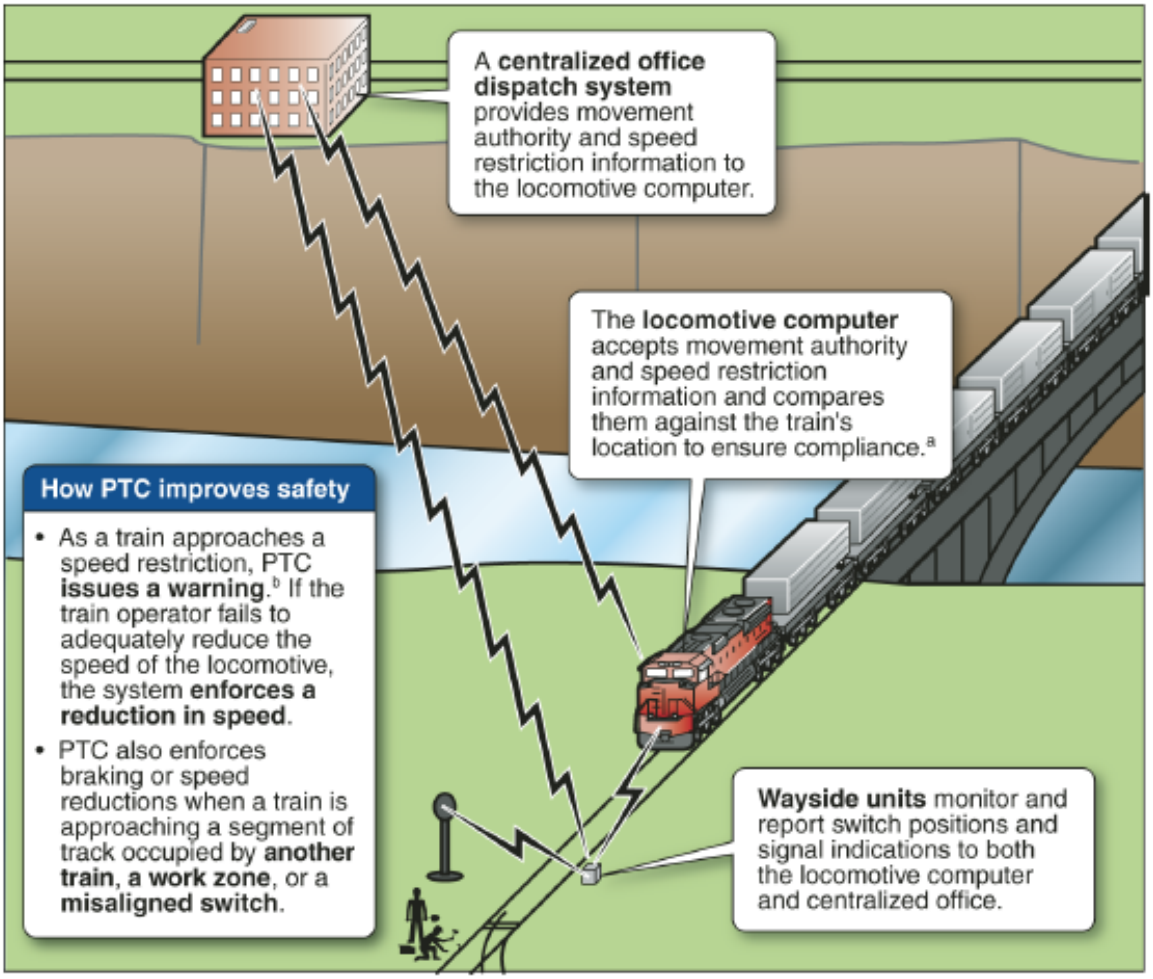

Figure 1-3 Basic operation of a Positive Train Control system (in the case of locomotive) [24]

- **System Safety Program (SSP)**

  This federal regulation published NPRM of this regulation, *49 CFR (Code of Federal Regulations) part 270 proposed rule*, in September 2012 [25]. This regulation aims to improve a safety level of the rail systems in operation and future HSR operations. The contents of the program are designed based on system safety approaches such as SMS (*safety management system*) of *Federal Aviation Administration* (FAA) [26]. This regulation requires commuter and intercity passenger railroads to develop and implement a S*ystem Safety Program plan* (SSP plan or SSPP) to improve the safety of their operations, involving contractors. SSP is one of the core approaches in FRA's safety strategy.

1.3 Background 2: Institutional Structure in Railway Industries

While safety management strategies and regulations for HSR systems in the US have been developed, institutional structures for them have not been determined yet. Specifically, the current NEC has a significantly complex institutional structure, and its future design is an important concern. From the STAMP-based system perspective, which is introduced in Chapter 2, different institutional structures would have different safety-related interactions among institutions, which are defined as system components in this research. Therefore, in analyzing safety risks of the NEC HSR, it is necessary to conduct the analysis in accordance with each possible institutional structure. The specific alternatives for the institutional structure of the NEC HSR are discussed in Chapter 4. This research specifically focuses on the following elements as key components to configure "institutional structure" in railway industries.

- **Vertical structure (vertical separation or vertical integration)**
  One key question in designing an institutional structure is whether rail infrastructure and train operations should be owned and operated by separate entities. This vertical separation of infrastructure ownership from the operation of services over the infrastructure was applied to network industries such as telecommunications and energy distribution at first, and afterward applied to railway industries mainly in Europe [27]. This structure typically adds complexity in administrative and regulatory activities, and economic costs to manage for institutional coordination [28], thereby possibly raising safety concerns due to the increased challenges of coordinating fragmented responsibilities. There are several definitions of vertical separation (or vertical integration) [29]–[31]. To specify the definition of vertical separation applied to the discussion on possible complex NEC HSR's institutional structures, this research introduce the nine responsibilities in railway services that Kurosaki defines as follows [9].

    1) Investment and ownership of infrastructure.
    2) Maintenance of tracks and infrastructure.
    3) Capacity allocations and timetabling.
    4) Route setting (daily traffic controlling and signaling).
    5) Investment and ownership of rolling stock.
    6) Maintenance of rolling stock.
    7) Daily operation of trains (train service running and crew roistering).
    8) Service marketing and ticket sales.
    9) Administrative regulations on safety, technology, services, fares, and so on.

Specifically, this research defines vertical separation as a situation in which the "above rail" functions, which are comprised of 5), 6), 7) and 8), are performed by a different, independent entity from the one taking "below rail" responsibilities of 1) - 4) or taking 2) - 4). As the *Fourth Railway Package* in EU permits[3], vertical separation includes the case in which a single holding company owns both "above rail" and "below rail" such as the cases of DB (*Deutsche Bundesbahn*) in Germany and SNCF[4] (*National Society of French Railways*) in France [32][33].

Also, based on this classification of railway responsibilities, this thesis research defines terminology about railway institutions, as shown in Table 1-1. There are various definitions used in practice, but this research uses *Regulator, Railroad, Train Operating Company* (TOC), *Infrastructure Manager* (IM), and *Infrastructure Owner*. TOCs take "above rail" responsibilities, and IMs take "below rail" responsibilities. "(x)" in the table represents the institution that has "(x)" in its column could take the responsibility designated by the "(x)". For example, Railroads could be institutions that take both "above and below rail" responsibilities in vertically integrated industries or take only "above rail" responsibilities in vertically separated responsibilities. Although *Infrastructure Owner* can have the same responsibilities as those of IMs, this research uses it together with IMs only when IMs do not have an infrastructure ownership, to show this clearly.

Table 1-1 Definitions of terminology about railway institutions in this research

		Regulator	Railroad (Railway Company)	Train Operating Company (Railway Undertaker)	Infrastructure Manager	Infrastructure Owner
1	Investment / ownership of infrastructure.		(x)		(x)	x
2	Maintenance of tracks and infrastructure.		(x)		x	(x)
3	Capacity allocations and timetabling.		(x)		x	(x)
4	Route setting		(x)		x	(x)
5	Investment / ownership of rolling stock.		x	x		
6	Maintenance of rolling stock.		x	x		
7	Daily operation of trains		x	x		
8	Service marketing and ticket sales.		x	x		
9	Administrative regulations	x				

[3] As of May 2014, the fourth railway package had been adopted by the *European Commission*, but not yet been approved by the *European Parliament* [32].

[4] France is initially regarded as fully separated. However, because third party access was not permitted for freight until 2007 and for domestic passenger services from 2010, vertical separation could have no impact on competition [123]. Also, *French Rail Network* (RFF) does not at the moment provide maintenance services or rail traffic control operations that are both done by *SNCF Infra*. Therefore, SNCF is regarded as a holding company with vertically separation.

- **Dedicated track or shared track**

  Tokaido Shinkansen in Japan is famous for its dedicated operation for HSR, which means no other passenger operations and freight operation are allowed on the track. By contrast, most of the HSR tracks in Europe as well as the current NEC are shared with other train operations. This decision is one of the critical aspects for rail safety from both technical and institutional standpoints, and significantly important in the NEC, where many different types of service (commuter, intercity passenger, and freight) wish to access the same track, as they are currently doing.

- **Private, public, or both**

  While most of the HSR railroads in Japan are privatized, most of the other regions in the world have state-owned agencies for HSR operations. Also, *Public-private partnerships* (PPP) have also been playing an important role in the construction and operation of HSRs [34]. In the US, while freight railroads such as UP (*Union Pacific Railroad*) and BNSF (*Burlington Northern and Santa Fe Railway*) are private companies, passenger railroads such as Amtrak are mostly public agencies. With respect to system safety, this aspect could lead to a significant difference of safety management or regulation required for the industries, due to the difference of their priorities in management, business goals, or level of responsibilities for local societies [35][36].

- **Market Competition**

  The last element is market competition. According to OECD (*Organization for Economic Co-operation and Development*), modes of market competition of rail sectors are grouped as shown in Table 1-2 [37]. This research focuses only on "Intra-modal" competition defined in Table 1-2.

  To date, only Italy has a competitive HSR market between a public *Train Operating Company (TOC)* and a private *TOC*; the rival private operator, *NTV*, began large-scale services in competition with the state-owned incumbent, *Trenitalia*, in 2012. This entry has brought about a strong increase in service levels [37]. Market competition could lead to improvement of the service qualities, including safety, but at the same time, losers of market competition could have difficulty managing an appropriate balance between cost reduction and safety.

Table 1-2 Definition of market competition of rail sectors [37]

Inter-modal		Air, water and road (trucks and cars) transport are all potential alternatives to the use of the railway. The extent of substitutability between these modes of transport, and hence the level of inter-modal competition railway services face, depends on the geographic, demographic and economic features of different countries and the availability of these different modes. It also varies considerably between freight and passenger services.
Intra-modal	**side-by-side competition**	Side-by-side, or parallel, competition is a form of "competition in the market" that takes place where competing vertically integrated railroads have their own infrastructure to serve a given market pair. This form of competition is prevalent in North America, where all major market areas are served by competing carriers, but it is absent in Europe.
	end-to-end competition	End–to-end competition is also a form of "competition in the market" that happens between vertically integrated railroads, but it concerns market pairs where their networks do not completely overlap, but compete in providing one leg of a multi-modal journey. This form of competition tends to be more effective for freight than for rail passenger services, as passengers tend to be more time-sensitive.
	competition between tenants and owner or among tenants	Competition can also take place on the same railroad between different service providers, either all tenants or tenant(s) and owner. This kind of competition can happen in a vertically integrated railroad, where tenants enter a market where the owner of the railroad already provides services, or in vertically separated systems, where the owner of the infrastructure either is not involved in the provision of freight and passenger services or is separated from its downstream operation.
	competition for the market	Competition can also be for the market, rather than in the market, when providers of rail services bid to obtain an exclusive franchise on a specific destination pair. Tenders are especially common where train services are subsidised because, when properly designed and managed, competition between bidders can significantly reduce the amount of the financial support needed.

Safety risk analysis of the NEC HSR must handle these complex backgrounds of the project. To meet this requirement, this research adopts a STAMP-based approach. In Chapter 2, the basic concepts of STAMP and the STAMP-based risk analysis methodology are described.

CHAPTER 2. METHODOLOGY

STAMP is the core theory applied to the methodology that this thesis proposes. Its key perspectives are introduced in Section 2.1, and compared to those of conventional safety analysis techniques. This is followed by a detailed explanation of the specific steps in the proposed methodology in Section 2.2.

2.1 STAMP-based Analysis

In Section 2.1.1, fundamental terminology is defined. In Section 2.1.2, traditional risk analysis tools and accident models are explained. In Section 2.1.3, the trend of risk analysis applied to rail sectors is discussed. In Section 2.1.4, 2.1.5, and 2.1.6, key terminology and perspectives in the STAMP theory, and two STAMP-based analysis approaches are explained. In Section 2.1.7, two examples of STAMP-based risk analysis are introduced.

2.1.1 Terminology

The definitions of key terms used in the methodology proposed in this paper are described below:

- ***Accident***: An undesired and unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc. [11]
- ***Safety***: The freedom from accidents
- ***System Safety***: The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle [38]
- ***Hazard***: A system state or set of conditions that, together with a particular set of environmental conditions, will lead to an accident.
- ***Hazard Severity***: The worst possible accident that could result from the hazard given the environment in its most unfavorable state. [12]
- ***Hazard Level***: The combination of hazard severity and likelihood of hazard occurrence. [11]
- ***Hazard Exposure***: A system state that a hazardous state exists.
- ***Causal factor***: One or several mechanisms that trigger a hazard [38]
- ***Risk***: Risk is the hazard level combined with the likelihood of hazard leading to an accident (sometimes called danger) and hazard exposure or duration (sometimes called latency), as shown in Figure 2-1 [12]. Specifically, this thesis refers to a system state that has an *unsafe control*

action(s) and its *causal factor(s)* identified in the context of the actual NEC HSR's situation in Chapter 5, which could lead to an accident, as a safety *risk* of the NEC HSR. Definitions of an u*nsafe control action* and a *causal factor* are described in Section 2.1.4 and 2.1.5.

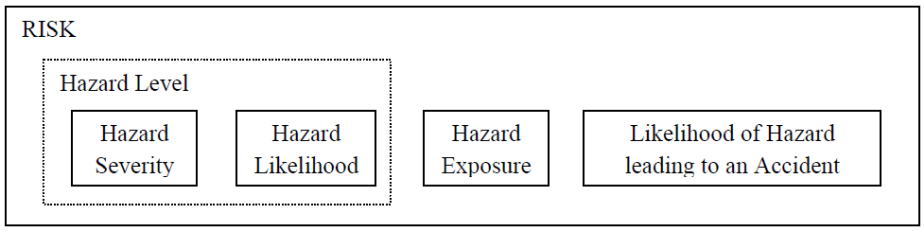

Figure 2-1 Components of risk [12]

Although risks and analysis of them could be discussed in various contexts such as financing, insurance and security, this thesis research uses these terms only in the context of passengers' safety in railway systems. Processes performed in risk analysis can be defined in several ways. For example, in *IEC 60300-3-9*[5] established in 1995, it was defined as the three processes shown in Figure 2-2: "definition of scope," "hazard/risk identification," and "estimation of their consequences and probabilities" [39]. This standard was replaced with *ISO 31000*[6] and *ISO/IEC 31010* in 2009, and the domain of risk analysis has slightly changed: the first two processes – "definition of scope" and "hazard/risk identification" – have been separated from a process newly defined as "risk analysis", as shown in Figure2-3 [5][6]. This thesis research defines risk analysis in accordance with *IEC 60300-3-9* and mainly discusses "definition of scope" and "hazard/risk identification" in risk analysis.[7] Specifically, "definition of scope" refers to clarifying project processes focused on in the NEC HSR, and "hazard/risk identification" refers to identifying causes of hazards and heir causal relations in the project processes.

[5] IEC: International Electrotechnical Commission
[6] ISO: International Organization for Standardization
[7] In the context of the latest *ISO 31000* and *ISO/IEC 31010*, the domain focused on in this paper is "Risk identification," instead of "Risk analysis."

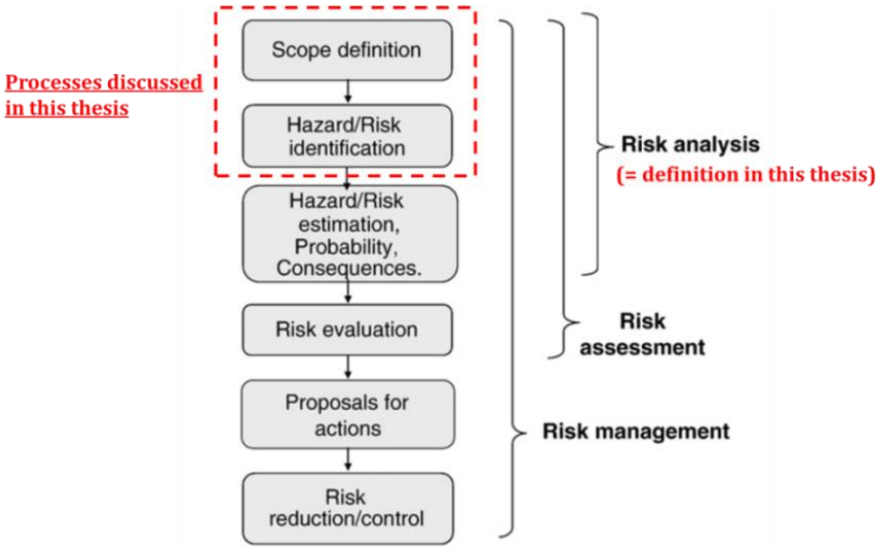

Figure 2-2 Discussed processes in this thesis as risk analysis in *ISO 60300-3-9* [42] (based on [39])

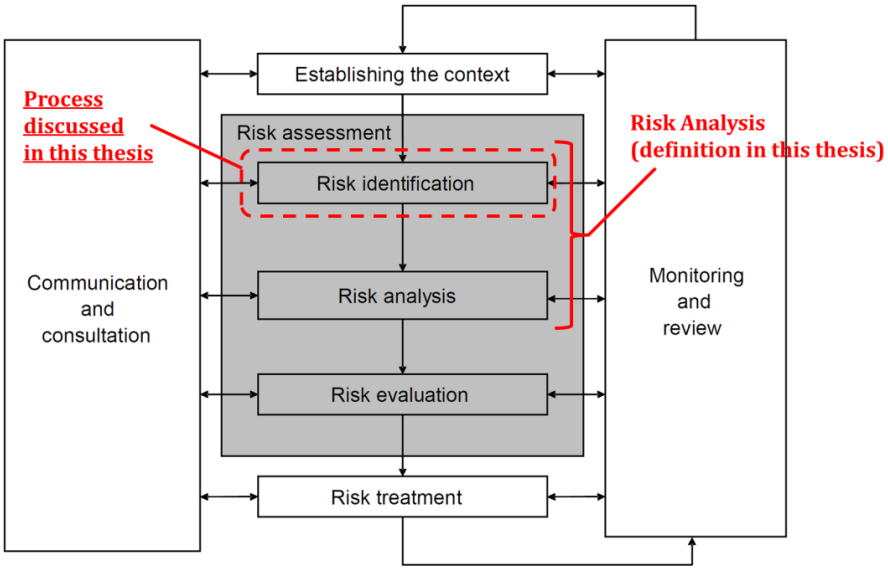

Figure 2-3 Discussed processes in this thesis as risk analysis in *ISO 31000* [40][41]

2.1.2 Reviews of Traditional Risk Analysis Tools and Accident Models

To date, many risk analysis methods have been proposed for the purpose of managing safety of complex systems. Tixier et al. reviews 62 risk analysis methodologies of industrial plants, categorizing risk analysis methods into four groups: deterministic, probabilistic, qualitative, and quantitative [43]. Patel et al. similarly classifies system safety assessment techniques into three main categories: qualitative, quantitative, and hybrid techniques that are qualitative-quantitative or semi-quantitative [44]. *ISO/IEC*

31010 compares applicability of 31 different risk assessment methods [41]. Among them, *Quantitative Risk Assessment* (QRA) methods such as FTA (*Fault Tree Analysis*) [45]–[48], FMEA (*Failure Mode and Effect Analysis*) [11][13][14], FMECA (*Failure Mode and Effect Criticality Analysis*) [13][14], and PRA (*Probabilistic Risk Assessment*) [15][16] have been widely used in various applications.

In order to identify safety risks of systems, it is important to understand how an accident occurs [52][53]. Each risk analysis method above is based on some accident model that describes the theory of accident causation [11]. Specifically, typical scopes of accident models are how accidents arise, what factors can lead to accidents, and how those factors work to cause an accident [54]. Most traditional accident models assume that accidents can be explained as a "chain of events." This event-chain model assumes that an accident and its causal events occur in a specific sequential order. This implies that the accident can be prevented by breaking the chain connecting the events in any way. One of the famous examples of the event-chain accident models is the *Domino Accident Model* (Figure 2-4) proposed by Heinrich in 1931 [55]. This model specifies five stages when an accident occurs; removing the middle domino can cut off the event chain leading to an accident or injury.

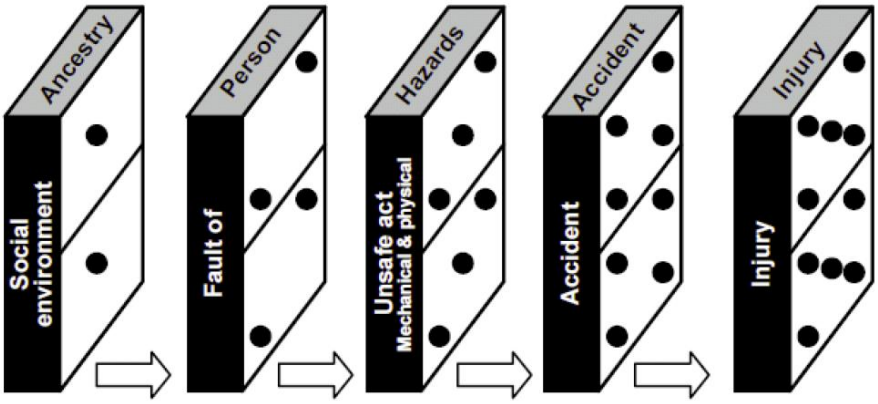

Figure 2-4 The Schematic of the *Domino Accident Model* [56] (originally from [55])

The *Swiss Cheese Model*, which was proposed by James Reason in 1990 (Figure 2-5), is another event-chain accident model [57]. This model has been widely applied to various industries. Reason claims that an accident can be caused as a result of failures in four layers: organizational influences, unsafe supervision, preconditions for unsafe acts, and unsafe acts. According to Reason, an accident happens "when the holes in many layers, which are represented as Swiss cheese, line up to permit a trajectory of accident opportunity" [58].

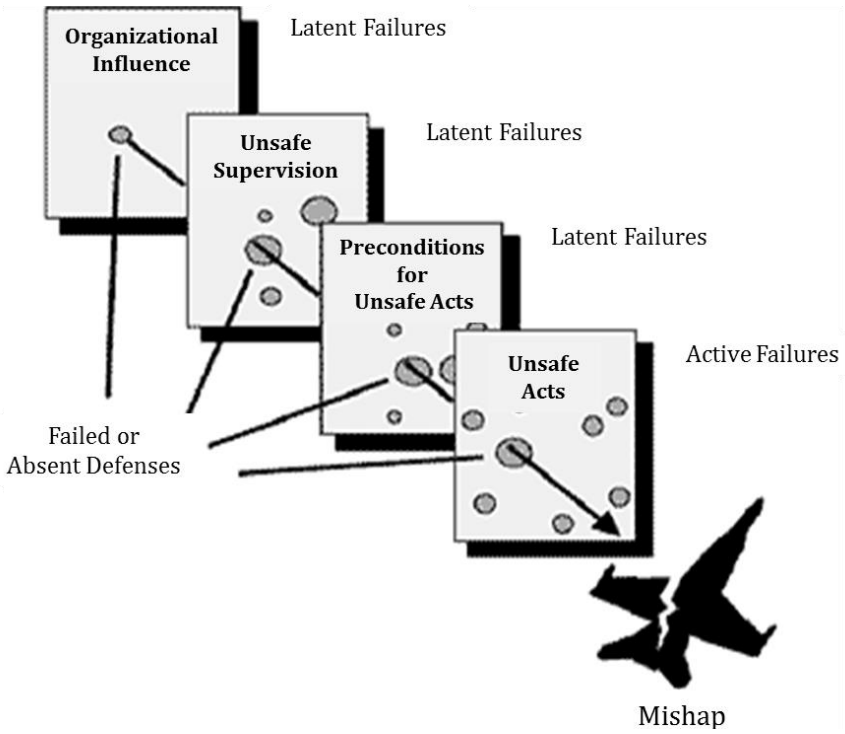

Figure 2-5 The Schematic of the *Swiss Cheese Model* [57]

Aforementioned quantitative techniques such as FTA, FMEA, and PRA are based on these event-chain models; specifically, probabilities or frequencies of occurrence of each event are estimated in these techniques.

Leveson casts doubt on the applicability of these event-chain-based quantitative techniques to complex, sociotechnical systems, arguing the necessity for a broader view of accident causation and indirect or non-linear interactions among events [11][12]. HSR systems can be regarded as complex sociotechnical systems in that they are composed of a highly-complex technical system, various stakeholders, diverse regulations, and their interactions, and that their development and operation could be influenced by social factors. Therefore, this thesis research adopts a new approach that allows analyzing risks of these complex sociotechnical systems at an institutional level. The details about this new approach are discussed in Section 2.1.4.

2.1.3 Application of Risk Analysis in Rail Sectors

This chapter argues risk analysis approaches applied to practical use in rail sectors in the world, clarifying the difference between them and the approach in this research.

- **Risk Analysis in the RAMS Approach**

  One of the prevalent approaches for analyzing system risks is RAMS, stipulated in *EN 50126*.[8,9] RAMS is an acronym of *Reliability*, *Availability*, *Maintainability*, and *Safety*; safety is analyzed in the RAMS processes as one of the crucial system attributes. This standard has been adopted by many railway organizations in Europe [59]. RAMS defines a life cycle of railway systems as comprised of 14 steps shown in Figure 2-6. Railway companies and suppliers involved in the 14 steps are required to manage RAMS in their activities. The third step is risk analysis of system design and implementation, and it is repeatedly performed throughout the system life cycle. This risk analysis in RAMS is based on an event-chain system perspective, evaluating risks by presuming reliability or availability of each system component. In *EN 50126*, FTA and FMEA are recommended as analysis tools [59]. This reliability-based approach[10] was originally developed as a method based on Reliable Engineering in the US, which can still be seen in various industries, including the railway industry, and in various safety standards such as *MIL-HDBK217F*. In fact, *California High-speed Rail Authority* (CHSRA), which is a state entity that is in charge of planning, designing, and constructing the high-speed rail system in the California HSR project, released a *Request For Proposal* (RFP) requiring design-build contractors to implement this RAM/RAMS approach in the project [60].

[8] EN: *European Norm*.
[9] IEC also established *IEC 62278, which is identical to EN 50126*.
[10] In the US, RAM, instead of RAMS, is often used to represent key system attributes. RAM is an acronym of *Reliability*, *Availability*, and *Maintainability*.

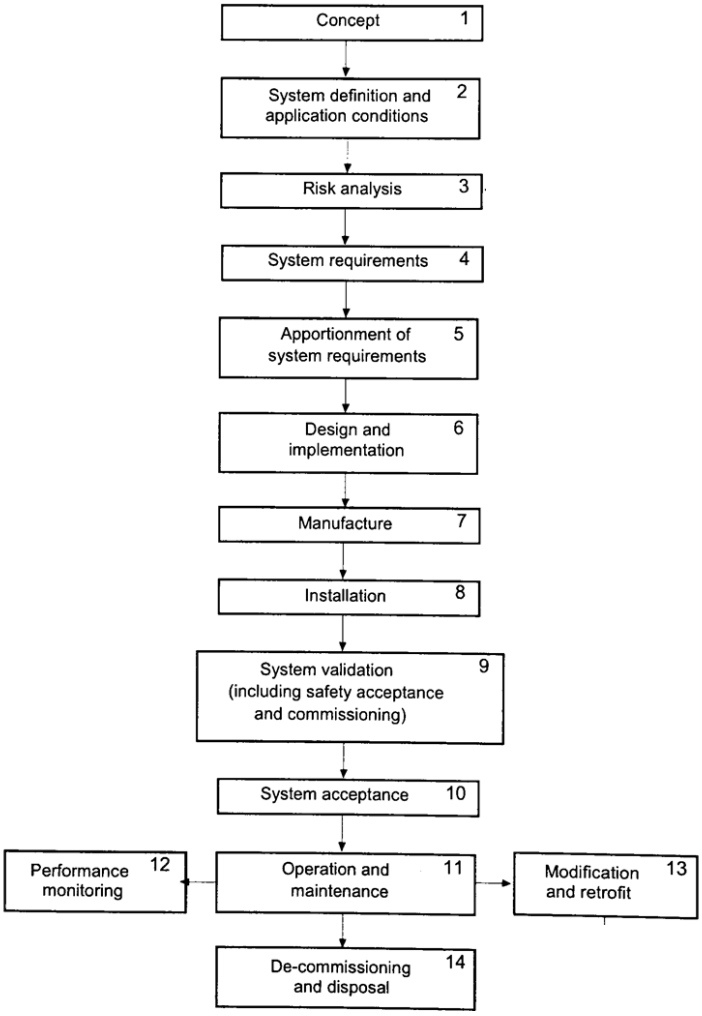

Figure 2-6 System life cycle defined in RAMS [59]

- **Risk Analysis in system safety approaches**

  Safety risk analysis can be also conducted in the context of system safety approaches. The application of system safety approaches to rail sectors is prevalent in Europe. The *European Railway Agency* (ERA) is one of the agencies of EU (*European Union*), established in 2004 for the purpose of reinforcing safety and interoperability among the integrated railway area in Europe. ERA has developed a guideline for *Train Operating Companies* (TOCs) and *Infrastructure Managers* (IMs) to support design and implementation of a system safety program called *Safety Management Systems* (SMS) [61]. ERA has provided various methods and frameworks for the program. *Common Safety Methods for Risk Assessment* (CSM RA)[11] is one of the core components in this SMS approach,

[11] The first CSM regulation, established in 2009, was revised and the new regulation was published in 2013 by *European Commission*, which is the executive body of the EU responsible for proposing new legislation to the European Parliament and the Council of the EU.

aiming at harmonizing differences of risk assessment in changing or newly developing railway systems among the integrated railway area [62]. Figure 2-7 represents the risk management processes in CSM RA; risk analysis plays an important role in these processes. The *System Safety Program* (SSP) in the US, described in Chapter1, is a similar approach to this SMS in that a regulation enforces TOCs and IMs to develop and implement a safety management program, identifying and managing risks in cooperation with their subcontractors and other partners involved in their operation. Both SMS in Europe and SSP in the US do not specify a technique for hazard/risk identification; each entity involved in the operation and system development has a responsibility to adopt an appropriate technique. In parallel with FRA's SSP approach, CHSRA is planning to implement a system safety approach called *Safety and Security Management Plan* (SSMP) in its system development processes. The SSMP is not applied to the revenue operations, but is designed in a compatible manner with FRA's SSP approach. SSMP's requirements for TOCs are also included in the RFP [63]. This RFP specifies risk analysis techniques such as FMEA and FTA for design, construction, testing, and start-up of the system, referring to RAMS as a basis of them.

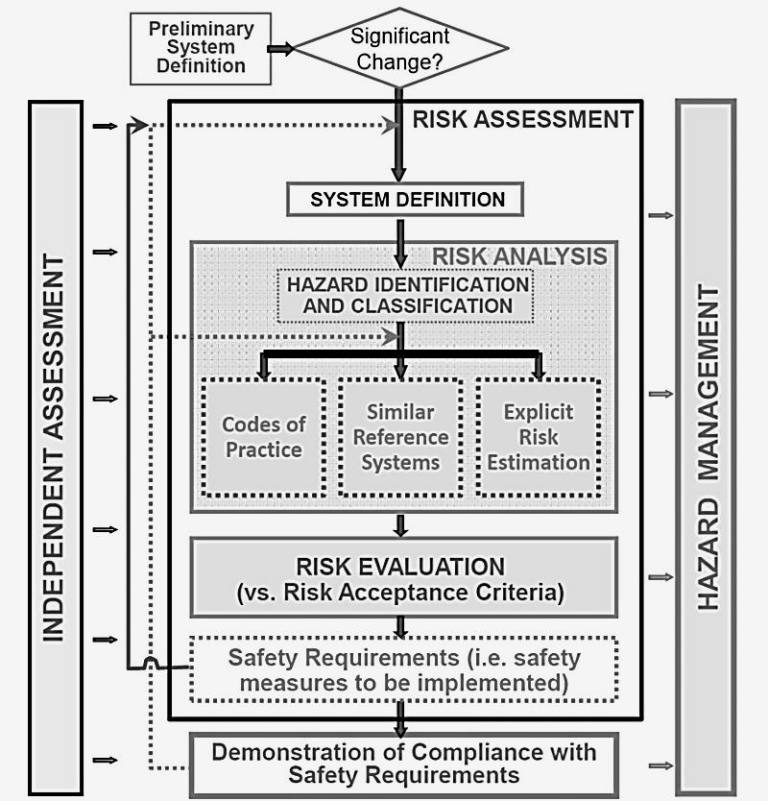

Figure 2-7 Processes in CSM RA [62]

- **Risk-based Hazard Analysis in MIL-STD-882**

  MIL Standard 882[12] [38] provides generic methods for the identification, classification, and mitigation of hazards. It also includes risk assessment methods, which provides a severity category and probability level of potential hazards. This standard has been widely applied as a foundational system safety standard to several regulations such as *49 CFR Part 238.103/603 Passenger Equipment Safety Standards* , *49 CFR Part 229 Locomotive Safety Standards*, *49 CFR Part 236 Signal and Train Control Systems*, and FRA's guidance document *Collision Hazard Analysis Guide: Commuter and Intercity Passenger Rail Service (2007).*[13] Also, RAMS in *EN 50126* contains a risk assessment method similar to that of *MIL-STD-882* [59].

- **Risk Analysis in this Research**

  The research aims to develop a risk analysis methodology applicable in designing an institutional structure and new regulations, identifying risks driven by industrial transformation. Risk analysis in this research focuses on all of the safety-related organizations in the entire industry and their safety-related interactions, instead of focusing solely on safety management of one specific organization or on a technical/operational physical domain of the system as RAMS, SSMP, SSP, or *MIL-STD 882* does. For this unique scope, a new risk identification technique and risk analysis processes are introduced in this thesis. Section 2.1.4 describes foundational concepts of this new approach.

2.1.4 Systems-Theoretic Accident Model and Process (STAMP)

The methodology that this research proposes is based on the STAMP theory. STAMP, proposed by Leveson [10][11], is a new system causality model that includes a broader view of accident causation and indirect or non-linear interactions among events. In this theory, safety of systems is modeled with a *hierarchical safety control structure*, in which people, organizations, engineering activities, and physical system elements are the components of the model, and their safety-related interactions, defined as *control actions* and *feedback*, are described with dynamic feedback *control loops*. This STAMP theory views an accident as a result of a violation of the *safety constraints* enforced by the control loops in the system, while most traditional safety analysis methods such as FTA or FMEA focus on a chain-of-events model, and regard an accident as a sequence of component failure of the system. Leveson describes this view as "safety is an emergent property of systems" [11]. In this section, key terminology and perspectives in the

[12] *U.S. Dept. of Defense Military Standard 882* presents standard practice for system safety. *MIL-STD-882E* is the latest version updated in May 2012.

[13] The *Federal Transit Administration*'s (FTA) guidance documents such as *Transit Safety Measurement and Performance Measurement (2011) and Hazard Analysis Guidelines for Transit Projects (2000)* are also based on *MIL STD 882*.

STAMP theory is explained. Also, this STAMP theory can be applied to accident analysis referred to as CAST (*Causal Analysis based on STAMP*) and hazard analysis referred to as STPA (*System-Theoretic Process Analysis*), and their processes are described in details in Section 2.1.6 and 2.1.5, respectively.

- **Hierarchical Safety Control structure and Safety Constraints**

  Figure 2-8 represents a general form of a hierarchical safety control structure in a regulated safety-critical industry [10]. There is a feedback control loop between each level of the hierarchy. Higher level components provide *control actions* such as safety-related policy, regulation, and procedures, and receive *feedback* about their effects in the shape of reports. Lower level components implement those regulations and procedures, and their feedback enables higher-level components to maintain or improve safety-level of their controls. The hierarchical safety control structure in Figure 2-8 consists of two basic hierarchical domains: *system development* (on the left in the figure) and *system operations* (on the right in the figure). *System development* hierarchy describes safety control structure of R&D, design, and manufacturing activities about the physical system[14] and regulatory activities about them. System operations hierarchy is comprised of an operating process and related management and regulation. This twofold structure is developed based on a concept "safety must be designed into physical systems and that safety during operations depend partly on the original design and partly on effective control over operations." [64] Importantly, these two domains are also interconnected with a control action and feedback for continuous system evolutions; system developers and its users must communicate about the operating procedures, environment, practical issues, and performance of the physical system, which should be continuously reflected to system development.

  Defining a safety control structure entails specifying expectations, responsibilities, authority, and accountability in enforcing safety controls of every component at every level of the hierarchy [64]. These safety controls at each level of the hierarchical safety control structure can be regarded as *safety constraints*. Appropriate safety constraints exercised by each system component that are ensured by appropriate *system requirements*, together lead to enforcement of the overall system safety constraint, which prevents an accident.

[14] For example, "Physical system" in automotive industries represents automobiles. In railway industries, physical system represents rolling stock and infrastructure (e.g., signal systems and rails) and other equipment required for operation and maintenance.

Thus, this STAMP-based approach is appropriate for this research, which discusses a new project that involves both system development processes and operations with a specific focus on the dynamics of the institutional level. However, this control structure is a "static" model of the system; if the structure of the system changes, the hierarchical safety control needs to be redesigned according to each change. This research aims to not only identify risks but also analyze how these risks would change over time. In order to perform this dynamic analysis more efficiently, *System Dynamics* (SD) models are used, in addition to the STAMP-based analysis. The details about SD will be explained in Section 5-3 and Appendix A.

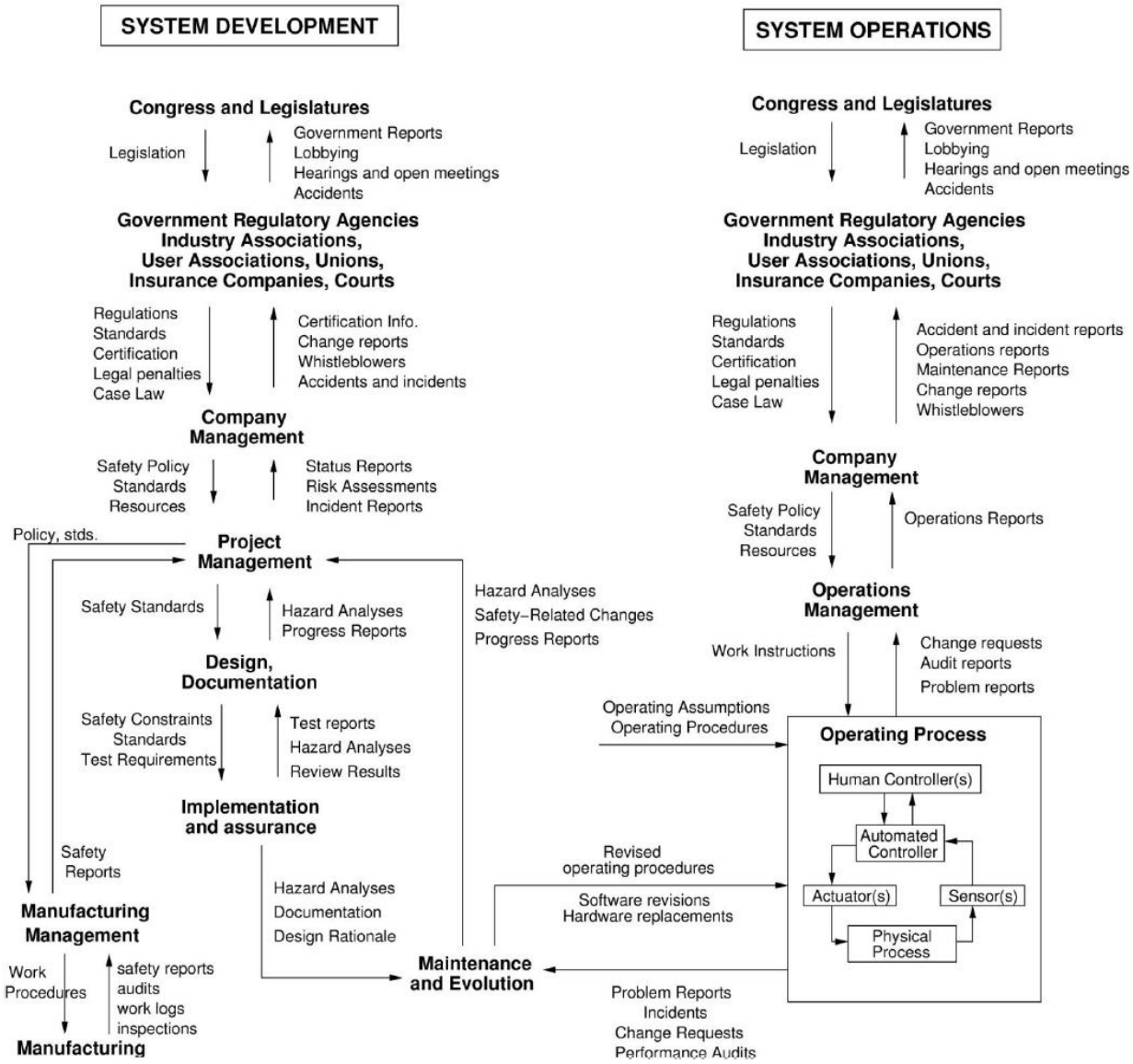

Figure 2-8 General Sociotechnical Safety Control Structure [11]

- **Control Loop and Process Model**

  Hierarchical safety control structures can be decomposed into control loops between each level. In each control loop, a higher-level component, referred to as *controller*, provides safety control to a lower-level component, referred to as *controlled process*, and the controlled process provides feedback to the controller. Figure 2-9 represents a generic control loop.

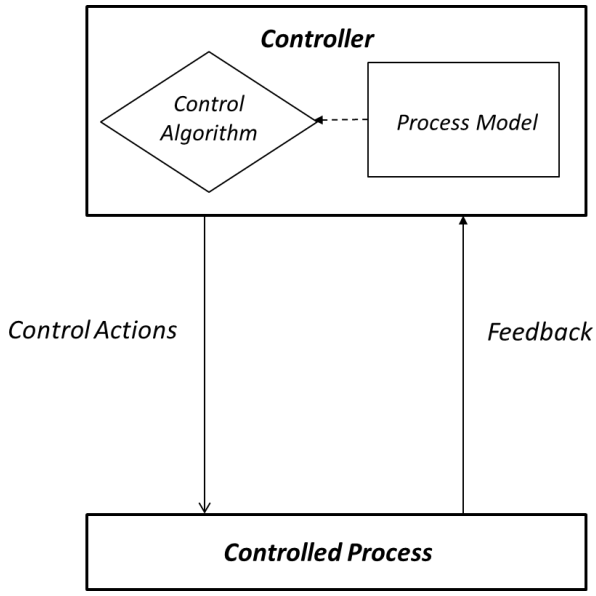

Figure 2-9 General control loop [11]

Controller has a decision-making algorithm to determine what control actions to provide. This decision making is performed based on a "model" of the current state of the system. Leveson refers to this model as *Process Model* [10]. If a controller is a human, the process model is called a "mental model." Inadequate safety control action could be provided if the decision-making is performed based on a wrong process model or mental model. In STAMP-based safety analysis, clarifying this process model is a crucial step. In addition to feedback from the controlled process, control inputs provided by controllers at further higher levels and external information such as feedback provided from other controlled processes could be sources of the process model of the controller. Also, at institutional levels that this research focuses on, control processes can be also regarded as controllers of lower levels.

- **Accident causes in the STAMP theory**

  According to Leveson [11], there are five general causes of accidents or hazards:

Unsafe Control Actions:

1) A control action required for safety is not provided or not followed.
2) An unsafe control action is provided that leads to a hazard.
3) A potentially safe control action is provided too late, too early, or out of sequence.
4) A safe control action is stopped too soon or applied to long (for a continuous or non-discrete control action)

Failure of Controlled Process:

5) Appropriate control actions are provided, but the controlled process does not follow them.

These five scenarios are used to identify causes of hazards in STPA and CAST. Section 2.1.5 and 2.1.6 explain the detailed processes of STPA and CAST, clarifying how to apply the STAMP theory to the actual analyses.

2.1.5 System-Theoretic Process Analysis (STPA)

STPA is a hazard analysis method based on the STAMP theory. Its goal is to identify design constraints necessary to maintain safety of a system, by analyzing hazards and their causal factors. STPA can support hazard/risk analysis of existing systems or a safety-driven design of new systems. STPA consists of the following three steps.

- **Create basic system engineering information**
  Basic system engineering information needs to be derived before the hazard analysis is performed. There are six tasks involved. In the first four tasks, the analyzed system is defined.

  1) Define accidents
  2) Draw a system boundary
  3) Define high-level system hazards, based on 1) and 2)
  4) Define high-level system requirements and safety constraints, based on 3)
  5) Construct a hierarchical safety control structure, based on 4)
  6) Allocate responsibilities and define control actions, feedback, and a process model for each component, based on 4) and 5)

  Based on the defined accidents and system boundary in 1) and 2), a small set of high-level system hazards need to be identified to define system requirements and safety constraints; starting with very specific hazards, instead of high-level ones, must be avoided because it could lead to disorganized or

non-comprehensive identification of system requirements and safety constraints. Based on the requirements and constraints, a hierarchical safety control structure is constructed. Thus, this developed control structure is defined within the system boundary. For each system component, responsibilities, control actions, feedback, and a process model are defined. Table 2-1 is an example of a format to organize this information.

Table 2-1 Allocation of responsibilities (format)

Controllers	Responsibility	Controlled Process	Control Action	Feedback	Process Model
A					
B					
C					
D					

- **Identify Unsafe Control Action (STPA-1[15])**

  In STPA-1, unsafe control actions are identified. The four types of unsafe control actions shown in Section 2.1.4 are applied to each control action defined in the control structure, and conditions under which the control actions are unsafe are identified. Table 2-2 represents a format used in this research to organize these conditions for each controller in the system.

Table 2-2 List of unsafe control actions in STPA-1 (format)

Controllers	Controlled Process	Control Action	Unsafe Control Actions			
			Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
A						
B						
C						
D						

- **Identify causal factors of unsafe control actions (STPA-2)**

  In STPA-2, causal factors of the identified unsafe control actions in STPA-1 are analyzed with guide words developed for scenario identifications. This research uses the guide words shown in Figure 2-10, which is proposed by Leveson [11]. Causal factors of the fifth type of the accident causes, "Appropriate control actions are provided, but the controlled process does not follow them," are also analyzed in this step.

[15] Leveson calls this step as STPA step 1 in [11], but this thesis use "STPA-1" to avoid confusion with steps of the proposed methodology in Section 2.2. Similarly, STPA-2 is used for STPA step 2.

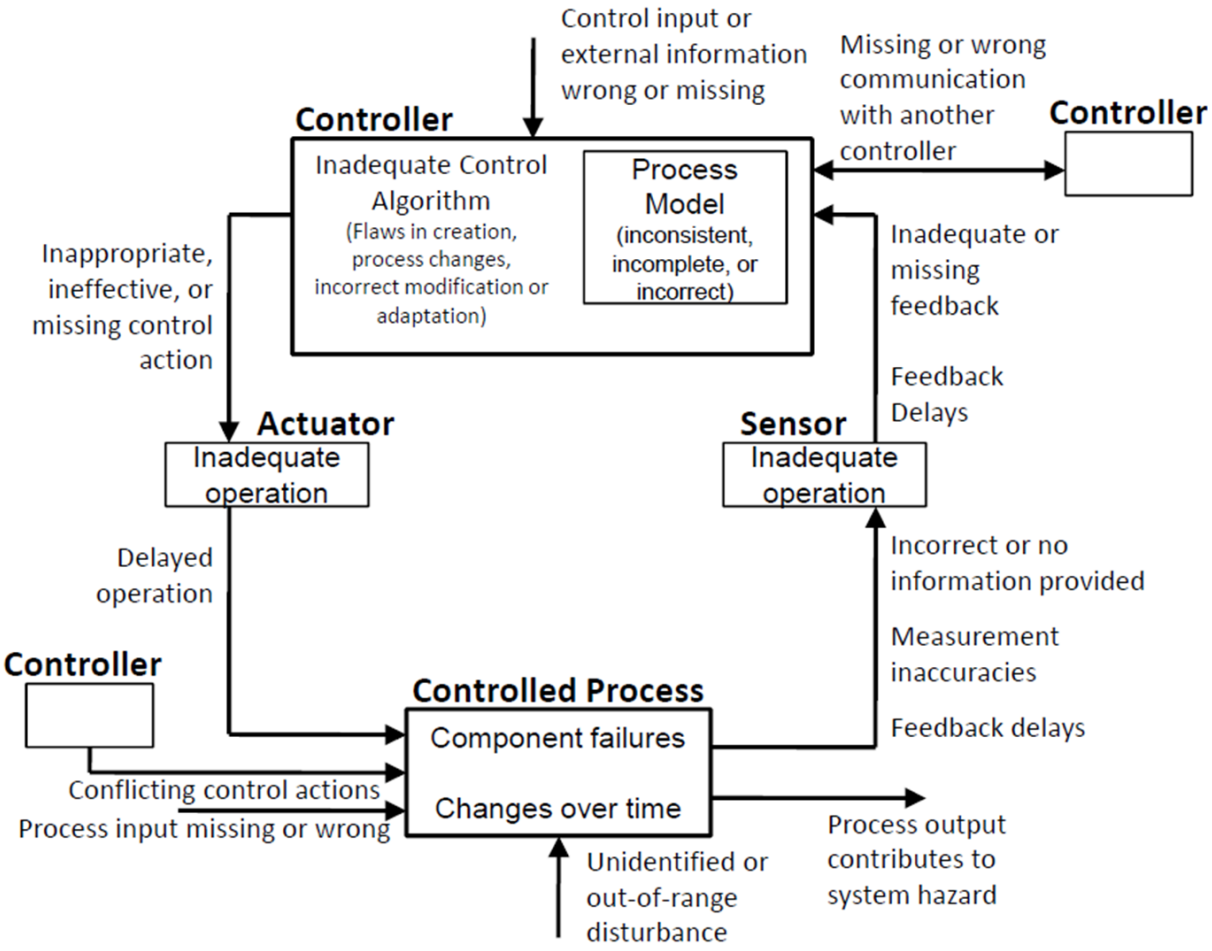

Figure 2-10 Guidewords for identifying causal factors [11][64]

Leveson classifies causal factors into three general categories: (1) *the controller operation*, (2) *the behavior of actuators and controlled processes*, and (3) *communication and coordination among controllers* [11].

(1) Controller Operation

Controller operation consists of three primary parts: control inputs and external information, the control algorithms, and the process model. Flaws in these parts can cause unsafe control actions.

- Control inputs represent control actions provided by higher level controllers in the hierarchical control structure, and external information represents inputs required for safe behavior of the controller that, for example, could be provided as feedback from other controlled processes or communication with other controllers. If these control inputs or external information are mission or wrong, they could lead to unsafe control actions.

- In adequate control algorithms (decision making algorithms) of the controller could cause unsafe control actions. For examples, if control algorithms are inadequately designed originally, if they are not modified according to change of the process model, or if they are not well maintained, control algorithms can be hazardous.
- Inconsistences between the process models used by the controller and the actual process state could be a source of unsafe control actions. Missing or incorrect feedback for updating the process model or time lags in the feedback loop are the main causes of the inconsistencies. Figure 2-10 includes *Sensor* as a transmission channel or tool of the feedback, and its inadequate operation could lead to inadequate feedback. At institutional levels that this thesis focuses on, there is no actual mechanical or electronic sensor, but this term "sensor" is used to represent a transmission channel or tool of the feedback.

(2) Behavior of actuators and controlled processes

This topic discusses the case in which the control actions are safe, but the controlled process may not follow the commands. One possible cause for this is a failure of the transmission channel of the control actions. Also, failures of the actuator or controlled process itself are other causes. At institutional levels that this thesis focuses on, this term "actuator" is used to represent a transmission channel or tool of the control actions. Lastly, missing or wrong safety-related inputs from outside the loop to the controlled process could hinder it from executing the control commands.

(3) Communication and coordination among controllers

The controlled process could be controlled by other controllers than the one in the loop. If their control actions from outside are not coordinated and conflict with the ones from the controller in the loop, the controlled process could behave unsafely.

Some of these causal factors could be further interconnected to each other and to ones outside of the loop. In this thesis research, System Dynamics is used to analyze further detailed causal relations after STPA is conducted.

2.1.6 Causal Analysis based on STAMP (CAST)

CAST is a STAMP-based accident analysis method, which is also proposed by Leveson [11]. Similarly to STPA, the whole system analyzed is modeled with a hierarchical safety control structure, and the causal factors of the accident are discussed in the context of control problems in this structure. The causal analysis is performed from some specific perspectives such as both lower- and higher-level controls, overall communications and coordination, and the dynamics and changes in the system. The specific steps of CAST are as follows [11]:

1) Identify high-level hazards involved in the accident.
2) Identify system requirements and safety constraints associated with these hazards.
3) Develop the safety control structure in place to control the hazard and enforce the safety constraints. Each system component's roles, responsibilities, controls provided or created pursuant to their responsibilities, and the relevant feedback are specified.
4) Determine the proximate events that led to the accident.
5) Analyze the accident at the physical system. Identify the contribution of the physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances to the events. Analyze why the physical controls in place were not adequate in preventing the hazard.
6) Moving up the levels of the safety control structure, determine how and why each successive higher level contributed to the inadequate control at the lower level. For each safety constraint, either the responsibility for enforcing it was never assigned to a component in the safety control structure or a component or components did not exercise adequate control to ensure their responsibilities (safety constraints) were enforced in the components below them. Any human decisions or flawed control actions need to be understood in terms of (at least): the information available to the decision maker as well as any required information that was not available, the behavior-shaping mechanisms (the context and influences on the decision-making process), the value structures underlying the decision, and any flaws in the process models of those making the decisions and why those flaws existed.
7) Analyze overall coordination and communications contributors to the accident.
8) Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.
9) Generate recommendations.

2.1.7 Examples of STAMP-based Risk Analysis

While there are several researchers who analyze a rail accident with CAST focusing on the institutional structure of the industry [31]–[34], there has been no STAMP-based research on safety risk analyses of rail industries in operation or of planned railway projects. Although the following two research papers are not about rail industries, they are excellent examples of applying STPA to safety risk analysis with a specific focus on institutional structures.

- **Paper 1: Risk management approach for CO_2 Capture project** [66]
  Samadi analyzes the risks, including safety, of CO_2 Capture project called CTSC project[16], focusing on the institutional structure and technology for each project phase. STPA is used for several case studies, identifying required safety controls and possible unsafe controls. *General safety control structure* is finally developed by integrating the insights acquired from the case studies. SD is used to model the dynamics of the non-linear causal relation of the risks, which are identified by literature reviews and discussion with experts in this industry, and finally the SD models are combined to represent the overall risks in the system. Samadi's approach is organized in Figure 2-11.

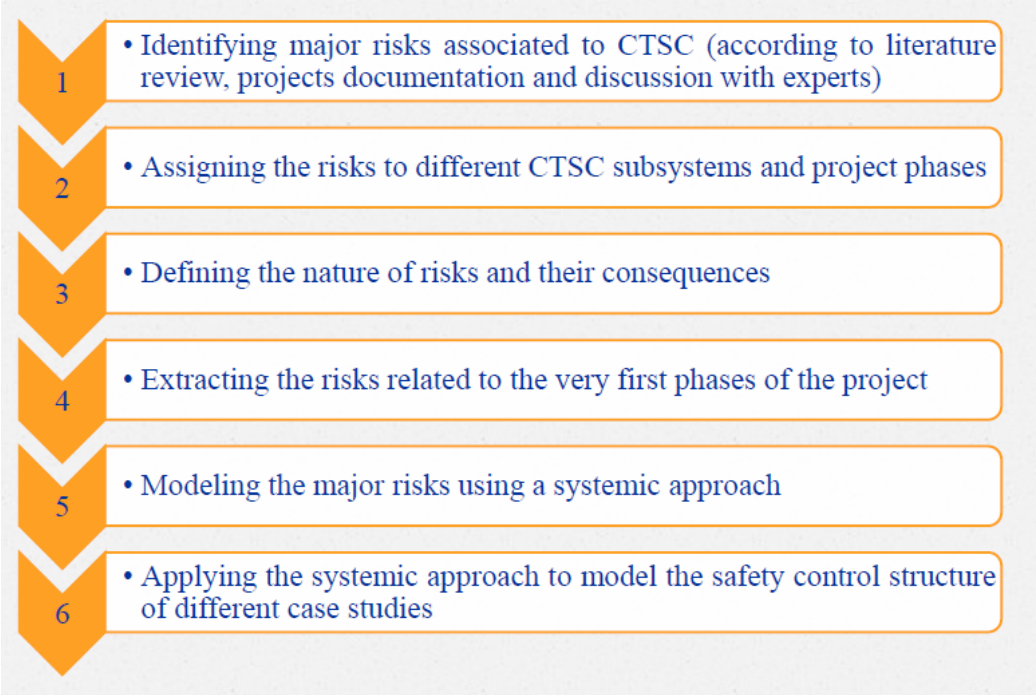

Figure 2-11 Proposed risk analysis method [53]

[16] CTSC is an acronym of *Capture, Transport and storage of CO_2*.

- **Paper 2: Risk analysis of NASA independent technical authority** [9][10]

  This research, conducted by Leveson and Dulac, is for the assessment of the health of NASA's ITA (*independent technical authority*) program. The organizational design of ITA is discussed from a safety perspective. STPA is used to identify inadequate control actions in the system. The identified risks are interconnected and correlated by a SD model to analyze their dynamics and to identify the best leading indicator of the increase in the system risk level. This approach is organized in Figure 2-12.

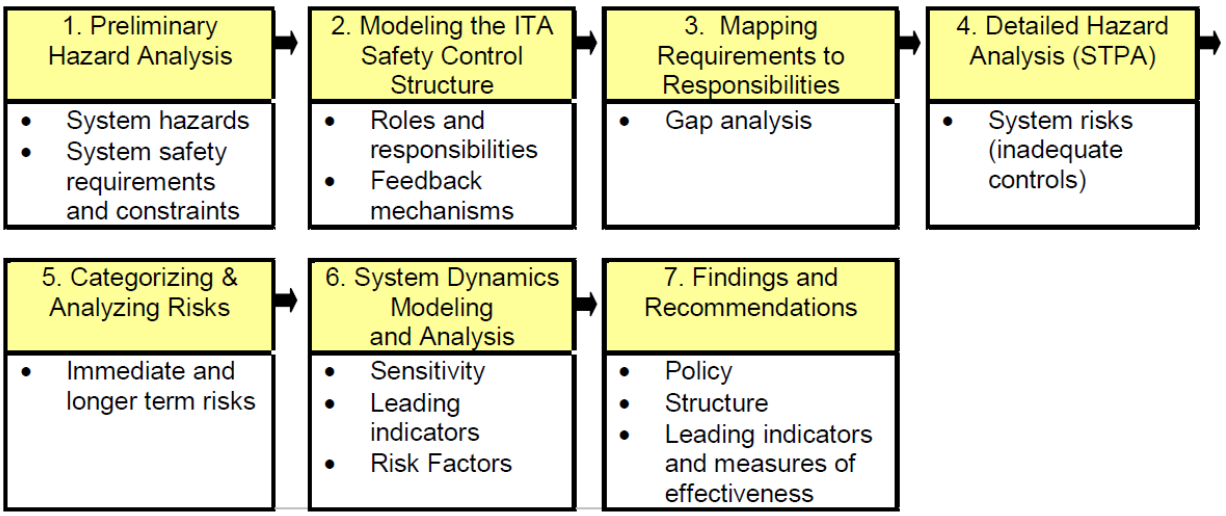

Figure 2-12 The STAMP-Based risk analysis process [9][10]

Although there are minor differences among them, both of the papers used STPA as a risk identification tool, and adopted SD to analyzed detailed causal relations of risks. The methodology that this research proposes is built based on these approaches. In Section 2.2, the methodology will be explained in detail step by step.

2.2 Proposed Methodology

This research proposes the following analysis methodology, which consists of five steps. This section explains specific processes in the five steps in the context of the case study about the NEC HSR conducted in this research.

Step 1: Accident Analysis (CAST)

- 1-1 Choose multiple accidents
- 1-2 Conduct CAST for them.
- 1-3 Identify any common requirements/constraints required at the institutional level

Step 2: Model Development and Preliminary Risk Analysis

- 2-1 Define a system and develop a generic model representing a typical railway industry with a particular focus on the institutional level.
- 2-2 Incorporate the findings in Step 1-3 into the generic model.
- 2-3 Choose institutional alternatives of the target project to analyze, develop their safety control models, and define responsibilities of each component of the models, based on the generic model.
- 2-4 Compare 2-3 with 2-2, and clarify structural differences that could possibly make it difficult to meet the system requirements adequately.

Step 3: Risk Analysis 1 (STPA of the NEC HSR)

- 3-1 Identify causes of hazards for each alternative with STPA-1 (shown Section 2.1.5).
- 3-2 Analyze causal factors of the identified causes of hazards for each alternative with STPA-2 (shown Section 2.1.5), based on the actual project plan, current issues, regulations, and safety management applied to the target project.

Step 4: Risk Analysis 2 (System Dynamics-based analysis of the target project)

- 4-1 Develop a System Dynamics model, incorporating the key risks identified in Step 3.
- 4-2 Analyze detailed causal relations and transition of the safety level of the system.

Step 5: Evaluate Risks and Design Safety Constraints (not performed in this thesis)

- 5-1 Evaluate and prioritize risks
- 5-2 Design the necessary safety constraints for each institutional alternative

Step 1 is a process to identify system-based lessons from past accidents with CAST. In this research, the following two rail accidents are analyzed.

1) *Hatfield Derailment* in the UK in 2000
2) *Wenzhou Train Collision* in China in 2011 (HSR accident)

As Chapter 3 will show, these two accidents each had complex issues at the institutional level. Also, these two industries have different institutional structures, so the analyses gave multi-angled lessons in analyzing the NEC HSR, which still has multiple alternatives for the institutional structure. Based on the results of the accident analyses, common system requirements/constraints required at the institutional level in the two accidents are identified. Although the CAST analyses deal with different accident modes, which are train collision and derailment, focusing on an institutional level in the following steps allows the system requirements/constraints of them to be integrated as generic "lessons" regardless of the types of the accidents.

In Step 2, a generic HSR model representing a typical HSR industry model is developed. The identified system requirements/constraints in Step 1-3 are integrated in this process. This generic HSR model can be regarded as the "simplest base case" that can meet all of the system requirements and safety constraints, including the "lessons" identified in Step 1. Based on the information acquired from stakeholders' industrial reports about the NEC HSR, the generic HSR model is tailored to safety control structures representing possible institutional alternatives of the NEC HSR. Specifically, three different institutional alternatives of the NEC HSR are chosen in Section 4.3.2. All of the control models are developed with a particular focus on the institutional levels. As shown in Section 4.3.2, compared to the generic HSR model, these alternatives have complex institutional structures. Based on the STAMP perspective, these additional complexities would require additional safety constraints, thereby providing "sources" of safety risks. As preliminary risk analysis, comparative analysis of the three alternatives with the generic HSR model is performed to identify the "sources" in Step 2-4, specifically aiming at identifying their structural flaws or additional safety-related interactions. Thus, the "simple" generic HSR model is used to help develop models of the "complex" unique institutional alternatives of the NEC HSR and highlight the structural differences.

As the analysis of NASA [67] did, it would be possible to perform risk analysis from scratch without the information given by CAST in Step 1, but this approach would require a comprehensive knowledge about the system to identify system requirements and constraints comprehensively. The CAST-based procedure

that this research proposes could help identify the system requirements and constraints more easily and perform the following risk analyses more efficiently. Furthermore, this CAST-based analysis helps directly and therefore, effectively focusing on the key elements of the system related to the fact-based valuable lessons learned from past accidents.

In Step 3, unsafe control actions in the system are analyzed for each alternative with STPA-1. As a next task, their specific causal scenarios are analyzed according to the guide words in STPA-2, based on the actual project plan, current issues, and regulations applied to the NEC HSR. This thesis refers to these unsafe control actions and their causal scenarios identified in the context of the actual NEC HSR's situation as risks. With the identified risks, the *System Safety Program* (SSP), proposed by FRA to handle possible safety risks, is evaluated in Section 5.2.2.

While Step 2 and Step 3 are the risk analyses relatively focusing on one static system structure, Step 4 takes into account dynamic changes of the system and external impact on the system, such as change of ridership or change of economic condition of the local societies. Also, the causal factors identified in Step 3-2 are the only ones directly related to the analyzed loop each time. System Dynamics (SD) [69] introduced in Step 4 can expand the causal relations identified in Step 3, which focuses on direct interactions, to the entire system, taking into consideration indirect causal factors and impact of multiple changes in the entire safety control structure. In this research, in order to present the applicability of SD to risk analysis of the NEC HSR, SD-based analysis is conducted by combining some of the key risks identified in Step 3 that have common causal factors to some extent, and their detailed causal relations and their dynamic behaviors are discussed.

Step 5 is not performed in the case study, but it is an important step in practice. The risks identified in Step 4 are evaluated and prioritized, and safety constraints are designed based on the evaluation. This process should be conducted cooperatively with experts from diverse organizations involved in the project. This thesis does not provide or suggest a specific risk evaluation method or a definition of acceptable/unacceptable risk, but importantly, these decisions must be implemented in a consistent way, which is not adequately established in the US rail sector.

Thus, the expected analysis outputs of this thesis research, which conducts Step 1 to Step 4, are as follows.

- Safety risks as unsafe control actions and their causal factors for each alternative of the NEC HSR
- Weaknesses of key safety regulations applied to the NEC HSR such as SSP

One important note about the scope of this research is that this thesis is not aiming to identify the optimal institutional structure with minimal safety risks among the alternatives. In reality, system complexities at an institutional level could be intentionally introduced for non-safety purposes such as an economic benefit [70][71]. Therefore, what risks these complexities could provide and whether these risks could be safely managed with appropriate safety constraints are rather important from a practical perspective. The outcomes of this thesis research can be valuable for the actual institutional design.

In the next chapter, Step 2 in the proposed methodology is performed, focusing on two milestone rail accidents.

CHAPTER 3. ACCIDENT ANALYSIS

3.1 Case 1 – Hatfield Derailment –

While most of the rail industries in other countries consisted of state-owned TOCs and IMs, the UK rail industry has a vertically separated private rail industry. In the 1990's, the state-owned railway company, British Railway (BR), was privatized for providing a better service, as many other state-owned industries in the UK had been similarly done since the 1980's. During the decade after the privatization, the UK rail industry had four fatal accidents, which totally caused 49 deaths. As the official accident reports of the four fatal accidents claim that immature corporate management of some of the privatized companies and the inadequate industrial structure are grave causal factors of the accidents, many researchers focusing on these accidents have been discussed the impact of the privatization and the industrial structure on rail safety in their papers [35][36][72]–[74]. This research focuses on *Hatfield Derailment* in 2000, the most symbolic accident among them, as the first case for accident analysis with CAST.

3.1.1 Summary of the Accident

This accident caused four fatalities and more than 70 injuries. In this thesis, this accident is analyzed mainly based on the two sources: the official accident report by *Office of Rail Regulation* (ORR) [75] and "Broken Rails," a book authored by C. Wolmar [76]. The overview of the accident is shown below [75].

- At 12.23 on Tuesday 17 October 2000, train ID38 travelling from London Kings Cross to Leeds derailed roughly 0.5 miles (0.8km) south of Hatfield Station. The train, operated by *Great North Eastern Railway* (GNER), was carrying one hundred and seventy passengers and twelve GNER staff. Four passengers were killed and over seventy people were injured, four seriously, including two of the GNER staff.
- The train was an Intercity 225 hauled by an electric Cl91 locomotive. The train was made up of a set of nine *Mark 4* (MK4) coaches comprising, six standard class coaches, one service coach/buffet car, two first class coaches and a trailing *Driving Van Trailer* (DVT).
- The train derailed on the down fast line (going north) as it travelled through the Welham Green curve. The rail fractured into over 300 pieces over a distance of approximately 35m. Beyond this, the rail was intact, although displaced for approximately 44m, followed by a further fragmented length of 54m.

- The locomotive and the first two MK4 coaches remained on the track, but the following eight vehicles derailed to varying degrees of severity. Some coaches were leaning over; the service coach was lying completely on its side (Figure 3-1).

Figure 3-1 The scene of the derailment (http://www.theguardian.com, 2/22/11)

3.1.2 Analysis

This accident is analyzed with CAST in accordance with the nine steps presented in Section 2.1.6.

- **Step 1: System Definition & Hazards**
  - **System Definition**

    The institutional structure of the railway industry in the UK right after the privatization is defined as the system discussed in this analysis..

  - **System Hazards**

    A train derailment at a high speed caused by rail cracks is specifically set as the accident in this system although there are generally many other possible accident types in rail systems. The high-level hazards that could lead to this accident are as follows:

    A. Rails have physical problems that could not endure the operation.
    B. The operational speed of the train exceeds the limit determined by durability of rails.

- **Step 2: Safety Constraints and System Requirements**

  The safety constraints and system requirements for the two system hazards defined in Step 1 are as follows:

  a) Rails must be maintained correctly in compliance with the relevant standards and regulations. (Hazard A)
  b) Standards and regulations on maintenance must be reasonable. (Hazard A)
  c) Defects of rails or their precursors must be detected and adequately dealt with in maintenance. (Hazard A)
  d) Operation must be restricted correctly according to the condition of the rails. (Hazard B)
  e) Decision criteria in restricting the operation must be reasonable. (Hazard B)

- **Step 3: Safety Control Structure**

  The safety control structure is developed in Figure 3-2. The roles and responsibilities of each component in the structure are described as follows.

  - **System Development**

    The institutional structure after the privatization was designed by the UK Parliament in the privatization process. This design process and designed structure can affect the safety of the system, so this research has included this safety-related interaction in the model.

  - **System Operations**

    As a result of the privatization implemented by the UK government, the structure of the railway industry became vertically separated; i.e., the operator of the trains and the owner of the infrastructure (e.g., rails, stations, tunnels, etc.) are different organizations, as explained in Section 1.3. The entire infrastructure is owned by Raitrack, and they sell the right of use of their infrastructure to *Train Operating Companies* (TOCs). TOCs are licensed by ORR, which is the state-owned institution also regulating Railtrack's contracts with operators (with respect to only finance, not safety). Railtrack makes contracts on maintenance of their infrastructure with maintenance companies such as *Balfour Beatty* and *Jarvis*, and these contractors are responsible for conducting maintenance in accordance with directives from Railtrack and reporting the results. Based on these reports, Railtrack is supposed to manage the maintenance data and judge the necessity of irregular maintenance or replacement of the infrastructure and of operational restrictions such as limitation of the maximum operational speed. Thus, train operation,

infrastructure operation, and infrastructure maintenance are performed by different companies. Also, industry safety standards called *Rail Group Standard* (RGS) are formulated by *Railtrack Safety and Standards Directorate* (RSSD), which is an internal board in Railtrack, and with them, Railtrack had been responsible for managing safety reports from the entire industry until the end of 2000.[17] Railtrack also has a control center called *Power Signaling Board* (PSB), which monitors the location of operated trains by detecting the signal current running in the rails. If there is a signal problem in a specific track, *Non Descried Alarm* (NDA) works in the control center. Although the main focus of this research is the institutional level, physical domains are partially included in the two CASTs in this research to help understand causal factors of the accidents more sufficiently.

[17]Before the accident, *Health and Safety Executive* (HSE), a governmental agency, was responsible for enforcing health and safety standards throughout the industry, but many regulations practically related to operation were established as RGSs. Railtrack was also in charge of accepting safety report from TOCs and maintenance contractors, so Railtrack had a regulatory function at this time, instead of HSE. This regulatory responsibility was transferred to HSE in 2000, and further transferred to ORR in 2006. Considering HSE was not closely involved in safety-related activities between Railtrack and TOCs and maintenance/renewal contractors, which is the main focus of this analysis, this research does not include HSE in the control structure.

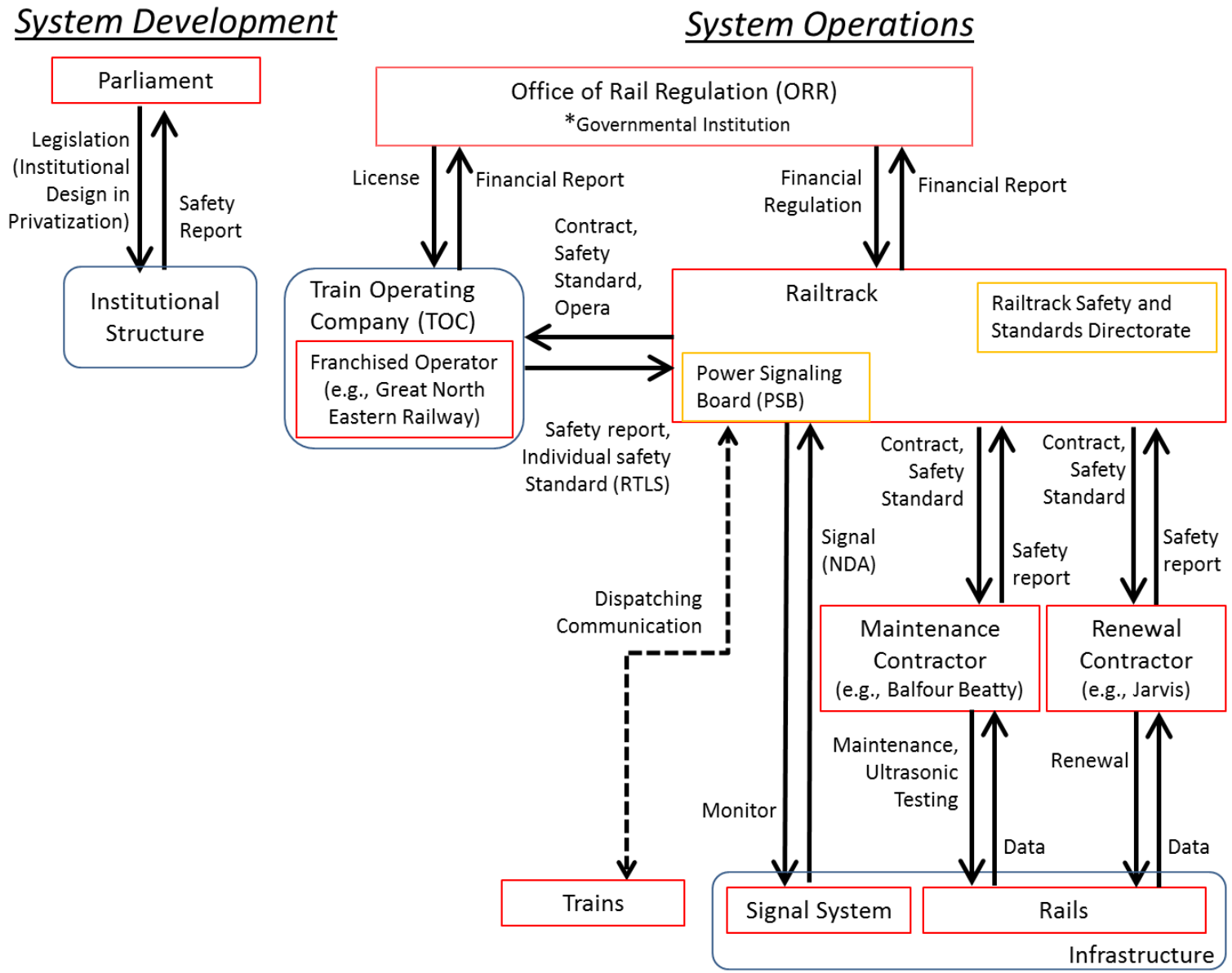

Figure 3-2 The safety control structure of the UK rail industry (1997-2000)

Table 3-1 Responsibility of each component of the model

Hierarchy	Components	Responsibility
System Development	Parliament	Design the institutional structure of the industry in the privatization process, based on adequate risk analysis
System Operations	Office of Rail Regulation (ORR)	ORR is the public economic regulator that licenses TOCs, and regulates Railtrack's contracts with TOCs. At this time, ORR was not responsible for licensing based on safety capability. (only based on financial capability)
	Railtrack	Infrastructure is owned by Raitrack, and it sells the right of use of their infrastructure to TOCs. Railtrack contracts-out the maintenance of their infrastructure to maintenance companies and renewal companies. Railtrack is supposed to manage the maintenance data, and judge the necessity of irregular maintenance or replacement of the infrastructure, and of operational restrictions such as limitation of the maximum operation speed. The safety standards called RGS are formulated by RSSD, and Railtrack had been responsible for managing all safety-related data and report.
	Railtrack: Dispatchers	The PSB in Railtrack monitors the location of operated trains by detecting the signal current running in the rails. (In this accident analysis, other types of controls are out of focus, so the location detection system only is reflected to the model.)
	Train Operating Companies (TOCs)	TOCs are the franchised operating companies. They own and operate trains under the signal control of Railtrack. At the time of the accident, there were 25 franchises in the industry.
	Maintenance Contractor	Maintenance contractors are responsible for inspecting tracks and conducting day-to-day maintenance operations in accordance with standards and directives from Railtrack, and for reporting the results from any inspections to Railtrack
	Renewal Contractor	Renewal contractors are responsible for conducting renewal operations (i.e. major repairs) in accordance with directives from Railtrack.
	Infrastructure (rails)	Tracks physically guide trains.
	Infrastructure (signal system)	Signal systems visually indicate go/stop to drivers using inputs from dispatchers, as well as the location of other trains provided by track circuits. They also send information to the on-board braking/warning systems such as *automatic warning system* (AWS) and *automatic train protection* (ATP).

- **Step 4: Proximal Event Chain**

  According to the accident report, the proximal event chain is developed as follows:

  i. *Balfour Beatty* reported about the crack of the rails around the accident site.
  ii. Railtrack did not comply with standards; they did not implement temporary speed restriction, and did not replace the rails within six months.
  iii. Railtrack postponed the replacement to avoid the interference by the time-requiring work during the profitable summer period.
  iv. *Balfour Beatty* did not comply with standards in maintenance, not correctly coping with the cracks.
  v. Ultra-sonic testing was conducted. Although the results implied the anomalies of the rails, Railtrack did not implement temporary speed restriction or make the timing of the replacement earlier.
  vi. The train operated on the rails fractured them into more than 300 pieces and the derailment occurred.

- **Step 5: Analyzing the Physical Process**

  In this accident, the physical system such as the train and its control system had worked soundly until the rails broke. The rails were broken due to inadequate maintenance of metal fatigue, known as *Rolling Contact Fatigue* (RCF) or more specifically, *Gauge Corner Cracking* (GCC), caused by the passage of trains. This analysis does not focus on their mechanism or monitoring method.

- **Step 6: Analyzing the Higher Levels of the Safety Control Structure**

  In this step, the higher-level safety control structures are analyzed. Specifically, analyses at three different levels are conducted below: Maintenance/operation management level, company management level (Railtrack), and system development level.

  - **Maintenance/operation Management Level Analysis**

    Violation of safety constraints and flaws in control actions and process models in maintenance/renewal and operation are analyzed here, focusing on the control structure in Figure 3-3. The analysis results are organized in Table 3-2.

    In this accident, there were critical problems both in maintenance and operation. The maintenance company, *Balfour Beatty*, did not comply with the standards (GDS); e.g., they handled defects of

rails with an inappropriate prioritization, implemented visual check in an inappropriate method, and did not corroborate the ultrasonic findings in the derailment zone. Railtrack's inappropriate decision on the timing of renewal of rails, in addition to these factors, led to the delay of the renewal of the rails in the derailment area. Additionally, some workers were not properly trained to identify a rail fracture (RCF), which represents a serious rail condition. In operation, Railtrack did not comply with the regulation, not restricting the operational speed of trains around the derailment area after they realized the cracks of the rails. Also, the dispatchers in Railtrack coped with NDA inadequately, which represents there is a signal problem in a specific track that could be caused by serious rail breaks. They received NDA from the zone that included the accident site, but he did not much care about the alert; the system frequently had an error, and receiving NDA was an ordinary event for them. Even though NDA does not necessarily mean rail problems such as rail cracks, Railtrack should have tackled this issue more proactively.

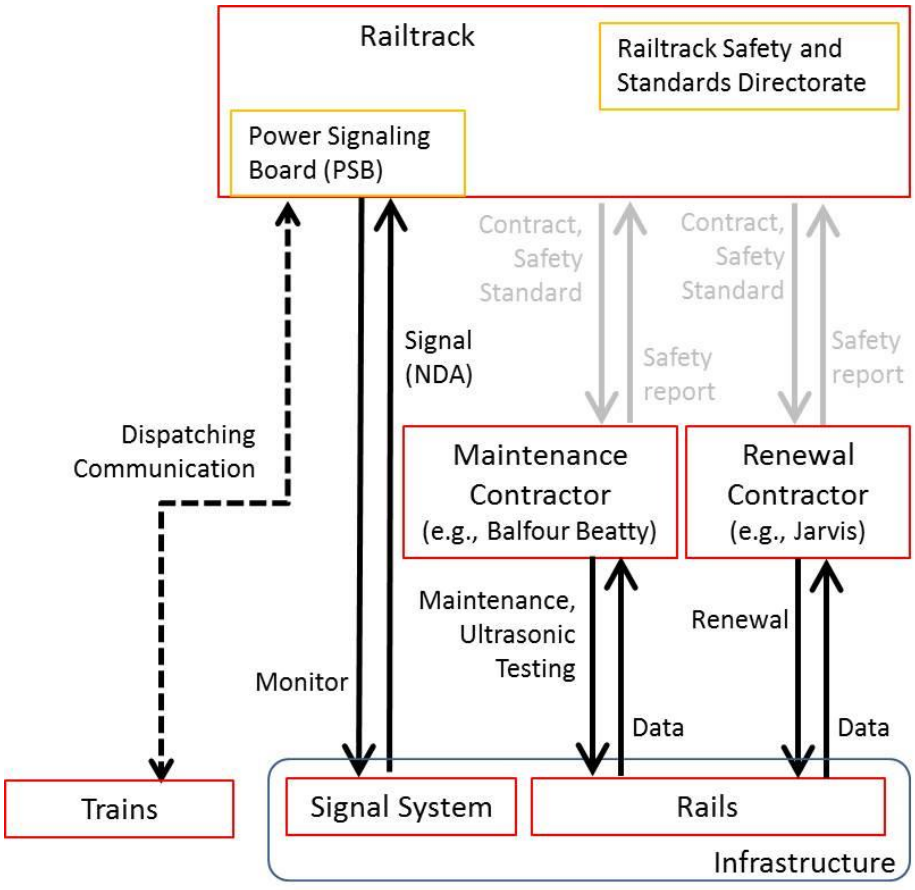

Figure 3-3 Control Structure (Maintenance and Operation)

Table 3-2 Analysis at a maintenance/operation management level

Safety Constraints Violated
• Rails must be maintained in compliance with the relevant standards and regulations. • Defects of rails or their precursors must be detected and applied to the maintenance. • Operation must be restricted correctly according to the condition of the rails. • Judgment in restricting the operation must be reasonable
Context
• The replacement of the rails postponed many times to avoid interfering with the commercial train operation. • According to the operation manual for dispatchers at this time, NDA did not require them to restrict operation.
Unsafe Decisions and Control Actions
• Inadequate implementation of temporary speed restriction.(Railtrack) • Inadequate implementation of maintenance/renewal (maintenance contractors) • Inadequate judgment on maintenance data. (maintenance contractors, Railtrack) • Inadequate compliance with regulation (Railtrack) • Inadequate monitoring of control signals (Railtrack)
Process Model Flaws
• Inadequate understanding of the rail maintenance method to achieve safety (maintenance contractors, Railtrack) • Inadequate understanding of the symptom and risk of RCF (*Balfour Beatty*) • Inappropriate timing of maintenance/renewal (Railtrack) • Lack of risk awareness of NDA (Railtrack)

- **Company Management Level Analysis (Railtrack)**

  The inadequate management by Railtrack is the most crucial factor in this accident. The safety control between Railtrack and maintenance/renewal contractors is discussed below, focusing on the control structure in Figure 3-4. The analysis results are organized in Table 3-3.

  After the privatization, achieving high profitability was one of the primary focuses of Railtrack's management, and managerial decisions of Railtrack were not adequately safety-oriented. For example, Railtrack drastically reduced the number of maintenance workers, and mitigated safety standards. Also, Railtrack made contract with a consulting company, *McKinsey & Company, Inc.*, and Railtrack adopted their cost-reduction advice that recommended not to replace rails periodically, but to replace them according to the necessity based on the maintenance reports from maintenance companies. Based on this decision, Railtrack reduced the frequency of maintenance. Also, they mitigated safety standards (e.g., reducing the number of people for visual check of rails) to reduce the cost. However, in spite of these aggressive decisions, Railtrack did not administer either the maintenance records or asset tracking record, so they could not prioritize risks of rails, or plan the long-term schedule of maintenance.

Additionally, although the rail cracks of the derailment area had already been reported by the maintenance contractor, Railtrack failed to place high safety priority on this area due to the inappropriate management. To make the matter worse, they infringed the regulation that requires the implementation of temporary speed restriction or replacement of the rails within six months after they receive a report about rail cracks. Furthermore, Railtrack postponed the renewal of the rails to avoid its interference with commercial operation by the time-requiring work during the lucrative summer period. Also, ultrasonic testing was conducted by a maintenance company, but in spite of the results implying the anomalies of the rails, Railtrack did not implement temporary speed restriction or replace the rails at an earlier timing.

In light of the process model of Railtrack, they did not adequately estimate the safety risk in changing the maintenance approach. Another problem in its process model was that Railtrack Headquarter did not understand the skill level, experience level, and management condition of some contractors due to the enormous organizational size of Railtrack and extremely fragmented industries. For example, there was an event that even though the zone manager of the accident site of Railtrack signed a certificate to inform Railtrack Headquarter that *Balfour Beatty* was not in compliance with standards, he did not. This is clearly because safety was not a core value in Railtrack's decision making. It is reasonable to say that the lack of the mechanisms to develop a safety culture among Railtrack's employees such as safety education and training and of adequate internal safety audit are the indirect yet crucial factor of this accident.

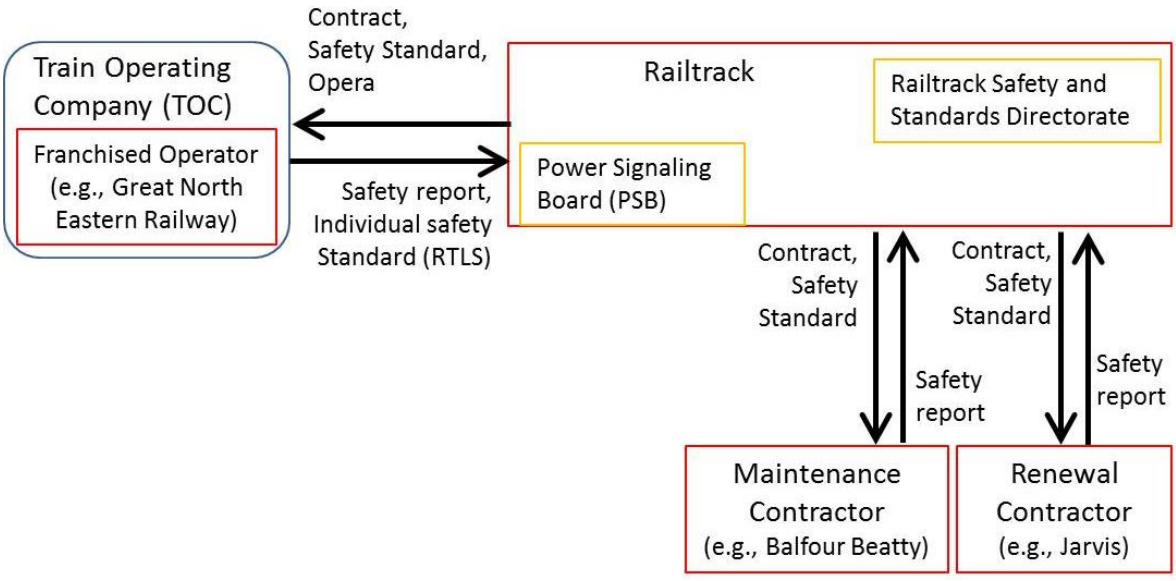

Figure 3-4 Control Structure (Corporate Management of Railtrack)

Table 3-3 Analysis at a company management level

Safety-Related Responsibilities of Railtrack
• Plan and implement the maintenance/replacement of infrastructure by making contracts with maintenance companies. • Establish safety standards (RGS), and enforce maintenance companies to comply with them. • Administer maintenance records and reflect them to the future maintenance plan. • Restrict operational speed according to the condition of the track. • Manage their own business by achieving both profitability and safety. • Dispatchers in Railtrack monitor the location of trains in operation and cope with signal problems.
Safety Constraints Violated
• Rails must be maintained in compliance with the relevant standards and regulations • Standards and regulations on the maintenance must be reasonable • Defects of rails or their precursors must be detected and reflected to the maintenance
Context
• While there were excessively many operation or maintenance companies in this industry after privatization, Railtrack was the only one infrastructure owner. • Railtrack, instead of an external regulatory organization, was in charge of maintaining industry safety standards. • After the privatization, the profitability of Railtrack received many attentions from the government, industry, and citizens.
Unsafe Decisions and Control Actions
• Direct a maintenance/renewal at an inappropriate timing • Develop inadequate safety standards and make a contract based on them.
Process Model Flaws
• Railtrack did not understand the impact of changing standards. • Railtrack did not understand the skill level of contractors.

- **System Development High-Level Analysis**

  This high-level analysis focuses on the institutional design by the UK parliament (Table 3-4). First of all, the parliament did not adequately realize impact of the institutional design on the safety of the industry. Railtrack was expected to achieve profitability as a non-public company in spite of its managerial inflexibility – they only owned the infrastructure and were not in charge of the passenger service of which profitability could be enhanced by managerial efforts –, so the most straightforward way for Railtrack to reduce its expenditure was to cut the maintenance cost. Nevertheless, RSSD in Railtrack, instead of *Health and Safety Executive* (HSE) or ORR, had a safety-related regulatory function to develop and maintain industry safety standards and manage safety reports from the TOCs and maintenance contractors. Also, even though the industry was organized by extremely fragmented operators and maintenance contractors, there was no mechanism to confirm their safety capabilities; for example, ORR was responsible only for licensing TOCs based on only their financial information.

Table 3-4 Analysis at a system development level

Safety Constraints Violated
• Implement safety risk assessment in the privatization process • Design institutional structure that can have effective safety constraints.
Context
• One of the privatization policies under Thatcher's administration; e.g., British Airways (1987), British Petroleum (gradually privatized between 1979 and 1987), and British Telecom (1984) are other privatized organizations. • The political leader's shift from Thatcher to Major in 1992, from Conservative party to Labor party in 1997.
Unsafe Decisions and Control Actions
• Inadequate institutional design in allocating safety responsibility and safety regulatory responsibility in the industry.
Process Model Flaws
• Parliament did not realize the impact of the privatization and the institutional structure on the safety. • Inadequate estimation and expectation of profitability of the post-privatization rail industry.

- **Step 7: Examination of Overall Communication & Coordination**

  Coordination and communication are important aspects in this vertically-separated horizontally-fragmented organizational structure. For example, train drivers and dispatchers belonged to TOCs and Railtrack respectively, so Railtrack needed to communicate fluently with multiple operators of different companies to coordinate them under the same operation standards. Similarly, Railtrack needed to have close communication with maintenance companies such as *Balfour Beatty*, and need to coordinate them under the same maintenance standards. However, in reality, communication on rail maintenance was severely inadequate. For example, as mentioned in Step 6, the Railtrack headquarter did not initially realize that *Balfour Beatty* was not in compliance with the safety standards. Also, Railtrack did not realize that some workers in *Balfour Beatty* were not well trained to detect rolling contact fatigue; thereby, Railtrack did not know in which location the rails have serious damages. Another critical flaw in communication is that Railtrack had a significant safety regulatory responsibility at this time, and they did not share safety-related information with other organizations such as TOCs and ORR; Railtrack made decisions based on only their managerial criteria and their performance-driven, less safety-oriented culture, and no other institution could not tackle or even detect this problem.

- **Step 8: Dynamics and Migration to a High Risk State**

  The UK parliament, most of the UK citizens, and most of the workers in the UK rail industry believed that the privatization was going to be successful as well as many other privatized industries in the 1980's, focusing on profitability, managerial efficiency, or convenience for users. However, the drastic change of the institutional structure had a big impact on the industry's safety management even though the physical control system did not have a particular change. Additionally, the gradual increase in the number of passengers in the 1990's invisibly accelerated the accumulation of the mechanical fatigue of the rails used for frequently operation. While these safety risks were emerging, mitigation mechanisms of them such as external safety inspections, safety trainings, and safety cultures were not adequately adapted or developed. As a result, the safety state of this system in terms of exercising adequate safety constraints migrated to a risker state in this short span. This analysis draws an important lesson that it is crucial to understand the safety control structure of the whole industry and its dynamic change when the institutional structure of the system is reformed even if the physical system does not change.

- **Step 9: Recommendations**

  In this analysis, most of the information about the accident and relevant organizations are based on the accident report. The official report carefully analyzed the accident from multi-angled perspectives. With these lessons, the UK rail industry has already exercised many countermeasures and transformed the industry. The STAMP-based analysis performed in this thesis can also provide multi-angled views about the accident in an organized way, and deepen the analytic perspectives; e.g., while the focuses of the official accident report are identifying the causes of the accident, CAST, with its system based approach, can also provide well-organized insights for better design of the institutional structure and its safety constraints. The following points are not adequately discussed in the official report, but important from a system safety perspective.

  - The inadequate contractor management of Railtrack is mainly discussed as the direct cause of the accident in the accident report, but the official report does not discuss the safety culture in Railtrack; Railtrack did not have effective safety training or education for their employees, and the lack of adequate internal safety audit could be another cause of having poor safety culture. Not only how to regulate unsafe actions from the high level of the industrial hierarchy, but also how to establish safe-oriented activities from the bottom part of the hierarchy should be a key perspective for managing system safety.

- Communication and coordination are also crucial issues in this accident. In designing institutional structure, it is necessary to take into consideration that excessively fragmented industry could increase managerial burden to establish adequate communication, thus increasing safety risks. From a STAMP perspective, fragmenting the institutional structure can be regarded as adding structural complexity to the safety control structure. Thus, in order to manage these communication/coordination risks, strict safety constraints must be designed for the additional complexity of the system.
- As discussed in the step 8, it is crucial to understand the safety control structure of the whole industry and its dynamic change when the institutional structure is reformed, even if the physical system does not change. As the STAMP theory tells, systems involve not only physical domains but also relevant institutional domains, and safety is an emergent property of the systems.

3.1.3 Conclusion

This CAST analysis organized key safety factors systematically based on the STAMP-based perspectives, paying specific attention to the institutional level in the hierarchical control structure. As discussed in each step, there are many causal factors of this accident. As mentioned in Step 8, these analysis results represent that the institutional structure must be carefully designed, and safety risks related to it should be well-analyzed before the industrial structure changes and managed with appropriate safety constraints.

Required safety constraints for the problems described in this CAST analysis (i.e. system-based lessons from this accident) are organized in Section 3.3 together with lessons from another accident that is explained in the next section.

3.2 Case 2 – Wenzhou Train Collision –

As a second case for accident analysis, this research focuses on Wenzhou Train Collision, which occurred in China in 2011. China launched its national HSR services in 2008, and has been developing their network at a drastic rate. As of Nov. 2013, the total length of the HSR lines in operation in China is approximately 50% of that in the world [1]. However, its rapid growth had been sometimes controversial in terms of quality of construction and operational safety. The Wenzhou HSR accident underpinned this safety concern about its rapid growth in a tragic way. This case is expected to provide meaningful lessons for this research in that the Chinese HSR industry has a new industrial structure for HSR operations and system development, and that the physical system is the integration of domestically-developed technologies and internationally-supplied technologies, which is the same strategy as that of the US HSR.

There are several researchers that implemented CAST of this accident, and they typically clarified more diverse causal factors of the accident than what the official report mentions [4][5][65][78]. However, different researchers analyzed from different perspectives, so the lessons learned from the accident is not well organized in a consistent way. This research reviews these CAST analyses with a specific focus on the institutional structure, further deepen the analysis, and thereby reorganize the system-based lessons.

3.2.1 Summary of the Accident

On July 23, 2011, this tragic railway accident occurred in the suburbs of Wenzhou, Zhenjiang Province, China. The high speed train *D301* rear-ended another high speed train *D3115* at a speed of 99 km/h, falling four cars from the viaduct. This accident caused 40 fatalities and 172 injuries. The following is the flow of the event, according to the official accident report [78].

- 19.30 (approx.): A lightning strike causes a problem in the *LKD2-T1* type train control system installed at Wenzhou South *Train Control Center* (TCC). A fuse in data collection unit blows out, cutting off the electronic channel for messages to pass between trains and the TCC. As there are no trains on the section monitored by Wenzhou South TCC prior to the blowout, signals remain at green. Frequent lightning strikes also cause a fault in the track circuit of the 750m block section 5829AG between Yongjia station and Wenzhou South station. Due to the problem, the train will stop when it arrives at this section. A red zone warning flashed on the screen at Wenzhou South TCC indicating the problem in the 5829AG section.

- 19.39: Mr. Zang Kai, on duty at Wenzhou South TCC, spots the red zone warning[18], informs the main dispatch center in Shanghai (*Centralized Train Control* - CTC), and reports the problem to technicians at Wenzhou South TCC.
- 19.45: Technicians start to repair the fault, but are unable to resolve it prior to the accident.
- 19.51: Train *D3115*, bound for Wenzhou South station, arrives at Yongjia station, 15.56km north of Wenzhou South station.
- 19.54: The Shanghai dispatch center, already informed about the red zone warning from Wenzhou South station, notices that the red zone warning has not appeared on its screen, indicating a system failure. Shanghai warns Yongjia TCC and Wenzhou South TCC not to rely on the automatic mode of train dispatching and orders them to dispatch trains manually.
- 20.09: Shanghai informs the driver of *D3115* waiting at Yongjia station about the problem with the 5829AG block section. Shanghai says the *automatic train protection* (ATP) system on *D3115* will stop the train when it arrives at the 5829AG section. The driver can switch to driving according to visible line-side signals at a maximum speed of 20km/h and restart the train. When the train leaves section 5829AG, the ATP should start to receive normal signals again, and the train should automatically switch back to standard operating mode. Shanghai asks *D3115* to prepare to leave Yongjia station and head for block section 5829AG.
- 20.12: Train D301 arrives at Yongjia station.
- 20.14: Train D3115 departs Yongjia station.
- 20.21: Train D3115 arrives at section 5829AG and the automatic brake system functions. The driver attempts to change the driving mode as instructed to restart the train, but he fails. He tries three times, but each attempt fails.[19]
- 20.22 - 20.27: The driver of Train *D3115* tries six times to contact Shanghai dispatch center, but all attempts fail. Wenzhou South TCC tries three times to call the driver, but is unable to reach him.
- 20.24: Shanghai dispatch center instructs train *D301* to depart Yongjia station and head for Wenzhou South station. The driver of *D301*, who has received the order from Shanghai and has seen a green signal indicating there is no train on the line ahead, starts the train and departs Yongjia station. The signal should be showing a red aspect as *D3115* is in the 5829AG block

[18] Red zone warning at TCC represents that the track in the indicated zone is occupied by a train or that the track circuit in the zone has a trouble.

[19] The lightning caused several electronic equipment failures, including track circuit failure in 5829AG, TCC equipment failure, data communication failure between TCC and track circuits, and dispatching communication interruptions between the train and CTC dispatcher [4].

section, but it is green because the lightning strike has damaged the data collecting unit in the *LKD2-T1* system installed at Wenzhou TCC.

- 20.27: Wenzhou TCC reaches the driver of train *D3115* and learns that the train is stationary.
- 20.29.26: The driver of train *D3115* successfully changes the driving mode and restarts the train, proceeding at less than 20km/h.
- 20.29.32: Wenzhou TCC calls the driver of *D301* that is now very close to section 5829AG, and says: "Be careful D301! D3115 is ahead of you! Be careful!" The line goes dead. Train *D301* is already in section 5829AG (ATP did not work). The driver applies the manual brake.
- 20.30.05: Train *D301* travelling at 99km/h rear-ends *D3115*, which is moving at 16km/h, killing 40 and injuring 172.

Figure 3-5 represents schematics of the control system.

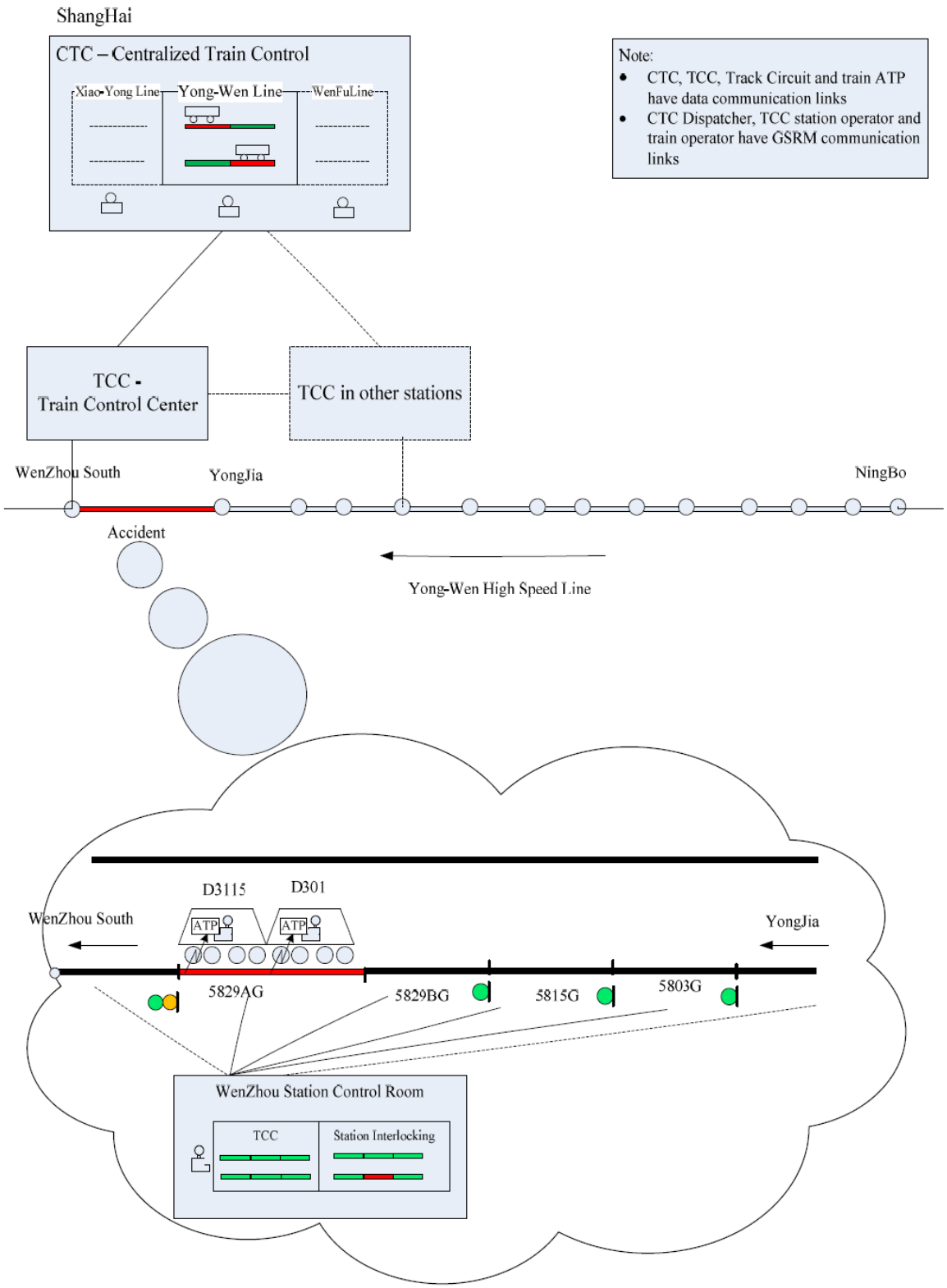

Figure 3-5 The schematic of the accident site and the control system [4]

3.2.2 Analysis

- **Official accident report**

  As a cause of this accident, the official report mentions “The disastrous crash was caused by serious design flaws in the train control system, inadequate safety procedure implemented by the authority and poor emergency response to system failure.” Specifically, the report refers to the following points as the main causes of this accident [78].

  - The train control system installed at Wenzhou South station, called *LKD2-T1*, is developed by *Signal & Communication's Beijing National Railway Research & Design Institute*, a subsidiary of *China Railway Signal & Communication Corporation* (CRSC). This R&D institute did not have a formal R&D team for the system and, therefore, failed to conduct a comprehensive assessment and testing before launching the system in commercial operation.
  - *Ministry of Railway* (MOR) did not play its role in the bidding, inspection and implementation of the *LKD2-T1* model, allowing it to be installed at Wenzhou South before sufficient testing had been completed.
  - Local railway staff at both Shanghai and Wenzhou poorly responded to the emergent situation, not notifying the driver of *D301* that *D3115* was ahead of it in a timely manner.

- **Control Structure**

  With these information, Dong and Suo develops a STAMP-based hierarchical model of the Chinese rail industry[4][5]. Figure 3-6 is a simplified control structure based on their models. The inadequate safety management that caused this accident lies in both the development phase of the malfunctioned signal system and the revenue operation phase, so the model includes both *System Development* and *System Operations*.

  The role of each organization in the structure is described in Table 3-5. CRSC described in the system development domain is the contractor of the signal and communication system of the Yong-Wen railway line and responsible for system integration of signal devices. *Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.* (CRSCD), a subordinate enterprise of CRSC, designed and developed the TCC system, referred to as *LKD2-T1*. In the system operations domain, *Shanghai Railway Bureau*, a regional bureau affiliated to the MOR, is responsible for supervising and implementing operation and maintenance of the total railway system. Thus, this Chinese HSR industry can be regarded as vertically integrated.

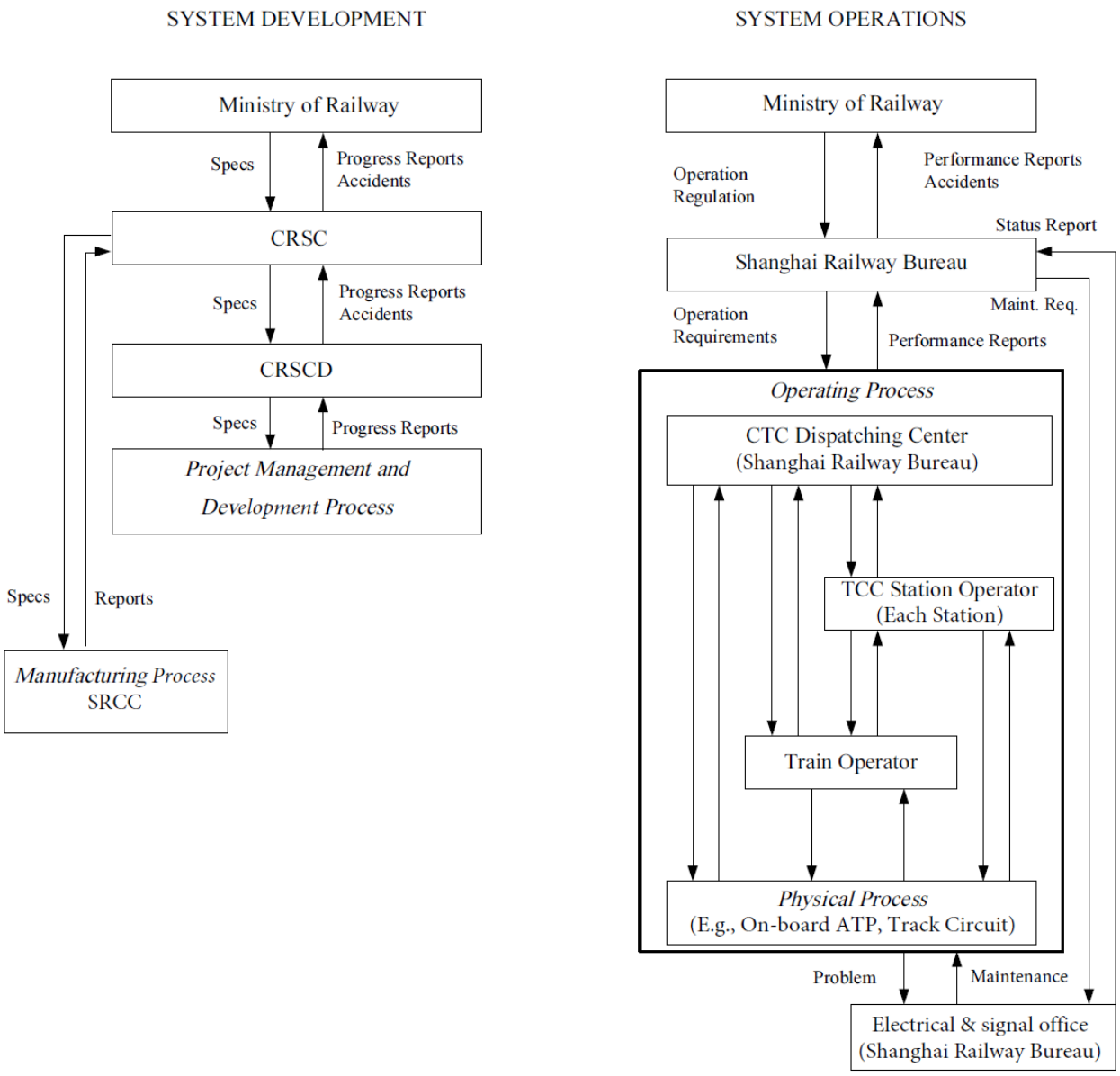

Figure 3-6 Safety control structure of the control system in the Chinese HSR (revised [4])

Table 3-5 Components of the control system and their responsibilities

	Main agencies in Chinese HSR Industry	Responsibility in the System
System Development	Chinese Ministry of Railways (MOR)	Governments regulation agencies
	China Railway Signal & Communication Corporation (CRSC)	Project Management
	Beijing National Railway Research & Design Institute of Signal & Communication Co. LTD (CRSCD)	Design and development of TCC system (LKD2-T1)
	Shanghai Railway Communication Company (SRCC)	Manufacturing of TCC system, subsidiary of CRSC
System Operations	Chinese Ministry of Railways (MOR)	Governments regulation agencies
	Shanghai Railway Bureau	Safety Assurance and Supervision, Operation, Maintenance
	Electrical & Signal Office (Shanghai Railway Bureau)	Maintenance of TCC system
	CTC dispatcher center (Shanghai Railway Bureau)	Management of the whole track/signal/train information, dispatching commands
	TCC (Wenzhou Station, Shanghai Railway Bureau)	Management of track/signal/train information in the segmented area, dispatching commands in emergency situations

- **Literature review**

  Dong, Suo, and Song discusses this accident mainly from three different perspectives: the operation process, the physical system, and the corporate management [4][5][65][78].

  - **Physical System**

    As discussed in Dong's and Suo's paper, the signal system, TCC, had a critical failure caused by the lightning, which led to sending output of no occupancy status of the track 5829AG and sending a wrong code that automatically brake *D3115*, which did not brake *D301*. The system design without the adequate consideration of these emergency situations resulted in this fail-out flawed system control.

  - **Operation**

    Dong discusses the situation of the Chinese high-speed railway industry in the world as an ambitious innovator of this field and she claims that this peer pressure might have inexplicitly caused performance pressure of the operators in the CTC and TCC. One officer in MOR also said that the operation staff were warned that delays would cut their bonuses [79]. Additionally, they did not have sufficient knowledge about the braking system in emergency situations, and did not

have sufficient practical experience or trainings for emergency operations. Poor communication hardware as well as these background factors led these operators to make the inadequate decisions, which are the crucial factors of the accident. Song discusses that Shanghai bureau did not take effective action to control the emergency situation caused by lightning.

- **Corporate Management and higher level**

  The official accident paper clarified that there were considerable managerial problems in the project. Dong and Suo discusses these issues in the context of inadequate hierarchical safety control structure, focusing on both system development and system operation. The following organizations had significant corporate management problems.

  - **MOR**

    In the system development process, MOR did not effectively enforce the signal system developer, CRSC, to conduct a comprehensive assessment and testing of the signal system before launching it in commercial operation; the possible errors were believed to be discovered after the commercial use. The tight schedule for the system development of the high-speed railway planned by MOR is also an issue lying behind the inadequate management of CRSC. According to the editorial [79], the signal system was developed over six months. Suo and Dong suggest the necessity of a dedicated department analyzing safety risks and supervising safety management in MOR for both development and operation phase.

  - **Shanghai Bureau**

    Shanghai Bureau had primary responsibility for enforcing its branches such as *Wenzhou South Station* to comply with safety regulations, but it was not sufficient. The emergency operation was not compliant with the regulation. Also, they did not provide sufficient training to the staff at their branches.

  - **CRSC**

    CRSC's poor management in supervising CRSCD led CRSCD to having no dedicated R&D team and focusing excessively on schedule or delivery, rather than safety. Dong discusses that CRSC did not provide sufficient documented manuals for TOCs and maintenance agencies.

- **Additional discussion**

  With a specific focus on the institutional structure, this research additionally discusses the following topics as safety-critical matters.

  - **Interaction between *System Development* and *System Operations***

    In the STAMP theory, the system development and system operations are connected by a feedback control called *Maintenance and Evolution*: system developers and its users must communicate about the operating procedures, environment, practical issues, and performance of the physical system, which should be continuously reflected to system development. However, the control structure of the Chinese HSR system totally lacked this linkage. According to Dong's research, "the project development team must provide complete operation and maintenance manuals to the operation and maintenance teams. The operation/maintenance team must provide detailed information about operational/maintenance problems they experience to the system design team." *Shanghai Bureau*, which was responsible for the total safety of the operation and maintenance, should have coordinated them and strictly supervise their management. Specifically, the managerial staff in the operation or maintenance division of *Shanghai Bureau* should have been involved in the development to reflect operation/maintenance perspectives to the system design. Also, CRSC should have had engagement, which should have been required by *Shanghai Bureau*, to keep improvement of their system for several decades based on the feedback of the actual operation, not just engagement for the initial development. And on the top of these aspects, safety culture that urges any operational workers to take a proactive action to improve the safety level at any time should have been developed: the mechanism to develop the safety culture should have been incorporated into the project planning.

    One of the unique points in the Chinese HSR development is that MOR took a strategy to develop its signal system by itself while MOR introduced high-speed trains from international suppliers or built them under technology transfer agreements with those suppliers. There are many countries that successfully self-developed or introduced a HSR system, and thus, MOR might have had overconfidence about the safety of the system due to successful cases of other countries or HSR's long safe history in other countries such as Japan. The important viewpoint is safety-proven trains do not necessarily guarantee the safety of the total system: trains are just one component in rail systems, and other components such as signal system, operation processes, maintenance processes, regulations, and their interactions should be taken into consideration in the project planning processes. Infrastructure development projects such as HSR projects could entail this

system integration tasks due to regulations or political reasons; e.g., in the US, there is a regulation that requires final assembly of trains to be conducted in the US domestically, so US railroads cannot simply import HSR trains from international suppliers. The key lesson learned by this case is that it is importance to design appropriate safety constraints for system integration, especially between self-developed domain and externally-introduced domain.

- **Excessively multi-layered, top-down hierarchy in the system development**

  Excessively multi-layered organizational hierarchy in system development contributed to inadequate safety management in the system development processes. This can be contrasted with Boeing's project management issue. Boeing Co. (Boeing) had grave managerial problems in the *787 Dreamliner* development, which caused 40-month project delay and approximately $10 billion cost overrun [49][50]. Additionally, the newly developed airplanes produced several safety-related incidents such as thermal runaway in their lithium-ion batteries, of which detailed causes are not yet clarified as of May 2014. Boeing introduced a worldwide supply chain to reduce its project cost, outsourcing more than 70% of the total manufacturing process. It is said that inadequate supplier management is one of the crucial causes of the malfunctioned project; some of the tier 2 and tier3 subcontractors did not follow Boeing's rules and specification, and Boeing did not realize them for several months [50][51]. A similar issue can be seen in the R&D managerial hierarchy of the Chinese HSR project. Specifically, the construction of the high-speed line, including the development of the signal system, was implemented by *Coastal Railway*, which was a state-own company invested by *Shanghai Bureau* and the local provincial government [4], and therefore, MOR indirectly managed the system developer (CRSCD) with three managerial buffers (*Shanghai Bureau*, *Coastal Railway*, and CRSC). This multi-layered managerial hierarchy and a demanding time constraint for the technology development is one of the causes of MOR's inadequate attention to the safety management of the lower players in the hierarchy, similarly to Boeing's case. The institution to take full responsibility for the total system integration – the total system includes not only physical system but also employee management, operation, maintenance, and evolution – should have been specified and had a tight-knit long-term relationship with relevant system developers such as CRSCD. In Japan, R&D on HSR signal systems and trains are mostly conducted by the initiative of railway companies, which are also in charge of both operation and maintenance. Those railway companies take full responsibility to develop new systems working together with specialized manufacturers and to evolve the systems incessantly for the following decades.

The excessively multi-layered hierarchy could cause another issue. At that time of the accident, corruption was a serious problem in the Chinese industry; some contracts were split into many sub-contracts for kickbacks. Bottom-level contractors of the hierarchy could use unskilled workers, or could substitute cheap materials for real ones, as other industries in China did at this time [84]. This may not be directly related to the Wenzhou Rail accident, but if these activities had been truly taken place, they could jeopardize the safety of the Chinese HSR in the future. As the case of the UK in Section 3-1 shows, strict rules and effective communication to manage subcontractors are required.

- **Certification**

  The certification given to CRSC by MOR was not based on thorough inspection or testing, and Suo and Dong suggest the necessity of a dedicated department in MOR for analyzing safety risks and supervising safety management. This is reasonable, but importantly, the safety division should have independency from other divisions, not being influenced by the project time, safety culture, and stakes of other agencies. In light of this and corruption culture in MOR [79], it would be better to establish a non-stakeholder third party to have the authority for certification, which can conduct thorough testing purely for safety.

3.2.3 Conclusion

This research reviewed several CAST analysis conducted by other researchers, and further analyzed safety issues with a specific focus on the institutional structure. In particular, this analysis focused on inadequate institutional design in the system development domain and inadequate safety interactions between the system development domain and system operations domain.

Required safety constraints for the problems described in this CAST analysis (i.e. system-based lessons from this accident) are organized in Section 3.3 together with lessons from *Hatfield Derailment* discussed in Section 3.1.

3.3 Key Lessons Learned from the Two CAST Analyses

This section represents Step 1-7 of the proposed methodology in Section 2.2. In order to apply the lessons learned from the CAST analyses to the STPA analysis of the NEC HSR, those lessons need to be transplanted as safety requirements or constraints of the system. With analysis results of the two accident cases, commonly important lessons applicable to both cases at the institutional level are organized as highly-desirable system requirements and safety constraints for generic railway industries in this section. The developed system requirements and safety constraints are incorporated into the development process of the generic HSR model in Chapter 4.

A. Maintenance management

a. Need an appropriate training that enables maintenance workers to identify a failure
b. Need to administer maintenance history appropriately
c. Need to leverage real-time-monitored data for future maintenance plan.
   *For fulfilling this requirement, installing an appropriate real-time monitoring system that can detect system flaws and their precursors is prerequisite.
d. Need to perform comprehensive risk analysis when maintenance rules change

B. Train operation management

a. Need an managerial structure to encourage operators to make safety-oriented decision without feeling performance pressure, including a training that enables operators to take appropriate actions in emergency situation

C. Corporate management of IMs

a. Need to administer information about contractors such as their skill levels, experience level, and corporate condition appropriately.
b. Managerial decision must be safety-oriented, based on an appropriate safety risk analysis

D. Corporate management in the system development domain

a. System development schedule must be sufficiently long for system integrator to conduct a comprehensive safety examination of the new system before starting its operation.
   *Examples of the “system” are parts for rolling stock and infrastructure, operation software, etc.
b. System integrator needs to realize the risk and perform comprehensive safety analysis in system integration, especially between self-developed domain and introduced domain from suppliers.

c. Need an appropriate communication channel with suppliers and outsourced companies to share correct, complete, and up-to-date information

E. The entire system, general

a. Need an appropriate structure to monitor financial/managerial capability of safety-related organizations in the industry.
b. Need an appropriate structure by which information about operational/maintenance problems identified through daily operation is fed back to the future system renewal.
c. Need an appropriate system structure by which the system integrator conducts system development taking into account usability of train operators and maintenance companies both in regular operation and emergency operation.
d. Need an appropriate structure by which train operators and maintenance companies have sufficient technical and operational background information about the physical system from the system integrator.
e. Need to clarify the organization to take safety initiative in integrating the total system in system development processes.
f. Need an independent authority or third party from other institutions (operator, developer, etc.) that monitor the system development/operations processes, regulate them, and certify the developed/operated system. It must not be influenced by the time constraints of the development/operation and stakes of other institutions.

These safety constraints and system requirements identified with CAST are applied to the risk analysis of the NEC HSR in Section 4.1 as system-based lessons from past accidents.

CHAPTER 4. SYSTEM DEFINITION AND MODEL DEVELOPMENT

This Chapter represents Step 2 of the proposed methodology in Section 2.2. A generic HSR model is developed for comparative analysis, which can be regarded as preliminary risk analysis, with the NEC HSR models. The generic model is introduced, aiming at making it easier to develop and analyze multiple alterative models of the NEC HSR on the same basis. In Section 4.1, the total system and its boundary that this research focuses on for risk analysis of the NEC HSR is defined. In Section 4.2, the generic HSR model is developed based on the STAMP theory. Responsibilities and control actions of each system component are defined. In Section 4.3, institutional alternatives of the NEC HSR are discussed based on the latest industrial reports from key stakeholders of this project. Among the possible alternatives, this research narrows down its focus to three alternatives. Control structures for them are developed in Section 4.4. The comparative analysis between them and the generic HSR model is conducted in Section 4.5.

4.1 System Definition

The system-based lessons from past accidents discussed in Chapter 3 are incorporated into the system requirements and safety constraints defined in Section 4.1.4.

4.1.1 Define Accidents

This research focuses on passengers' safety. Accidents with automobiles at grade crossings or accidents of maintenance workers are not considered in this research, even though those aspects are also significantly important in risk managements. In general, the following accidents are the main modes of railway accidents, which can lead to a personal injury or loss.[20]

- Train derailment
- Train collision
- Train fire
- Passenger injured by train equipment

[20] This analysis focuses on an institutional level, and thus, different types of accidents do not make a significant difference in defining system requirements and safety constraints at the institutional level. For example, there is little difference in the managerial requirement for TOCs between in the case of train derailment and collision, while train operators would have different requirements between them. In fact, the high-level hazard defined in Section 4.1.3 does not incorporate perspectives of specific accidents. Therefore, in the following analysis, any specific accident mode is not mentioned.

4.1.2 Draw a System Boundary

- **Project processes**

  HSR projects are comprised of various processes. In order to develop control models and perform risk analysis, it is necessary to specify processes on which this thesis focuses. Figure 4-1 represents a process flow of a typical HSR project development and operation.

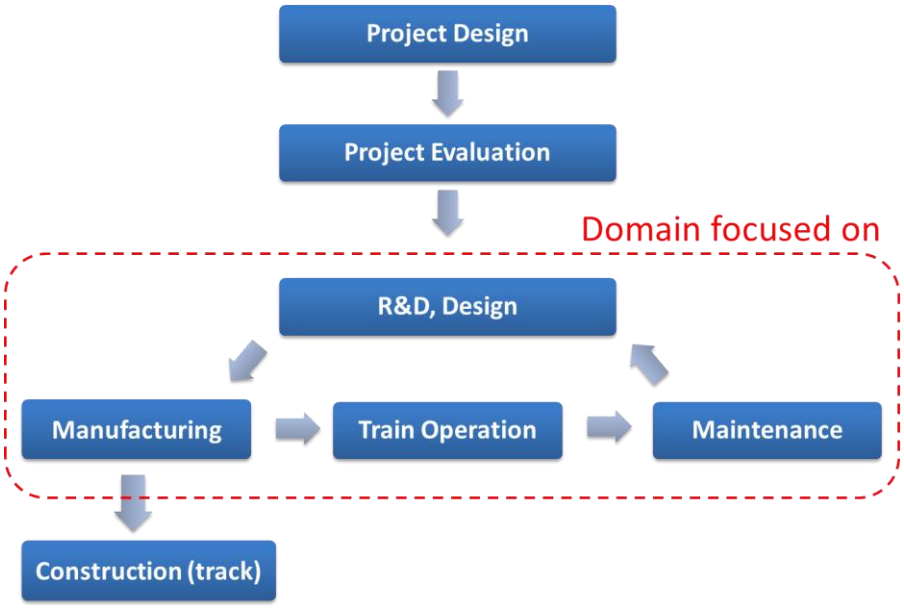

Figure 4-1 Project Development and Operation Flow Diagram

In emerging markets for HSRs, the first process is *Project Design*, in which multiple feasible plans about the institutional structure, route, capacity, and other basic specifications of the system are developed as alternatives. In the next *Project Evaluation* phase, those alternatives are evaluated and compared, through implementing evaluation processes such as *Environmental Impact Assessment*, *Cost-Benefit Analysis*, *Demand Analysis*, or *Service Development Planning* [17]. In reality, projects typically go back and forth between these initial two phases. In the *R&D/Design* phase, physical systems such as a signal system, control system, rolling stock, and operation system are developed for starting commercial operation and improved for system evolution after the commercialization. In the system evolution phase, *R&D/Design* process is repeated as one process in the lifecycle that also includes *manufacturing*, *train operation*, and *maintenance* processes. In this research, CAST of the Hatfield accident focused on the state of the railway industry after privatization that includes *train operation* and *maintenance* processes, and *project design* process is also discussed in terms of the institutional design by the parliament. CAST of the Wenzhou accident focuses on the state after the

commercialization that includes *train operation* process and the R&D/design process before/after the commercialization were mainly analyzed. The risk analysis of the NEC HSR in Chapter 4 and 5 focuses on *R&D, Design, Manufacturing, Train Operation,* and *Maintenance* processes as a total system modeled with safety control structures; thus, *project design, project evaluation,* or *construction (track)* processes are out of the boundary of the total system.

- **Institutional level**

  Also, this research focuses on the institutional level of the total system. This "institutional level" specifically means regulatory and managerial activities in *R&D, Design, Manufacturing, Train Operation,* and *Maintenance* processes; i.e., the physical domains such as specific methods of maintenance, manufacturing, and train operation, or specific technologies related to infrastructure and rolling stock are not discussed in this research.

4.1.3 Define High-level System Hazards

The high level system hazard at an institutional level of railway industries is described as follows. To avoid disorganized or incomplete hazard identification in the subsequent steps, this hazard is defined to be broad and preliminary. The similar definition is made by Leveson in the risk analysis of NASA ITA [67].

- Poor safety-related decision-making and its implementation leading to an accident

This *safety-related decision-making* is defined as a decision made based on both managerial and technical aspects; this research focuses on an institutional level, in which safety-related decision-making is not necessarily performed only by pure technical perspectives.

4.1.4 Define System Requirements and Safety Constraints

The preliminary hazard defined in Section 4.1.3 can be translated into the following four high-level safety requirements and constraints at the institutional level.

I. Safety-related decision-making and its implementation must be based on correct, complete, and up-to-date information, complying with state-of-the-art safety standards and regulations.
II. Safety considerations must be critical in safety-related decision-making and its implementation.
III. Safety-related decision-making and its implementation must be done by qualified personnel.

IV. Safety analyses must be available and used throughout the processes in the system lifecycle, and must be continuously evolved.

Specific system requirements and safety constraints are organized based on these four items as follows, according to the system boundary defined in Section 4.1.2. The lessons from the past accidents discussed in Section 3.3 are this list, being represented, for example, by "(lesson A-b)." Also, some items are adopted from the risk analysis of NASA ITA conducted by Leveson [67].

- **Maintenance**
  - I. Safety-related decision-making and its implementation must be based on appropriate information, complying with state-of-the-art safety standards and regulations.
    - i. State-of-the art safety standards and regulation regarding maintenance must be established, implemented, enforced, and maintained.
    - ii. Qualified third parties must develop the state-of-the art safety standards and regulations regarding maintenance, being independent from programmatic aspects such as cost and schedule of the system development/operations and other stakes of other agencies. They must evolve safety standards and regulations as needed.
    - iii. A regulatory structure is necessary to monitor, evaluate, and certify safety-critical decision-making and its implementation in maintenance.
    - iv. Correct, complete, and up-to-date information about the physical system and maintenance must be available and used in safety-related decision-making and its implementation in maintenance. (Lesson E-d)
  - II. Safety considerations must be critical in safety-related decision-making and its implementation
    - i. Safety-related decision-making in maintenance must be independent from programmatic considerations, including cost, schedule, and performance.
    - ii. Safety-related decision-making in maintenance must be appropriately done, taking into account safety-related technical perspective
    - iii. Safety-related decision-making and its implementation in maintenance must continuously pursue future improvement of the safety based on safety-related data and experience acquired through maintenance. (Lesson E-b)

III. Safety-related decision-making and its implementation must be done by qualified personnel

i. Safety-related decision-making in maintenance must be credible (executed using credible personnel, technical requirements, and decision-making tools).

ii. Safety-related decision-making in maintenance must be clear and unambiguous with respect to authority, responsibility, and accountability.

iii. All safety-related decisions in maintenance, before being implemented, must have the approval of the technical decision-maker assigned responsibility for the technical decisions.

iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in maintenance.

v. Maintenance workers must be well-trained enough to identify any system failure and to manage emergent situations. (Lesson A-a)

vi. The skill levels and experience levels of an individual maintenance worker and financial/managerial capability of agencies involved in maintenance must be evaluated, certified, and constantly monitored. (Lesson E-a)

IV. Safety analyses must be available and used throughout the processes in the system lifecycle.

i. High-quality system hazard analyses of maintenance must be created.

ii. Personnel must have the capability to produce high-quality safety analyses.

iii. Engineers and managers must be trained to use the results of hazard analyses in their decision-making in maintenance. (Lesson C-b)

iv. Adequate resources must be applied to the hazard analysis process.

v. Hazard analysis results must be communicated in a timely manner to those who need them. A communication structure must be established that includes contractors and allows communication downward, upward, and sideways.

vi. Hazard analyses must be elaborated (refined and extended) and updated as the design evolves, maintenance processes change. (Lesson A-d)

vii. During maintenance, safety-related logs must be maintained and used as experience is acquired. All anomalies in maintenance must be evaluated for their potential to contribute to hazards. (Lesson A-b)

viii. During train operation, safety-related real-time monitored data must be analyzed and used for designing a future maintenance plan. (Lesson A-c)

- **Train operation**

I. Safety-related decision-making and its implementation must be based on correct, complete, and up-to-date information, complying with state-of-the-art safety standards and regulations.

i. State-of-the art safety standards and regulation regarding train operation must be established, implemented, enforced, and maintained.

ii. Qualified third parties must develop the state-of-the art safety standards and regulations regarding train operation, being independent from programmatic aspects such as cost and schedule of the system development/operations and other stakes of other agencies. They must evolve safety standards and regulations as needed.

iii. A regulatory structure is necessary to monitor, evaluate, and certify safety-critical decision-making and its implementation in train operation.

iv. Correct, complete, and up-to-date information about the physical system and train operation must be available and used in safety-related decision-making and its implementation in train operation. (Lesson E-d)

II. Safety considerations must be critical in safety-related decision-making and its implementation

i. Safety-related decision-making in train operation must be independent from programmatic considerations, including cost, schedule, and performance. (Lesson B-a)

ii. Safety-related decision-making in train operation must be appropriately done, taking into account safety-related technical perspectives.

iii. Safety-related decision-making and its implementation in train operation must continuously pursue future improvement of safety of the system based on safety-related data and experience acquired through train operation.(Lesson E-b)

III. Safety-related decision-making and its implementation must be done by qualified personnel and agencies

i. Safety-related decision-making in train operation must be credible (executed using credible personnel, technical requirements, and decision-making tools).

ii. Safety-related decision-making in train operation must be clear and unambiguous with respect to authority, responsibility, and accountability.

iii. All safety-related decisions in train operation, before being implemented, must have the approval of the technical decision-maker assigned responsibility for the technical decisions.

iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in train operation.

v. All operators involved in train operation must be well-trained enough to identify any system failure and to manage emergent situations. (Lesson B-a)

vi. The skill levels and experience levels of an individual operator and financial/managerial capability of agencies involved in train operation must be evaluated, certified, and constantly-monitored. (Lesson E-a)

IV. Safety analyses must be available and used throughout the processes in the system lifecycle.

i. High-quality system hazard analyses of train operation must be created.

ii. Personnel must have the capability to produce high-quality safety analyses.

iii. Engineers and managers must be trained to use the results of hazard analyses in their decision-making in train operation. (Lesson C-b)

iv. Adequate resources must be applied to the hazard analysis process.

v. Hazard analysis results must be communicated in a timely manner to those who need them. A communication structure must be established that includes contractors and allows communication downward, upward, and sideways.

vi. Hazard analyses must be elaborated (refined and extended) and updated as the design evolves, train operation processes changes.

vii. During train operation, safety-related logs must be maintained and used as experience is acquired. All anomalies in train operation must be evaluated for their potential to contribute to hazards.

- **R&D/Design/Manufacturing**

I. Safety-related decision-making and its implementation must be based on correct, complete, and up-to-date information, complying with state-of-the-art safety standards and regulations.

i. State-of-the art safety standards and regulation regarding system design must be established, implemented, enforced, and maintained.

ii. Qualified third parties must develop the state-of-the art safety standards and regulations regarding R&D/Design/Manufacturing, being independent from programmatic aspects such as cost and schedule of the system development/operations and other stakes of other agencies. They must evolve safety standards and regulations as needed.

iii. A regulatory structure is necessary to monitor, evaluate, and certify safety-critical decision-making and its implementation in R&D/Design/Manufacturing. (Lesson E-f)

iv. Correct, complete, and up-to-date information about R&D/Design/Manufacturing, train operation, and maintenance must be available and used in safety-related decision-making and its implementation in R&D/Design/Manufacturing. (Lesson D-c)

II. Safety considerations must be critical in safety-related decision-making and its implementation

i. Safety-related decision-making in R&D/Design/Manufacturing must be independent from programmatic considerations, including cost, schedule, and performance. (Lesson D-a)

ii. Safety-related decision-making in R&D/Design/Manufacturing must be appropriately done, taking into account safety-related technical perspectives.

III. Safety-related decision-making and its implementation must be done by qualified personnel

i. Safety-related decision-making in R&D/Design/Manufacturing must be credible (executed using credible personnel, technical requirements, and decision-making tools).

ii. Safety-related decision-making in R&D/Design/Manufacturing must be clear and unambiguous with respect to authority, responsibility, and accountability. (Lesson E-e)

iii. All safety-related decisions in R&D/Design/Manufacturing, before being implemented, must have the approval of the technical decision-maker assigned responsibility for the technical decisions.

iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in R&D/Design/Manufacturing.

v. Engineers involved in R&D/Design/Manufacturing must be well-trained enough to identify any safety-related system failure.

vi. The skill levels and experience levels of an individual engineer and financial/managerial capability of agencies involved in R&D/Design/Manufacturing must be evaluated, certified, and constantly-monitored. (Lesson E-a)

IV. Safety analyses must be available and used throughout the processes in the system lifecycle.

i. High-quality system hazard analyses of R&D/Design/Manufacturing must be created with caution to system interfaces such as a boundary between self-developed domain and introduced domain from other agencies, and with caution to usability of the system for system users in any possible situations, involving their perspectives in each step of system design/integration processes. (Lesson D-b, E-c)

ii. Personnel must have the capability to produce high-quality safety analyses.
iii. Engineers and managers must be trained to use the results of hazard analyses in their decision-making in R&D/Design/Manufacturing.
iv. Adequate resources must be applied to the hazard analysis process.
v. Hazard analysis results must be communicated in a timely manner to those who need them. A communication structure must be established that includes contractors and allows communication downward, upward, and sideways. (Lesson D-c)
vi. Hazard analyses must be elaborated (refined and extended) and updated as the design evolves.

As Leveson' s analysis shows [67], focusing on an institutional level typically requires deep understanding of the system to clarify specific safety constraints and system requirements because this clarification is typically done through a top-down approach from a few preliminary hazards. As shown in this research, CAST analyses performed in advance can facilitate analysts to identify key safety constraints and system requirements in this process efficiently.

4.2 Generic HSR Model

In this section, a generic HSR model is developed based on the system boundary defined in Section 4.1.2 and the system requirements and safety constraints defined in Section 4.1.4. Also, responsibilities, control actions, feedback, and a process model are defined for each component. As explained in Section 2.2, this generic HSR model can be regarded as the simplest structure that can meet all requirements from Section 4.1. This generic HSR model is introduced to help develop models of the complex unique institutional alternatives of the NEC HSR and highlight the structural differences, which can provide safety risks in the NEC HSR.

Figure 4-2 represents a safety control structure of the generic HSR model. Table 4-1 organizes responsibilities, control actions, feedback, and process models for each system component of the model.

In the hierarchical model, *System Development* is comprised of *R&D/Design/Manufacturing*, and *Train System Operations* is comprised of *Train Operation* and *Maintenance.* These activities are regulated by *Regulation/certification Agency*, which is located at the highest level of the model. Being regulated by it, TOC and IM manage train operation, providing operational directive/manual/training to frontline workers such as *Train Operator* and *Dispatcher*. This research defines that the generic HSR model represents a vertically integrated industry. Thus, TOC and IM are functions in the same organization. Also, TOC and IM are in charge of maintenance of the physical system, working with *Maintenance Company* that manages on-site *Maintenance Workers*. TOC and IM are also responsible for managing system development and evolution, providing safety specifications to *System Integrator*, which is in charge of integrating the entire physical system by handling supply chains comprised of *R&D Company/Suppliers* and *Manufacturer*. Also, this research does not analyze the physical domains in details such as specific technologies or operational processes in maintenance, manufacturing, or train operation, so they are simplified as controlled components *Physical System*; e.g., the interaction between *Train Operator* and *Dispatcher* are not discussed in this research.

Each component of the model represents a function to meet the defined system requirements and safety constraints: importantly, different components do not necessarily mean different organizations; e.g., TOC and IM are in the same company as this research defines the generic HSR model as a vertically integrated industry. Some HSR industries that have complex institutional structures, including institutional alternatives of the NEC HSR, could have multiple organizational boundaries in single component of this generic HSR model; e.g., there might be several TOCs in open access rail industries. Institutional

alternatives of the NEC HSR have this additional structural complexity, so different control models from this simple generic HSR model need to be additionally developed, which is discussed in Section 4.4.

With respect to corporate boundaries of the model, the following points can be seen in the actual HSR industries in operation.

- While large suppliers such as *Alston*, *Siemens*, and *Bombardier* play can play a role of *System Integrator* as a single organization; *System Integrator* could be played by cartels. In some cases, they are also in charge of maintenance.
- In some industries, TOC or IM plays additional roles in the model such as *System Integrator*, *R&D Company*, *Manufacturer*, or *Maintenance Company*.
- *Regulator* and *Certification Agency* could be different organizations.
- In open access industry, TOC could be multiple corporations.
- If infrastructure is owned by a different organization from IM, IM in the model would be decomposed into IM and *Infrastructure Owner*.

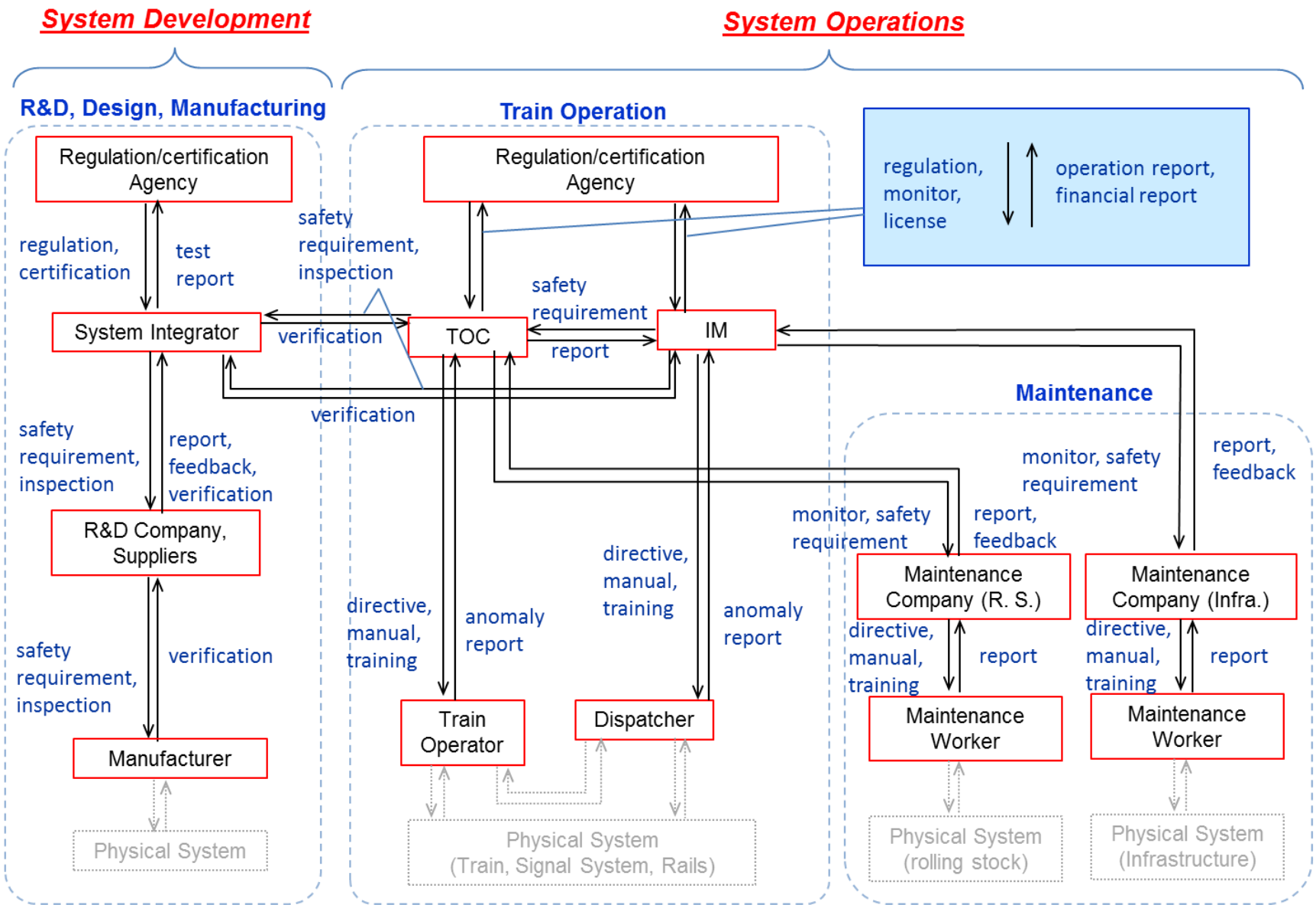

Figure 4-2 Safety control structure of the generic HSR model

Table 4-1 Responsibilities, control actions, feedback and process models (generic HSR model)

Components	Responsibility	Controlled Process	Control Action	Feedback	Process Model
Regulation/certification Agency (R&D, Design, Mfg.)	-develop safety standards and safety-related regulation about railway systems. -certify the developed system through the design and manufacturing processes.	System Integrator	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
System Integrator	-integrate railway system components for practical use such as a rolling stock, signal system, control system, and infrastructure from a technical, operational, and business perspective, based on the specification given by TOC and IM, complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
R&D Company, Suppliers	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
Manufacturer	-manufacture the components of the system	*Physical System*			
Regulation/certification Agency (Train operation, maintenance)	-develop safety standards and safety-related regulation about operation and maintenance. -license TOC and IM. -monitor the capability of these companies, checking financial and managerial condition.	TOC	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
		IM	regulation, license, monitor	operation report, financial report	
TOC	-manage train operation, designing operation schedule, frequency, fleet management plan, and operation manuals. -perform safety training and education to operators. - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. -design a specification for developing/updating rolling stock, and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator	Train Operator	operational directive, operation manual, training	anomaly report	knowledge about the developed system and operation, capability of operators, hazard analysis
		Maintenance Company (rolling stock)	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
		System Integrator	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis

(continued)

Components	Responsibility	Controlled Process	Control Action	Feedback	Process Model
IM	-own infrastructure and manage infrastructure operation such as operation regarding signal systems, station operation, etc. -perform safety training and education to dispatchers. -manage infrastructure operation, based on safety regulation and rules - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. - -design a specification for developing/updating infrastructure such as s signal system and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to dispatcher management	TOC	safety requirement	report	safety regulation about train operation, corporate safety operation rules, condition of operated trains and infrastructure
		Dispatcher	operational directive, operation manual, training	anomaly report	capability of Dispatcher, knowledge about the developed system and operation, capability of Dispatcher, hazard analysis
		Maintenance Company (infrastructure)	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
		System Integrator	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
Train Operator	-operate trains - report safety issues in operation, and manage them on the train	*Physical System*			
Dispatcher	-communicate with train operators and control train signals - report safety issues in operation, and manage them in the control center	*Physical System*			
Maintenance Company (rolling stock)	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to Train Operator.	Maintenance Worker (rolling stock)	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the rolling stock, capability of Maintenance Worker
Maintenance Company (infrastructure)	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to IM	Maintenance Worker (infrastructure)	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the infrastructure capability of Maintenance Worker
Maintenance Worker (rolling stock)	-conduct maintenance of rolling stock	*Physical System*			
Maintenance Worker (infrastructure)	-conduct maintenance of infrastructures	*Physical System*			

4.3 Institutional Alternatives of the NEC HSR

The project of the NEC HSR is still on the stage of discussing environmental impact, service, route, and regulations as of May 2014, and the institutional design is the next step. However, as many stakeholders have already been discussing, there are many possible alternatives for the institutional structure. This research insists that safety-related requirements and constraints, which are necessary for designing safety regulations, be defined, taking into consideration the possible variations of the alternatives.

In Section 4.3.1, the current institutional structure of the HSR operation (*Acela Express*) on the NEC and the planned institutional structure of the California HSR are introduced to understand the trend of institutional structures in the US. In Section 4.3.2, possible institutional alternatives of the NEC HSR are analyzed based on the latest industrial reports from key stakeholders of this project. After this intensive research, this research chooses specific three alternatives as cases for risk analysis. Main parameters differentiating these alternatives, which are defined in Section 1.3, are also clarified in this process.

4.3.1 Current Structure in the US

4.3.1.1 Case of the current NEC –*Acela Express*— [85]–[87]

The operation of the *Acela Express* started in 2000. It runs from Boston to Washington via New York, Philadelphia, and Baltimore, and is currently the only one high speed rail service operated in the U.S. The current NEC, where the *Acela Express* is operated, has one of the most complex institutional structures in the world. The 457-mile corridor runs through eight states and the District of Columbia. As shown in Figure 4-3, its infrastructure is owned by Amtrak and the several municipalities that it passes through. While eight different agencies operate commuter rails, Amtrak operates all intercity rail services, including the *Acela Express*. Freight trains are also operated by seven freight railroads on the same right-of-row. Thus, the major parameters of the institutional structure in the current *Acela Express* operation are organized as follows. These items are based on the definition in Section 1.3.

- Vertical structure : partially vertically separated
- Market competition : no competition[21]
- Private/public : public
- Dedicated/shared : shared

[21] This "no competition" means there is no other competitive rail service in this market, although Amtrak's intercity service, in reality, has inter-modal market competition.

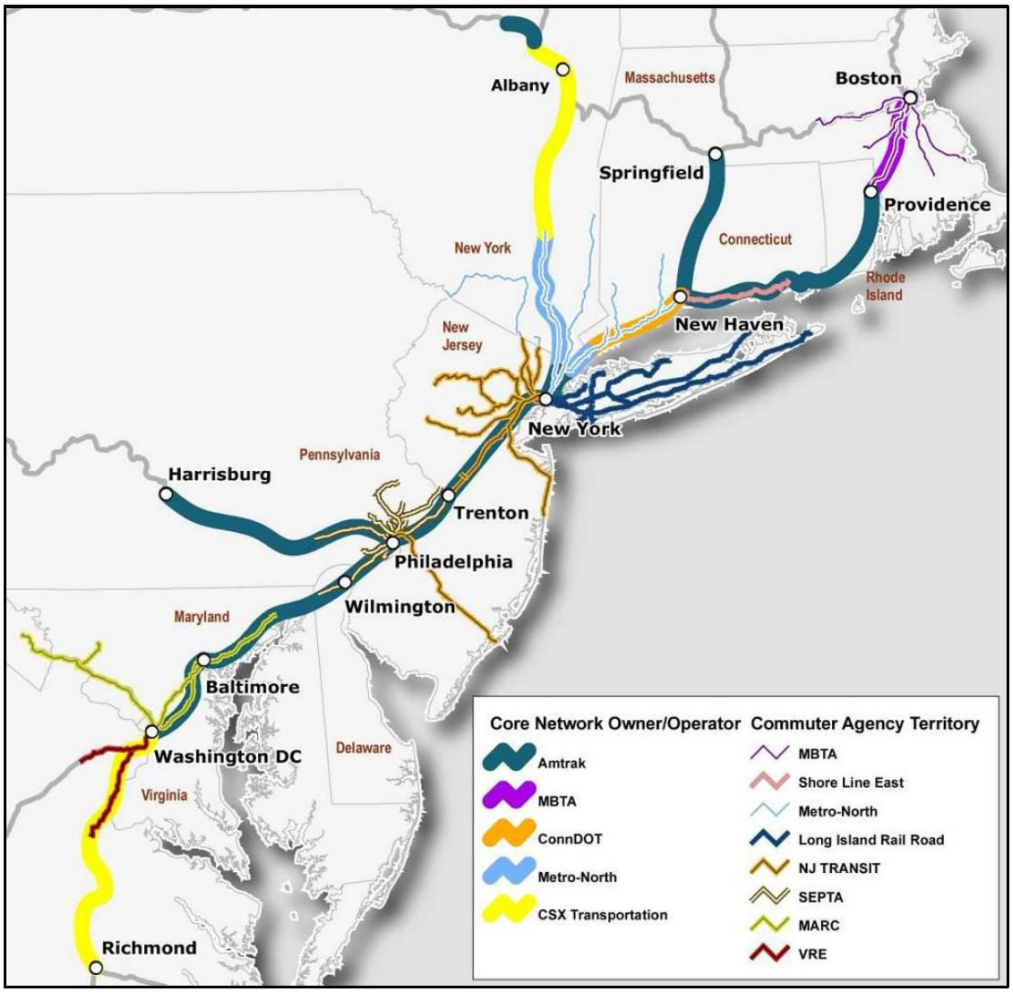

Figure 4-3 The current NEC ownership and operations [86]

4.3.1.2 Case of the California High Speed Rail

One of the most promising corridors in addition to the NEC is the California corridor. Although it was announced that the start of its construction delayed in September, 2013, this project is planned to start its commercial operation in the initial operating segment in 2022. *California High Speed Rail Authority* (CHSRA) is a state entity that is in charge of planning, designing, and constructing the high-speed rail system. CHSRA released its implementation plan several times that include discussion about the institutional structure in the project management and commercial operation [57][58]. Figure 4-4 represents the schematic of the institutional structure of this project.

CHSRA discusses the procurement methods such as DBM (*Design/Build/Maintenance*) and DBOM (*Design/Build/Operate/Maintenance*) [89] and expects the private sector to take the initiative in this

process, although this organization has not yet been specified. Regardless of the procurement method, the infrastructure is owned by the state, and the HSR operation will be in the charge of another (public or private) organization, so the institutional structure can be regarded as vertically separated. Additionally, CHSRA specifically mentions that it is desirable that a single operator would be responsible for providing a variety of services, which implies they would not introduce market competition in the high speed rail operation. Also, this corridor has a blended operation and service with the existing conventional lines [90][91]. Thus, the right-of-way for the high speed rail will be shared with the existing non-high speed services.

To sum up, the major parameters of the institutional structure in the California HSR are organized as follows.

- Vertical structure : vertically separated
- Market competition : desirably no competition
- Private/public : public, private (TBD)
- Dedicated/shared : shared

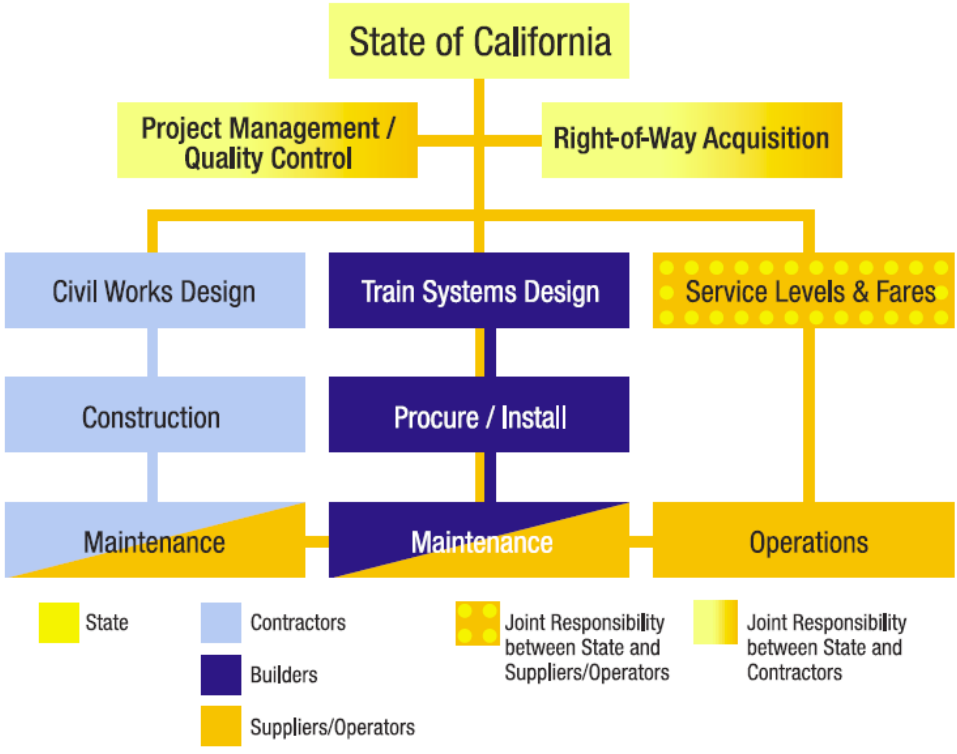

Figure 4-4 California High Speed Rail project structure [89]

4.3.1.3 New NEC HSR – literature reviews –

There are several key stakeholders of this project and research institutes discussing the institutional structure of the NEC HSR from various perspectives. Key industrial reports from each of them are organized below to identify reasonable alternatives focused in this research.

- **FRA**

  FRA is the institution that will make the most influential decision in the project development and implementation. Thus, their strategies are discussed first in this section.

  As a response to the *American Recovery and Reinvestment Act* (ARRA), FRA released the *High-Speed Rail Strategic Plan* in 2009, proposing 10 potential corridors, including the NEC [20]. This plan is mainly about the fund allocation provided by the ARRA. Additionally, FRA reported the *National Rail Plan* in accordance with the direction in the *Passenger Rail Investment and Improvement Act of 2008* (PRIIA). This report is groundwork for developing policies to improve the U.S. Rail systems, including HSRs [60][61]. In these reports, FRA did not discuss the institutional structure of specific corridors.

  In 2012, the *NEC FUTURE* program, which focuses only on the NEC and its intercity rail development, was launched under the initiative of FRA. This NEC FUTURE program mainly consists of two parts: the development of a *Service Development Plan* (SDP) focused on passenger rail service planning and possible alternatives for the corridor, and the preparation of *Environmental Impact Statement* (EIS) of these alternatives that is required under the *National Environmental Policy Act* (NEPA) [17]. In 2013, FRA announced the preliminary 15 alternatives of which the route and service environment are varied as shown in Figure 4-5 [18]. One of the potentially influential parameters in these alternatives on the safety control structures focused on the institutional level is whether the line is incrementally upgraded or newly constructed; the alternatives 1-11 are based on the incremental approach, and the alternatives 12-15 requires a new spine. The development of a new line would require the involvement of new infrastructure owner(s) and operators as well as new suppliers if these alternatives adopt new different technical systems from the current line such as maglev technologies.

With respect to the institutional structure, FRA implies the necessity of the involvement of the private sector in the NEC FUTURE report [17]. However, alternatives are being developed from the neutral standpoint about the institutional structure; they do not consider any specific structure.

Also, the possibility of introducing market competition by multiple HSR operators is not yet clarified.

Alt	Level	Network	Service Environment
1	A	Some increase in service and capacity along the existing NEC Spine	Conventional intercity/commuter
2			Conventional intercity/commuter
3			Introduce intra-urban metropolitan service
4	B	Increased service to existing and connecting markets along the existing NEC Spine	Conventional intercity/commuter
5			Focus: Maximize train frequency / service
6			Focus: Minimize travel time
7			Focus: Maximize one-seat ride options on and off NEC Spine
8	C	Targeted expansion of the existing NEC Spine to serve new markets, reduce trip time, and introduce robust regional services	Conventional intercity/commuter
9			Focus: Maximize train frequency / service
10			Focus: Minimize travel time
11			Focus: Maximize one-seat ride options on and off NEC Spine
12	D	2nd spine generally parallel to existing NEC	Dedicated high-speed rail; robust intercity and regional services on existing NEC Spine
13		2nd spine via Danbury-Hartford-Providence	
14		2nd spine via Suffolk-Hartford-Worcester	
15		2nd spine via Delmarva and Nassau-Stamford-Danbury-Springfield	

Figure 4-5 NEC preliminary alternatives [18]

- **NEC Master Plan Working Group and NEC Commission**

  The *NEC Master Plan* released in 2010 describes the required improvement to bring the current infrastructure of the NEC to a *state of good repair* and to accommodate the future growth in travel demand by 2030 [86]. This planning approach is regarded as a path breaking achievement to have a closer coordination among various operators on the NEC; this working group includes the representatives from Amtrak, the FRA, 12 northeastern states, the District of Columbia, and eight commuter railroads and three freight railroads. With regard to the HSR, although this plan clarified expected expenditures to incrementally improve the infrastructure for the future HSR operation, there is no specific proposal about how the ownership or operation of the NEC should be improved.

  Congress formed the *Northeast Corridor Infrastructure and Operations Advisory Commission* (*NEC Commission*) mandated by PRIIA, which is similarly comprised of each of the NEC states, Amtrak, and the U.S. Department of Transportation. While FRA's work in the NEC FUTURE program will not be finalized until 2015, this work is focusing on more immediate issues in the NEC infrastructure that lack adequate funding, and developing a comprehensive investment plan, based on the Master

Plan. As of May 2014, the discussion about the institutional structure is not yet made in this commission [94][95].

- **Amtrak**

  Amtrak is the current operator of the only high-speed train, *Acela Express*, and is proposing a plan to upgrade and renew the current NEC [63][64]. This plan is comprised of two programs, as shown in Figure 4-6: the *NEC Upgrade Program* (2015-2025), which incrementally transforms the current infrastructure into a state of good repair, improves the capacity of the NEC by procuring additional Acela trainsets and reduces travel time through track improvements, and *the NEC Next Generation HSR* (2025-2040), which constructs a fully new dedicated HSR right-of-way. However, this $150-billion "vision" is based on unpromising federal financing; Amtrak could not implement this plan by itself.

  Regarding the institutional structure, Amtrak's reports [63][64] suggest that Amtrak would be the only operator of the new HSR on the both upgraded and newly developed lines and that the upgraded infrastructure would be still owned by the current multiple states. While Amtrak expects the $150 billion funding from the federal government, the reports mention the importance of capital from the private sector, so the ownership of the Next-Gen HSR right-of-way could not be specified at this moment. However, it is not reasonable to assume from the reports that Amtrak welcomes private operators and market competitions with them.

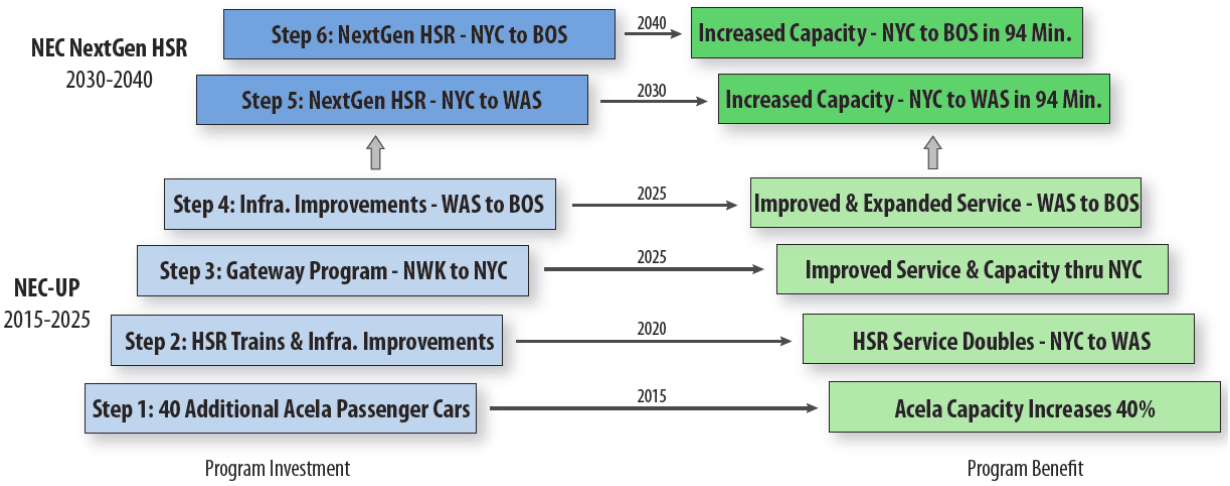

Figure 4-6 Stair-step phasing strategy [97]

- **Regional Plan Association (RPA)**

  RPA is an independent urban research and advocacy organization, having been providing influential ideas and recommendation for policy makers in New York-New Jersey-Connecticut metropolitan region for many years. *America 2050* is RPA's influential work on national infrastructure planning and policy program, and it also discusses the future of the NEC as one of the most important potential megaregions [65][66].

  RPA made a legislative proposal called *NEC NOW* in 2013 for the reauthorization of the expired PRIIA, recommending that the next funding bill, which is expected to be issued in 2014, authorizes the creation of a new corridor management and project delivery structure designed in *NEC NOW* [87]. Specifically, RPA recommends establishing an agency to implement this program, which involves representatives from the states on the NEC and Amtrak. While RPA supports the plan designed by the NEC Commission, it also proposes to develop new dedicated lines for the HSR to significantly reduce travel times and to increase capacity. Additionally, RPA mentions the benefit of open access system by introducing the European model, which implies its positive standpoint about the involvement of private operators and market competition.

- **University of Pennsylvania (UPENN)**

  From 2010 to 2012, University of Pennsylvania School of Design annually has proposed HSR design plans in the NEC with a specific focus on the urban development [100]–[102]. This program has been led by Robert Yaro, who is a professor of practice in the school and the president of *Regional Plan Association*. Similarly to RPA's proposal, the necessity of a new dedicated HSR line and the restoration of the existing lines is mentioned. Additionally, the involvement of private operators in both train and infrastructure operation is supported. For this purpose, UPENN proposes creating a public benefit corporation called *NEC Systems Authority* (NECSA) under DOT, which would become the owner of the both upgraded and newly constructed lines instead of Amtrak and take a comprehensive initiative in financing/designing/building/managing the HSR, franchising private operators, and developing new safety standards such as crashworthiness with regulators, as shown in Figure 4-7. According to UPENN's reports, Amtrak does not have adequate ability to comprehensively manage NEC's future.

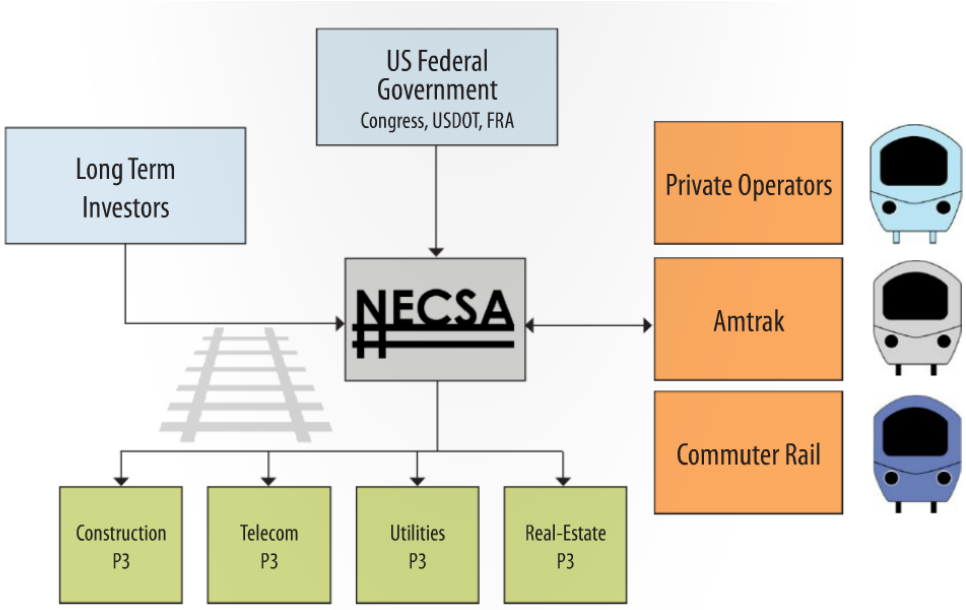

Figure 4-7 Proposed structure of NECSA [101]

- **Railroad Safety Advisory Committee (RSAC)**

  RSAC, established by FRA in 1996, is an advisory committee to provide advice on railroad safety to FRA. RSAC provides a forum for collaborative safety-related rulemaking with representatives from various stakeholders in the US rail industry, including railroads, labor unions, suppliers, and other interested agencies [103]. In *Engineering Task Force*, one of the working groups in RSAC, regulatory standards of high speed rails such as crashworthiness of HSR rolling stock are currently discussed. As introduced in Section 1.2, the *System Safety Program (49 CFR part 270 Proposed Rule in 2012)* is one of the most influential safety-related regulations currently discussed by RSAC. This is a safety regulation pursuant to *Rail Safety Improvement Act* (RSIA), which requires commuter and intercity passenger railroads to develop and implement a safety program to improve the safety of their operations from multi-angled perspectives such as corporate management, contractor management, safety culture, risk-based hazard analysis, and accident report and investigation.

  It can be assumed from these contents that this rulemaking is performed from a neutral standpoint, without assuming any specific technological system or institutional structure of the new HSR.

- **Other research institutions**

  There are many agencies discussing the institutional structure and alternatives of the NEC HSR. Sussman et al. performed a comprehensive analysis on the multimodal transportation system of the

NEC and its stakeholders using an engineering systems framework called the *CLIOS Process* (*Complex Large-scale Interconnected Open Sociotechnical Process*) [104]. They introduced a term, *bundle*, which represents a set of several decisions of the parameters about the institutional structure and technology of the NEC HSR. Specifically, the following four items are discussed:

1) Infrastructure structure : new dedicated line[22] vs. incrementally upgraded shared line
2) Infrastructure ownership : current Amtrak + states vs. new public owner
3) Vertical structure : vertically integrated vs. vertically separated
4) Competitive structure : open access vs. closed market

They concluded that it is beneficial for decision makers to incorporate flexibility to jump between the bundles to adapt the project to multiple economic, political, and technological uncertainties; this paper does not necessarily aim at identifying the optimal structure and flexibility to be incorporated in practice, but aim at validating the benefit of applying this engineering systems framework-based flexible design. With respect to the private sector, the authors mention that they would not be main players in the infrastructure ownership, but could be involved as operators if a new public infrastructure owner is established and considers market competition.

CALPRIG (*California Public Interest Research Group*) also reported an interesting discussion about the risks as well as benefits of the involvement of the private sector in the HSR construction and service, introducing failed international public-private partnership (PPP) cases [34]. According to them, the utilization of PPP would require various public commitments and understanding of the risks.

Thompson discusses problems with Amtrak's current ownership in the NEC, using cases of the rail industry reconstruction in the UK. This report claims that it is important to cut the "inertia" of the ownership cumulatively created in Amtrak's history, and to transfer the ownership from Amtrak to the DOT with subsequent leaseback either to Amtrak or another newly-created federal-state agency under new conditions [105]. In his latest report about the NEC HSR, he mentions that it is reasonable that the NEC infrastructure is owned by a public agency. Also, he mentions another type of NEC infrastructure ownership type like a DB (*Deutshe Bundesbahn*)-type organization, in which Amtrak acts as a holding company controlling both HSR operations and infrastructure, but infrastructure is

[22] In their report, the authors used *International Quality* to represent developing a new dedicated line, comparing to incrementally updating the existing line. The word international could be misleading because the incremental process could involves international technologies in renewing rolling stock and other systems, so in this paper, the term *new dedicated line* is used instead of *International Quality.*

operated by an independent subsidiary [106]. With these two options, he claims that vertical separation is an obvious solution in the NEC to clarify the economic performance of Amtrak as well as commuter operators on the same basis. Franchising or concessioning operation in the NEC is also mentioned as one possibility.

The Northeast Maglev (TNEM) is the US-based company closely working closely with the Central Japan Railway Company (JR Central), which operates the most intensive HSR from Tokyo to Osaka and takes an initiative for launching the world fastest *Superconducting Magnetic Levitation System* (SCMAGLEV) in Japan [107]. TNEM is committed to applying this maglev system to the NEC HSR. This innovative technology would require the construction of a dedicated right-of-way.

4.3.2 Alternatives Focused on in this Research

The alternatives for the institutional structure in the NEC HSR discussed in the previous chapter are integrated into the following Table 4-2 and 4-3. The alternatives that this research focuses on are chosen from these. Importantly, these lists do not necessarily include all of the possible alternatives or possibly involved organizations.

Table 4-2 Alternatives and parameters of the upgraded NEC HSR

Papameters\Alternatives	**Upgrade-1**	**Upgrade-2**	**Upgrade-3**	**Upgrade-4**	**Upgrade-5**
1 Infrastructure structure	upgrate				
2 Infrastructure ownership	Amtrak + states	new public agency			
3 Infrastructure manager	Amtrak + states	new public agency		Amtrak	
4 TOC(s)	Amtrak	Amtrak	Amtrak + private sector(s)	Amtrak	Amtrak + private sector(s)
Vertical structure	*integrated separated*	*separated*		*integrated*	*integrated separated*
Market competition	*no*	*no*	*open access*	*no*	*open access*
Involvement of private sector	*no*	*no*	*yes*	*no*	*yes*
FRA	neutral				
Master Plan	x	x		x	
NEC Commission	x	x		x	
Amtrak	x				
RPA	neutral				
UPENN		x	x		
RSAC	neutral				
Sussman *et al.*	x	x	x		
Thompson		x	x	x	x

This table is comprised of the alternatives for the incrementally upgraded HSR, which are specifically discussed in *NEC Master Plan*, *NEC Commission*, or *NEC NOW* of RPA. Each alternative has four independent parameters: 1) *Infrastructure structure*; 2) *Infrastructure ownership*; 3) *Infrastructure Manager*; and 4) *Train Operating Company (TOC)*. The other three parameters are automatically determined from these four independent parameters; *Vertical structure* is determined by parameter 3 and 4, and *Market competition* and *Involvement of private sector* are determined only by parameter 4 in this case. This paper assumes that the type of *Market competition* is "Intra-modal competition for the market" in Table 1-2. The bottom half of the table represents what alternatives each paper introduced in Section 4.3.1.3 proposes or discusses.

Upgrade-1 represents the current structure, in which Amtrak and multiple municipalities that the NEC line goes through, have the ownership and control of the NEC infrastructure. *Upgrade-2* and *-3* includes the new public ownership of the infrastructure, which is proposed by UPENN or Thompson. *Upgrade-4* and *-5*, which include leaseback of the control of the infrastructure from the new public owner to Amtrak, are the proposed approached by Thompson. *Upgrade-4* is defined as a vertically integrated structure, but it could be redefined as a vertically separation if Amtrak makes a subsidiary dedicated to the infrastructure operation like DB, as Thompson mentions. Also, although the HSR train operator could be a single private or public operator, this table does not include this option; this research presumes that the possibility of this approach is low, as there are few research/industrial reports about this approach in the updating process of the NEC. FRA, RPA, and RSAC discuss the NEC HSR from a neutral standpoint. Although RPA proposes creating a comprehensive project management agency, it is not specifying any parameters of this table.

Table 4-3 Alternatives and parameters of the new NEC HSR

Papameters\Alternatives		New-0	New-1	New-2	New-3	New-4	New-5	New-6
1	Infrastructure structure	none	new dedicated					
2	Infrastructure ownership		Amtrak		new public agency			
3	Infrastructure manager		Amtrak		new public agency		Amtrak	
4	TOC(s)		Amtrak	Amtrak + private sector(s)	Amtrak	Amtrak + private sector(s)	Amtrak	Amtrak + private sector(s)
Vertical structure			*integrated*	*integrated separated*	*separated*		*integrated*	*integrated separated*
Market competition			*no*	*open access*	*no*	*open access*	*no*	*open access*
Involvement of private sector			*no*	*yes*	*no*	*yes*	*no*	*yes*
FRA		neutral						
Master Plan								
NEC Commission								
Amtrak			x		(x)		(x)	
RPA			x	x	x	x	x	x
UPENN					x	x		
RSAC		neutral						
Sussman *et al.*		x	x		x	x		
Thompson			x	x	x	x	x	x

This table represents the alternatives for the new dedicated[23] HSR, which are mentioned by many agencies such as FRA (*NEC FUTURE*), Amtrak, RPA, UPENN, and Thompson. *New-0* represents the case when the new dedicated line is not constructed. *New-1* is proposed by Amtrak and Thompson, but Thompson critically mentions that, in this case, Amtrak should create an independent subsidiary to operate infrastructure for achieving vertical separation of the NEC infrastructure. *New-3* to *-6* is the same structure as *Upgrade-2* to *-5*. Even though the line is newly constructed, this research regards the possibility of the significant involvement of the private sector in the infrastructure ownership, as many publications mention. Also, the option to have a single public or private train operator could be possible but this research presumes this possibility, Amtrak is not involved in the train operation, is relatively low on account of the dominant expectation shown in Table 4-2 that the incrementally upgraded NEC intercity is basically operated Amtrak.[24] While FRA and RSAC discuss a new NEC HSR from a neutral standpoint, Amtrak and UPENN suggest specific structures.

[23] This "dedicated" does not necessarily mean the HSR trains run only on the HSR line. Specifically, the dedicated lines could be connected to the current tracks in urban areas, and in this case, HSR trains would have to be operated on the current tracks together with conventional passenger trains and freight trains.

[24] The safety risks related to the involvement of private train operator(s) can be complementally discussed by analyzing an *open access* case.

In practice, one of the alternatives from each list would be chosen; for example, if the authority decides not to change anything about the current NEC, the set of *Upgrade-1* and *New-0* represents the decision. However, this research deal with these alternatives independently, less taking into account the interaction between the structure of the upgraded NEC and that of new dedicated line. Specifically, the following three alternatives are chosen and analyzed in this research.

Alternative 1 (*Upgrade-1*): incrementally upgraded HSR with the current institutional structure.
Alternative 2 (*New-3*) : vertical separation with a new public ownership of the new dedicated line.
Alternative 3 (*New-6*) : open access with a new public ownership of the new dedicated line.

These highly-diverse alternatives are chosen to allow this research to analyze the safety impact of the difference in the institutional structure.

4.4 Safety Control Structures of the Alternatives

The next step is to develop safety control structures of the chosen three alternatives. The specific components in these models are presumed based on the key industrial reports discussed in Section 4.3, and their responsibilities, control actions, feedback, and process models are tailored from those of the generic HSR model. [25]

4.4.1 Alternative 1: Multiple Ownership / Upgraded Line

Figure 4-8 represents the control structure of Alternative 1.[26] According to this structure, the specific players in the industry for each component are organized in Table 4-4. Responsibilities, control actions, feedback, and process models in Table 4-4 are tailored from those of the generic HSR model in Table 4-1. In Alternative 1, the control structure is based on the current institutional structure of the HSR operation in the NEC; specifically, Amtrak is the sole TOC, and Amtrak and regional authorities are IMs. Although there are more than two IMs in the structure in reality, for simplify, this model only shows with two IMs that the industry has multiple IMs. TOC and IMs are individually coupled with *System Integrator* and *Maintenance Company*. *System Integrator (Rolling stock)* and *System Integrator (Infrastructure)* for Amtrak (TOC + IM) can be a single company. The individual regional authority has *System Integrator* focusing only on infrastructure-related equipment. These system integrators are either domestic or international companies, but at this moment, the possible agency is not specified at all. It is assumed in the model that these institutions are all regulated under the control of FRA. With respect to certification of the developed technologies, a third party, instead of FRA, could play the role, but this thesis assumes that FRA also takes this responsibility. Each system integrator works with R&D institutions and suppliers, which are also domestic or international agencies. Amtrak, in reality, also has maintenance workers to some extent, but the model assumes that maintenance contractors are the *Maintenance Companie*s, although the roles of *Maintenance Companies* could be assigned to the system integrators, R&D agencies, or suppliers of the system.

[25] In this process, the developed control structures can be regarded as "designed structures" by the author based on the generic HSR model, rather than the most "likely structures"; although the choice of the specific components in the models are presumed based on the key industrial reports, this information is still insufficient to describe the whole models. Whether these structures should be improved or not will be discussed later in this thesis from STAMP perspective.

[26] In this model, control actions and feedback are represented by single arrow, for simplicity.

Figure 4-8 Safety Control Structure of Alternative 1 “Multiple ownership / Upgraded line”

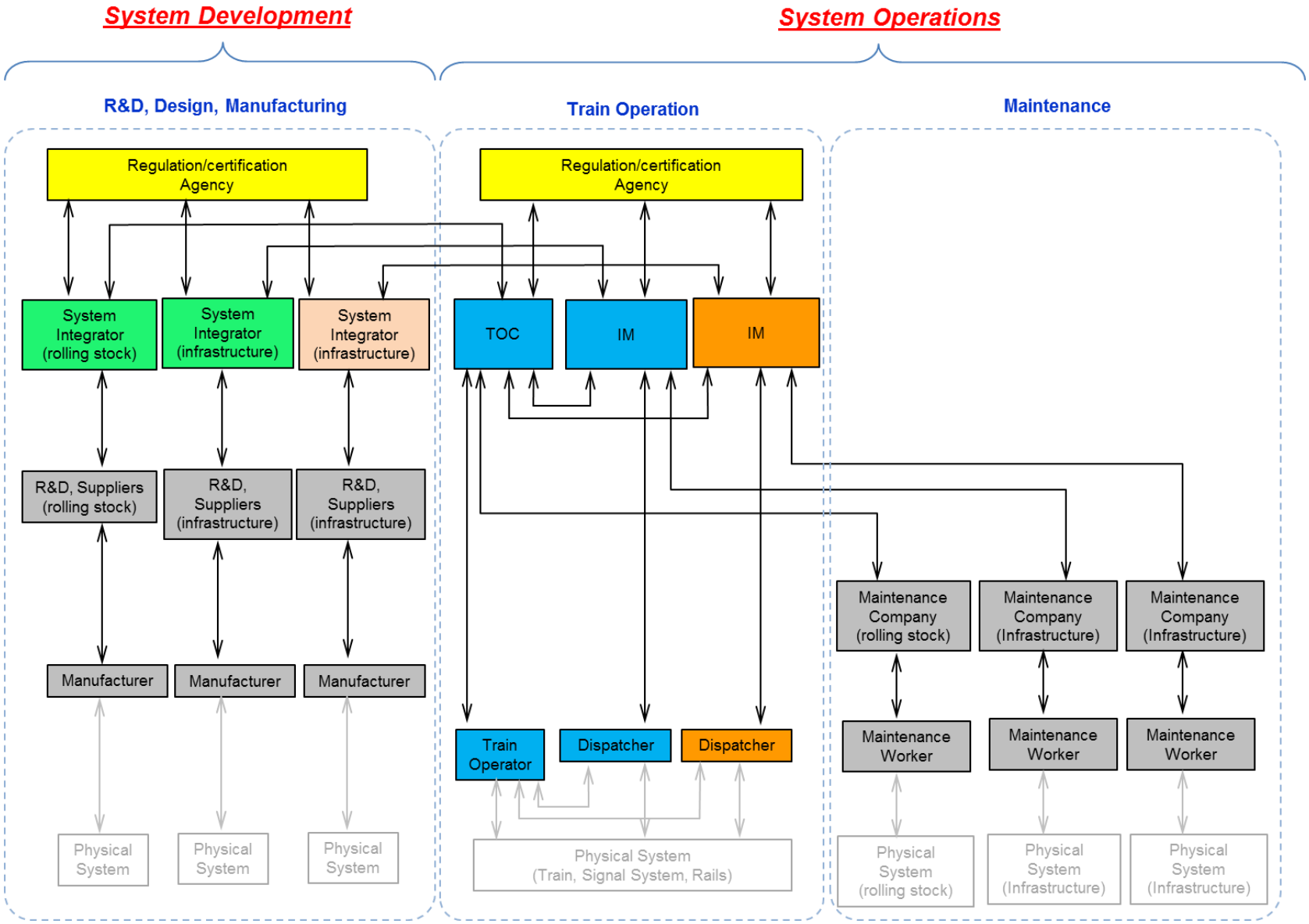

Table 4-4 Responsibilities, control actions, feedback and process models (Alternative 1)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
Regulation/certification Agency (R&D, Design, Mfg.)	*FRA*	-develop safety standards and safety-related regulation about railway systems. -certify the developed system through the design and manufacturing processes.	System Integrator (Rolling Stocks)	*domestic or international supplier*	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
			System Integrator (infrastructure)		regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
			System Integrator (infrastructure)	*domestic or international supplier*	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
System Integrator (Rolling Stocks)	*domestic or international supplier*	-integrate railway system components related to rolling stocks for practical use from a technical, operational, and business perspective, based on the specification given by TOC , complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers (rolling stocks)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
System Integrators (Infrastructure)		-integrate railway system components related to infrastructure for practical use from a technical, operational, and business perspective, based on the specification given by TOC , complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
	domestic or international supplier		R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
R&D Company, Suppliers (Rolling Stocks)	*domestic or international suppliers*	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer (Rolling Stocks)	*domestic or international manufacturers*	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer (infrastructure)	*domestic or international manufacturers*	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
Manufacturers	*domestic or international manufacturers*	-manufacture the components of the system	*Physical System*				

(continued)

Controllers	Presumed Players	Responsibility	Controlled Process	Presumed Players	Control Action	Feedback	Process Model
Regulation/certification Agency (Train operation, maintenance)	*FRA*	-develop safety standards and safety-related regulation about operation and maintenance. -licenseTOC and IM. -monitor the capability of these companies, checking financial and managerial condition.	TOC	*Amtrak*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
			IM	*Amtrak*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
				regional authorities	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
TOC	*Amtrak*	-manage train operation, designing operation schedule, frequency, fleet management plan, and operation manuals. -perform safety training and education to operators. - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. -design a specification for developing/updating rolling stocks, and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to train operator management	Train Operator	*Amtrak*	operational directive, operation manual, training	anomaly report	knowledge about the developed system and operation, capability of operators, hazard analysis
			Maintenance Company (rolling stocks)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (Rolling Stocks)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
IM		-own infrastructure and manage infrastructure operation such as operation regarding signal systems, station operation, etc. -perform safety training and education to dispatchers. -manage infrastructure operation, based on safety regulation and rules - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. - design a specification for developing/updating infrastructure such as s signal system and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to dispatcher management	TOC	*Amtrak*	safety requirement	report	safety regulation about train operation, corporate safety operation rules, condition of operated trains and infrastructure
			Dispatcher		operational directive, operation manual, training	anomaly report	capability of Dispatcher, knowledge about the developed system and operation, capability of Dispatcher, hazard analysis
			Maintenance Company (infrastructure)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis

(continued)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
IM	*regional authorities*	-own infrastructure and manage infrastructure operation such as operation regarding signal systems, station operation, etc. -perform safety training and education to dispatchers. -manage infrastructure operation, based on safety regulation and rules - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. - -design a specification for developing/updating infrastructure such as s signal system and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to dispatcher management	TOC	*Amtrak*	safety requirement	report	safety regulation about train operation, corporate safety operation rules, condition of operated trains and infrastructure
			Dispatcher	*regional authorities*	operational directive, operation manual, training	anomaly report	capability of Dispatcher, knowledge about the developed system and operation, capability of Dispatcher, hazard analysis
			Maintenance Company (infrastructure)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
Train Operator	*Amtrak*	-operate trains - report safety issues in operation, and manage them on the train	*Physical System*				
Dispatcher	*Amtrak*	-communicate with train operators and control train signals - report safety issues in operation, and manage them in the control center	*Physical System*				
Dispatcher	*regional authorities*	-communicate with train operators and control train signals - report safety issues in operation, and manage them in the control center	*Physical System*				
Maintenance Company (rolling stocks)	*contractors*	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to Train Operator.	Maintenance Worker (rolling stock)	*contractors*	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the rolling stocks, capability of Maintenance Worker
Maintenance Company (infrastructure)	*contractors*	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to IM	Maintenance Worker (infrastructure)	*contractors*	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the infrastructure capability of Maintenance Worker
Maintenance Workers	*contractors*	-conduct maintenance of rolling stocks	*Physical System*				

4.4.2 Alternative 2: Vertically Separated / New Line

Figure 4-9 represents the control structure of Alternative 2. According to this structure, the specific players in the industry for each component are organized in Table 4-5. Due to the structural similarity, responsibilities, control actions, feedback, and process models in Table 4-5 are identical to those of the generic HSR model in Table 4-1. This alternative has a similar structure to the generic HSR model. The regulators are assumed as FRA, as similarly presumed in Alternative 1. The industry has only one TOC, Amtrak, and one IM, a new public agency. They individually have contracts with *System Integrator*. These system integrators, R&D agencies, and suppliers can be domestic or international firms. Also, *Maintenance Companies* are assumed as contractors with Amtrak or the new public infrastructure owner.

Figure 4-9 Safety Control Structure of Alternative 2 “Vertically separated / New line”

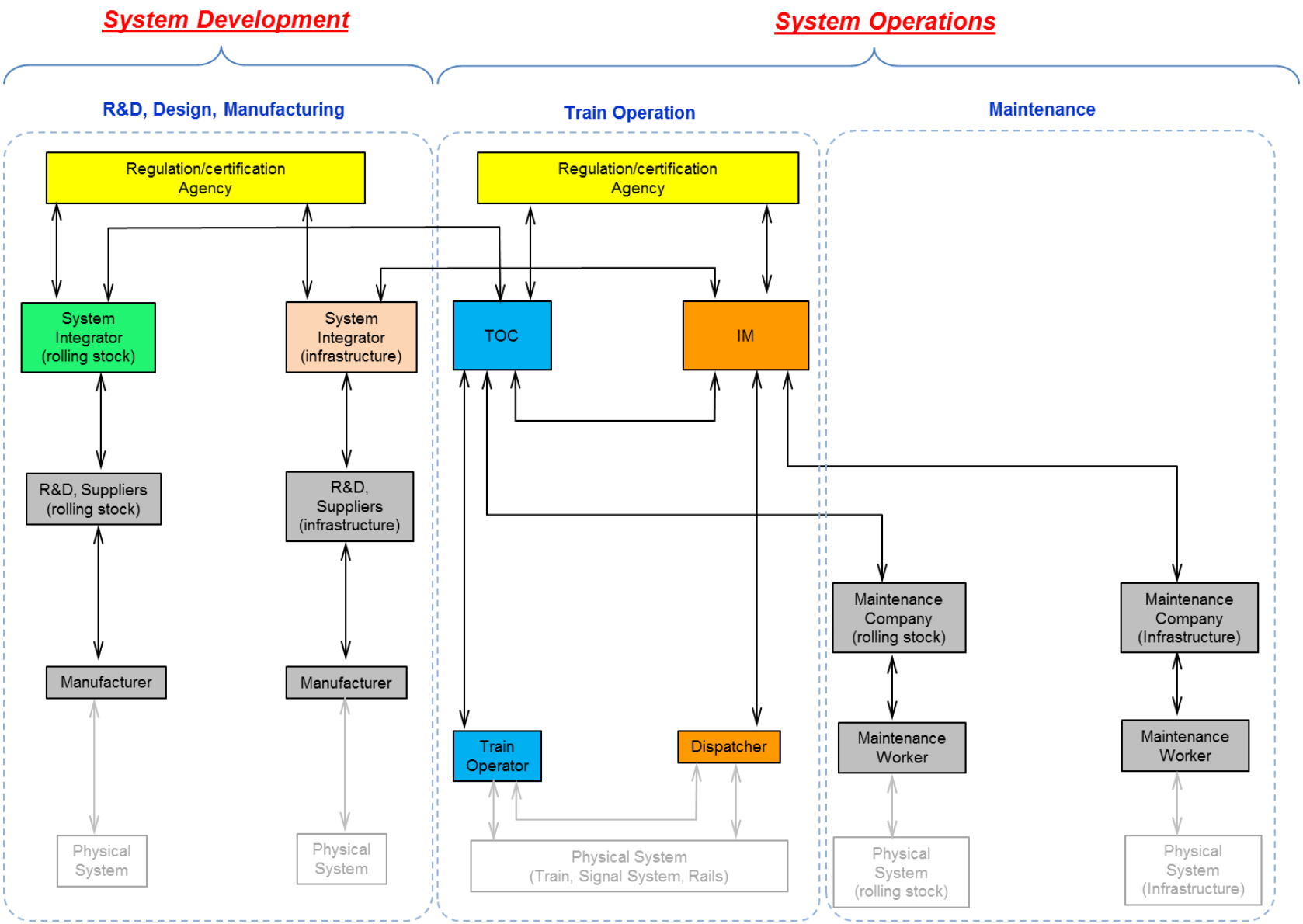

Table 4-5 Responsibilities, control actions, feedback and process models (Alternative 2)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
Regulation/certification Agency (R&D, Design, Mfg.)	*FRA*	-develop safety standards and safety-related regulation about railway systems. -certify the developed system through the design and manufacturing processes.	System Integrator (rolling stock)	*domestic or international supplier*	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
			System Integrator (infrastructure)	*domestic or international supplier*	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
System Integrator (rolling stock)	*domestic or international supplier*	-integrate railway system components related to rolling stock for practical use from a technical, operational, and business perspective, based on the specification given by TOC , complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers (rolling stock)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
System Integrators (Infrastructure)	*domestic or international supplier*	-integrate railway system components related to infrastructure for practical use from a technical, operational, and business perspective, based on the specification given by TOC , complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
R&D Company, Suppliers (rolling stock)	*domestic or international suppliers*	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer (rolling stock)	*domestic or international manufacturers*	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer (infrastructure)	*domestic or international manufacturers*	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
Manufacturers	*domestic or international manufacturers*	-manufacture the components of the system	*Physical System*				
Regulation/certification Agency (Train operation, maintenance)	*FRA*	-develop safety standards and safety-related regulation about operation and maintenance. -license TOC and IM. -monitor the capability of these companies, checking financial and managerial condition.	TOC	*Amtrak*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
			IM	*new public agency*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry

(continued)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
TOC	*Amtrak*	-manage train operation, designing operation schedule, frequency, fleet management plan, and operation manuals. -perform safety training and education to operators. - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. -design a specification for developing/updating rolling stock, and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to train operator management	Train Operator	*Amtrak*	operational directive, operation manual, training	anomaly report	knowledge about the developed system and operation, capability of operators, hazard analysis
			Maintenance Company (rolling stock)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (rolling stock)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
IM	*new public agency*	-own infrastructure and manage infrastructure operation such as operation regarding signal systems, station operation, etc. -perform safety training and education to dispatchers. -manage infrastructure operation, based on safety regulation and rules - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. - -design a specification for developing/updating infrastructure such as s signal system and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to dispatcher management	TOC	*Amtrak*	safety requirement	report	safety regulation about train operation, corporate safety operation rules, condition of operated trains and infrastructure
			Dispatcher	*Amtrak*	operational directive, operation manual, training	anomaly report	capability of Dispatcher, knowledge about the developed system and operation, capability of Dispatcher, hazard analysis
			Maintenance Company (infrastructure)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
Train Operator	*Amtrak*	-operate trains - report safety issues in operation, and manage them on the train	*Physical System*				
Dispatcher	*new public agency*	-communicate with train operators and control train signals - report safety issues in operation, and manage them in the control center	*Physical System*				
Maintenance Company (rolling stock)	*contractors*	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to Train Operator.	Maintenance Worker (rolling stock)	*contractors*	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the rolling stock, capability of Maintenance Worker
Maintenance Company (infrastructure)	*contractors*	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to IM	Maintenance Worker (infrastructure)	*contractors*	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the infrastructure capability of Maintenance Worker
Maintenance Workers	*contractors*	-conduct maintenance of rolling stock	*Physical System*				

4.4.3 Alternative 3: Open Access / New Line

Figure 4-10 represents the control structure of Alternative 3. According to this structure, the specific players in the industry for each component are organized in Table 4-6. One of the critical differences of this model from the other two alternatives is that *Infrastructure Owner* and IM are different institutions; *Infrastructure Owner* is a newly created public institution, and IM is Amtrak, which is one of the TOCs in the model, as well. A single or multiple private TOCs are also involved and are in charge of maintenance, system development, and train operation, under FRA's regulation and IM's supervision. Although there could be more than one private TOC in the structure in reality, for simplify, this model only shows with IM (Public) and IM (Private) that the industry has an open access system involving the private sectors. This research assumes that the operational line is entirely shared by all of the TOCs, instead of assuming that their operational areas are horizontally separated. Multiple *System Integrators* of rolling stock are involved due to open access system of the industry, and they are assumed to be different agencies. The system integrators of rolling stock and infrastructure for Amtrak could be a single firm. The system integrators, R&D agencies, and suppliers can be domestic or international firms. Also, *Maintenance Companies* are assumed as contractors with Amtrak or the private TOCs.

These models of the three alternatives are compared with the generic HSR model to clarify their structural differences in detail in the next section.

Figure 4-10 Safety Control Structure of Alternative 3 “Open access / New line”

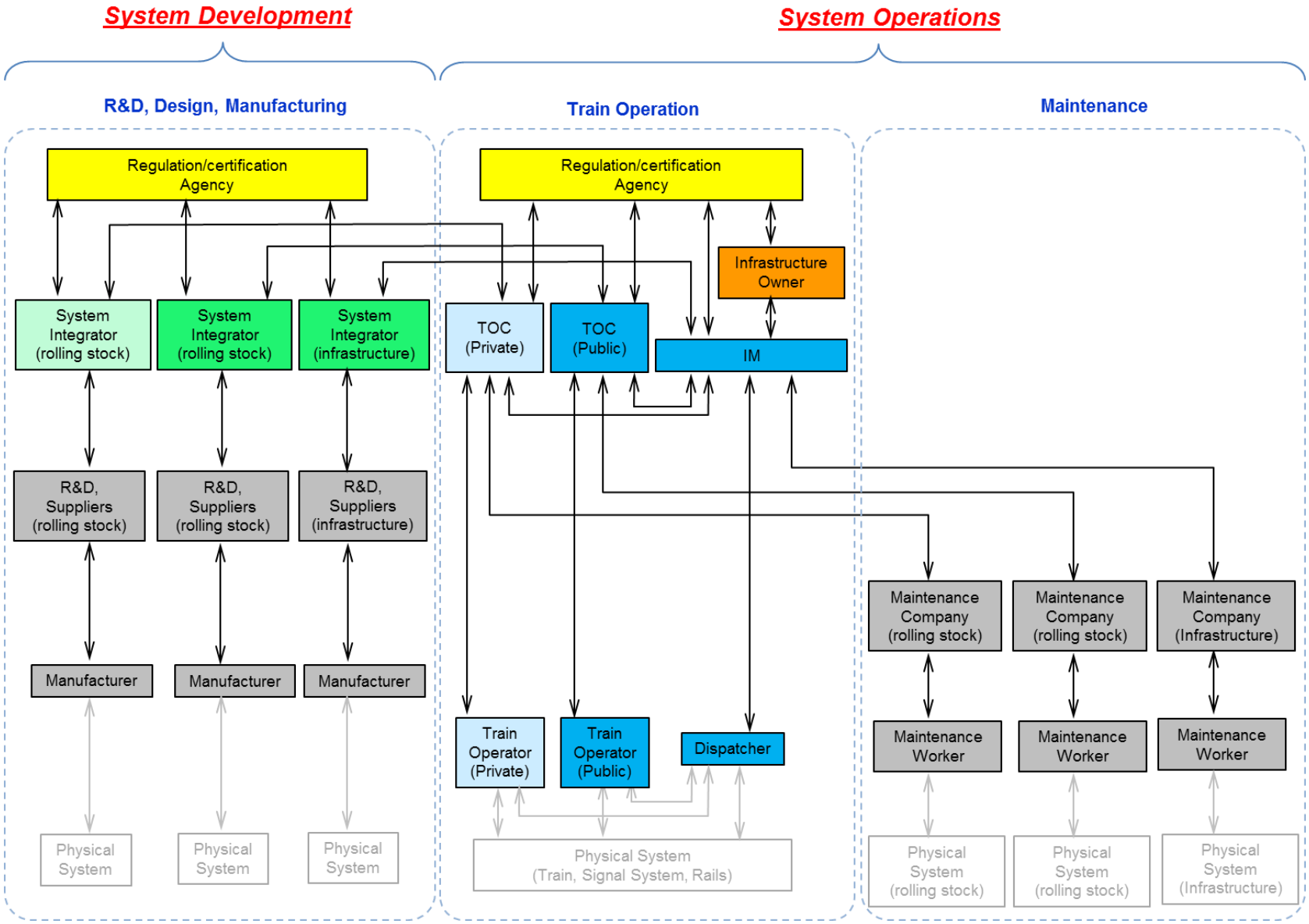

Table 4-6 Responsibilities, control actions, feedback and process models (Alternative 3)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
Regulation/certification Agency (R&D, Design, Mfg.)	*FRA*	-develop safety standards and safety-related regulation about railway systems. -certify the developed system through the design and manufacturing processes.	System Integrator (rolling stock)	*domestic or international supplier*	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
			System Integrator (rolling stock)	*domestic or international supplier*	regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
			System Integrator (infrastructure)		regulation, certification	test report for certification	technical knowledge and potential safety risks about the system in commercial operation, financial impact of regulatory change on the entire industry
System Integrator (rolling stock, for private TOCs)	*domestic or international supplier(for Private TOCs)*	-integrate railway system components related to rolling stock for practical use from a technical, operational, and business perspective, based on the specification given by TOC , complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers (rolling stock)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
System Integrator (rolling stock, for Amtrak)	*domestic or international supplier(for Amtrak)*		R&D Company, Suppliers (rolling stock)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
System Integrators (Infrastructure)		-integrate railway system components related to infrastructure for practical use from a technical, operational, and business perspective, based on the specification given by TOC , complying with the regulation and standards. -perform comprehensive safety hazard analysis and reflect it to specifications to R&D Company and Suppliers	R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	development report, safety-related feedback, verification for acceptance	information about practical operation and maintenance, capability of R&D companies and suppliers, hazard analysis
R&D Company, Suppliers (rolling stock)	*domestic or international suppliers*	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer (rolling stock)	*domestic or international manufacturers*	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
R&D Company, Suppliers (infrastructure)	*domestic or international suppliers*	-develop and supply system components to System Integrator. -make a contract with Manufacturer to manufacture those components.	Manufacturer (infrastructure)	*domestic or international manufacturers*	safety requirement, receiving inspection	verification for acceptance	specification from System Integrator, capability of manufacturer
Manufacturers	*domestic or international manufacturers*	-manufacture the components of the system	*Physical System*				

(continued)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
Regulation/certification Agency (Train operation, maintenance)	*FRA*	-develop safety standards and safety-related regulation about operation and maintenance. -license TOC and IM. -monitor the capability of these companies as well as infrastructure owner, checking financial and managerial condition.	TOC (Private)	*private operator(s)*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
			TOC (Public)	*Amtrak*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
			Infrastructure Owner	*new public agency*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
			IM	*Amtrak*	regulation, license, monitor	operation report, financial report	potential safety risks about train operation and maintenance in commercial operation from both technical and managerial perspectives, financial impact of regulatory change on the entire industry
TOC (Private)	*private operator(s)*	-manage train operation, designing operation schedule, frequency, fleet management plan, and operation manuals. -perform safety training and education to operators. - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. -design a specification for developing/updating rolling stock, and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to train operator management	Train Operator (Private)	*private operator(s)*	operational directive, operation manual, training	anomaly report	knowledge about the developed system and operation, capability of operators, hazard analysis
			Maintenance Company (rolling stock)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (rolling stock)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
TOC (Public)	*Amtrak*	-manage train operation, designing operation schedule, frequency, fleet management plan, and operation manuals. -perform safety training and education to operators. - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. -design a specification for developing/updating rolling stock, and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to train operator management	Train Operator (Public)	*Amtrak*	operational directive, operation manual, training	anomaly report	knowledge about the developed system and operation, capability of operators, hazard analysis
			Maintenance Company (rolling stock)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (rolling stock)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis

(continued)

Controllers	*Presumed Players*	Responsibility	Controlled Process	*Presumed Players*	Control Action	Feedback	Process Model
Infrastructure Owner	*new public agency*	-own and lease infrastructure to infrastructure operators. -monitor financial and safety-related managerial condition of operators	IM	*Amtrak*	safety requirement, monitor financial/managerial condition	report	capability of infrastructure operator, safety regulation about infrastructure ownership and operation
IM	*Amtrak*	-manage infrastructure operation such as operation regarding signal systems, station operation, etc. -perform safety training and education to dispatchers. -manage infrastructure operation, based on safety regulation and rules - develop a maintenance plan and conduct it, making a contract with Maintenance Company. -maintain maintenance record and make a future maintenance plan. -have close communication with Maintenance Company, monitor financial/managerial condition, and receive safety-related feedback which can be reflected to system improvement. -design a specification for developing/updating infrastructure such as s signal system and make a contract with System Integrator. -perform comprehensive safety hazard analysis and reflect it to specifications for Maintenance Company and System Integrator and to dispatcher management	TOC (Private)	*private operator(s)*	safety requirement	report	safety regulation about train operation, corporate safety operation rules, condition of operated trains and infrastructure
			TOC (Public)	*Amtrak*	safety requirement	report	safety regulation about train operation, corporate safety operation rules, condition of operated trains and infrastructure
			Dispatcher	*new public agency*	operational directive, operation manual, training	anomaly report	capability of Dispatcher, knowledge about the developed system and operation, capability of Dispatcher, hazard analysis
			Maintenance Company (infrastructure)	*contractors*	safety requirement, monitor financial/managerial condition	maintenance report, safety-related feedback about design	capability of maintenance company, hazard analysis
			System Integrator (infrastructure)	*domestic or international suppliers*	safety requirement, receiving inspection	verification for acceptance	capability of System Integrator, operation/maintenance issues to be improved, hazard analysis
Train Operator (Private)	*private operator(s)*	-operate trains - report safety issues in operation, and manage them on the train	*Physical System*				
Train Operator (Public)	*Amtrak*	-operate trains - report safety issues in operation, and manage them on the train	*Physical System*				
Dispatcher	*Amtrak*	-communicate with train operators and control train signals - report safety issues in operation, and manage them in the control center	*Physical System*				
Maintenance Company (rolling stock)	*contractors*	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to Train Operator.	Maintenance Worker (rolling stock)	*contractors*	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the rolling stock, capability of Maintenance Worker
Maintenance Company (infrastructure)	*contractors*	-manage maintenance. -perform safety training and education to maintenance workers. - organize maintenance results and provide safety feedback to IM	Maintenance Worker (infrastructure)	*contractors*	maintenance directive, maintenance manual, training	maintenance report, anomaly report	technical knowledge about the infrastructure capability of Maintenance Worker
Maintenance Workers	*contractors*	-conduct maintenance of rolling stock	*Physical System*				

4.5 Comparative Analysis

In reality, complexities of an institutional structure (e.g. market competition) could be intentionally introduced for non-safety purposes such as an economic benefit or a regulatory constraint. From the STAMP perspectives, they require additional safety constraints. The main purpose of this comparative analysis is to clarify the structural difference between the generic HSR model and each alternative model. This process can help analyze potential weaknesses and flaws of the control structures that could be driven by the additional complexities in the institutional structures of the NEC HSR, qualitatively confirming whether the complex control structures of the alternative could adequately meet the system requirements and safety constraints. Thus, this comparative analysis, as preliminary risk analysis, can facilitate STPA in Chapter 5 by highlighting inherent weaknesses of each alternative.

The results of the analysis are organized in Table 4-7, 4-8, and 4-9, according to each system requirement and safety constraints organized in Section 3.3. The results are discussed in Section 4.5.1 - 4.5.3.

Table 4-7 Potential risks due to structural differences (Maintenance)

System Requirements / Safety Constraints		Potential risks in Alternative 1 (Multi-ownership / Upgrade)	Potential risks in Alternative 2 (Vertical Separation / New)	Potential risks in Alternative 3 (Open Access/New)
High-level	**Specific**			
I. Safety-related decision-making and its implementation must be based on appropriate information, complying with state-of-the-art safety standards and regulations.	iv. Correct, complete, and up-to-date information about the physical system and maintenance must be available and used in safety-related decision-making and its implementation in maintenance. (Lesson E-d)	Multiple ownerships of the infrastructure could cause inadquate sharing of maintenance data and issues which could influence the safety of the other owners' operation.		Having multiple TOCs could cause inadquate sharing of maintenance data and issues which could influence the safety of the other TOCs' operation.
II. Safety considerations must be critical in safety-related decision-making and its implementation.	i. Safety-related decision-making in maintenance must be independent from programmatic considerations, including cost, schedule, and performance.			Having market competition among multiple TOCs could make them more concerned with cost, schedule, and performance, which could lower the priority of safety.
	iii. Safety-related decision-making and its implementation in maintenance must continuously pursue future improvement of the safety based on safety-related data and experience acquired through maintenance. (Lesson E-b)	Multiple ownerships of the infrastructure could cause inadquate sharing of maintenance data and issues which could can be applied to the inprovement of the system safety.		Having multiple TOCs could cause inadquate sharing of maintenance data and issues which could be applied to the inprovement of the system safety.
III. Safety-related decision-making and its implementation must be done by qualified personnel.	iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in maintenance.	Multiple ownerships of the infrastructure could cause inconsistent implementation of safety-related decision-making in maintenance.		Having multiple TOCs could cause inconsistent implementation of safety-related decision-making in maintenance.
	vi. The skill levels and experience levels of an individual maintenance worker and financial/managerial capability of agencies involved in maintenance must be evaluated, certified, and constantly monitored. (Lesson E-a)	Multiple ownerships of the infrastructure could cause difficulty in managing the skill/experience of the individual infrastructure maintenance worker comprehensively.		Having multiple TOCs could cause difficulty in managing the skill/experience of the individual rolling stock maintenance worker comprehensively.
	iv. Adequate resources must be applied to the hazard analysis process.			
IV. Safety analyses must be available and used throughout the processes in the system lifecycle, and must be continuously evolved.	v. Hazard analysis results must be communicated in a timely manner to those who need them. A communication structure must be established that includes contractors and allows communication downward, upward, and sideways.	Multiple ownerships of the infrastructure could cause untimely communication of hazard analyisis results.		Having multiple TOCs could cause untimely communication of hazard analyisis results among TOCs.
	vi. Hazard analyses must be elaborated (refined and extended) and updated as the design evolves, maintenance processes change. (Lesson A-d)	Multiple ownerships of the infrastructure could cause inadquate management of hazard analysis update.		Having multiple TOCs could cause inadquate management of hazard analysis update.

Table 4-8 Potential risks due to structural differences (Train Operation)

System Requirements / Safety Constraints		Potential risks in Alternative 1 (Multi-ownership / Upgrade)	Potential risks in Alternative 2 (Vertical Separation / New)	Potential risks in Alternative 3 (Open Access/New)
High-level	**Specific**			
I. Safety-related decision-making and its implementation must be based on appropriate information, complying with state-of-the-art safety standards and regulations.	iv. Correct, complete, and up-to-date information about the physical system and train operation must be available and used in safety-related decision-making and its implementation in train operation. (Lesson E-d)			Having multiple TOCs could cause inadquate sharing of operation data and issues which could influence the safety of the other TOCs' opereation.
II. Safety considerations must be critical in safety-related decision-making and its implementation.	i. Safety-related decision-making in train operation must be independent from programmatic considerations, including cost, schedule, and performance. (Lesson B-a)			Having market competition among multiple TOCs could make them more concerned with cost, schedule, and performance, which could lower the priority of safety.
	iii. Safety-related decision-making and its implementation in train operation must continuously pursue future improvement of safety of the system based on safety-related data and experience acquired through train operation.(Lesson E-b)			Having multiple TOCs could cause inadquate sharing of operation data and issues which could be applied to the inprovement of the system safety, and disorganization of system safety improvement.
III. Safety-related decision-making and its implementation must be done by qualified personnel.	i. Safety-related decision-making in train operation must be credible (executed using credible personnel, technical requirements, and decision-making tools).	Partially vertically separated strcture could technical decision maker's acquisition of broad knowledge of the system, thereby lowering the credibility of the decision.	Vertically separated strcture could technical decision maker's acquisition of broad knowledge of the system, thereby lowering the credibility of the decision.	Partially vertically separated strcture could technical decision maker's acquisition of broad knowledge of the system, thereby lowering the credibility of the decision.
	ii. Safety-related decision-making in train operation must be clear and unambiguous with respect to authority, responsibility, and	Having multiple infrastructure operaters could cause ambiguous allocation of safety responsiblities.		
	iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in train operation.	Having multiple infrastructure operaters and partially vertically separated structure could cause inefficient communication or miscommunication in the decision making process.	Vertically separated structure could cause inefficient communication or miscommunication in the decision making process.	Having multiple TOCs and partially vertically separated structure could cause inefficient communication or miscommunication in the decision making process.
	vi. The skill levels and experience levels of an individual operator and financial/managerial capability of agencies involved in train operation must be evaluated, certified, and constantly-	Having multiple infrastructure operaters could cause difficulty in managing the skills of the individual operator comprehensively.		Having multiple TOCs could cause difficulty in managing the skills of the individual operator comprehensively.
IV. Safety analyses must be available and used throughout the processes in the system lifecycle, and must be continuously evolved.	v. Hazard analysis results must be communicated in a timely manner to those who need them. A communication structure must be established that includes contractors and allows communication downward, upward, and sideways.	Having multiple infrastructure operaters and partially vertically separated structure could cause inefficient communication or miscommunication.	Vertically separated structure could cause inefficient communication or miscommunication.	Having multiple TOCs and partially vertically separated structure could cause inefficient communication or miscommunication.

Table 4-9 Potential risks due to structural differences (R&D, Design, and Manufacturing)

System Requirements / Safety Constraints		Potential risks in Alternative 1 (Multi-ownership / Upgrade)	Potential risks in Alternative 2 (Vertical Separation / New)	Potential risks in Alternative 3 (Open Access/New)
High-level	**Specific**			
I. Safety-related decision-making and its implementation must be based on appropriate information, complying with state-of-the-art safety standards and regulations.	iv. Correct, complete, and up-to-date information about R&D/Design/Manufacturing, train operation, and maintenance must be available and used in safety-related decision-making and its implementation in R&D/Design/Manufacturing. (Lesson D-c)	Multiple ownerships of the infrastructure and partially vertically separated structure could cause inadquate sharing of safety-related maintenance/operation data and issues which should be organized for consisntent R&D/Design/Manufacturing.	Vertically separated structure could cause inadquate sharing of safety-related maintenance/operation data and issues which should be consistently applied to R&D/Design/Manufacturing.	Having multiple TOCs and partially vertically separated structure could cause inadquate sharing of safety-related maintenance/operation data and issues which should be consistently applied to R&D/Design/Manufacturing.
II. Safety considerations must be critical in safety-related decision-making and its implementation.	i. Safety-related decision-making in R&D/Design/Manufacturing must be independent from programmatic considerations, including cost, schedule, and performance. (Lesson D-a)			Having market competition among multiple TOCs could make them more concerned with cost, schedule, and performance, which could lower the priority of safety.
III. Safety-related decision-making and its implementation must be done by qualified personnel.	iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in R&D/Design/Manufacturing.	Having multiple infrastructure operaters could cause inefficient communication or miscommunication for achieving consistent safety-related decision making.		Having multiple TOCs could cause inefficient communication or miscommunication for achieving consistent safety-related decision making.
	vi. The skill levels and experience levels of an individual engineer and financial/managerial capability of agencies involved in R&D/Design/Manufacturing must be evaluated, certified, and constantly-monitored. (Lesson E-a)	Having multiple infrastructure operaters and their system integrators could cause difficulty in managing the skill/experience level of the individual engineer comprehensively.		Having multiple TOCs and their system integrators could cause difficulty in managing the skill/experience level of the individual engineer comprehensively.
IV. Safety analyses must be available and used throughout the processes in the system lifecycle, and must be continuously evolved.	i. High-quality system hazard analyses of R&D/Design/Manufacturing must be created with caution to system interfaces such as a boundary between self-developed domain and introduced domain from other agencies, and with caution to usability of the system for system users in any possible situations, involving their perspectives in each step of system design/integration processes. (Lesson D-b, E-c)	Having multiple infrastructure operaters and their system integrators could cause incompatibility or complex technical interface in the boundaries of the multi-owned infrastractures.		

4.5.1 Alternative 1 (Multiple Ownership / Upgraded Line)

The fragmented ownership of the infrastructure of Alternative 1 could have structural risks about some of the system requirements and safety constraints. Multiple ownerships would have different types of infrastructure operation and maintenance according to the operational areas, and they could lead to sharing data and issues inefficiently among these agencies. For example, a safety-critical operational issue newly found in one area might not be shared with other IMs if they do not have an appropriate mechanism of knowledge/information sharing. Also, fragmented ownership of the infrastructure could provide difficulty for the regulator in closely monitoring their skills, and financial and managerial capabilities in a consistent way.

No critical structural flaw[27] that cannot meet the requirements or safety constraints at all is identified in this alternative, although there are some differences that could provide safety concerns. Specific causes of hazards and their scenarios leading to breakage of the system requirements and safety constraints are analyzed with STPA in Chapter 5.

4.5.2 Alternative 2 (Vertically Separated / New Line)

The largest difference between this alternative and the generic HSR model is that Alternative 2 has a vertically separated structure. Except for this point, it can be said that the structure of Alternative 2 is the same as that of the generic HSR model, so there are only a few items that describe the structural differences. Specifically, the vertically separated structure could have an inefficient or inadequate communication in implementing consistent safety-related decision making in train operation and have a drawback in integrating data and issues for the R&D, Design, and Manufacturing process for developing a safer system, due to the organizational boundary between TOC and IM. Also, vertically separated responsibilities of the technical operators in the industry could have difficulty acquiring broad knowledge about the system for implementing safety measures, thereby lowering the credibility of their decision making[9]. These points are also mentioned in the same items of the tables in Alternative 1 and 3, which also have a vertically separated operational structure to a certain degree.

Also, it is reasonable to conclude that this alternative does not have a critical structural flaw that does not meet the requirements and constraints at all.

[27] For example, if a control structure does not have control action and feedback for system evolution, its structure can be regarded as flawed.

4.5.3 Alternative 3 (Open Access / New Line)

The fragmented TOCs in Alternative 3 create additional system components and interactions, compared to the generic HSR model, and this difference could give birth to risks of not sharing safety-related data and issues that could affect the safety of other TOCs' operation, which is similarly discussed in Alternative 1. Additionally, the involvement of the market competition among the TOCs could distort safety-oriented decision making due to schedule, cost, and performance pressure induced by the competition.

Also, it is reasonable to conclude that this alternative does not have a critical structural flaw that does not meet the requirements and constraints at all.

In the next chapter, based on the identified structural weaknesses, causes of hazards and their causal factors are analyzed in detail with STPA and SD.

CHAPTER 5. RISK ANALYSIS OF THE NEC HSR

In this chapter, causes of hazards and their causal factors are identified by performing STPA analysis about the three alternatives. While the comparative analysis in Section 4.5 focuses on the structure of the control models, STPA focuses on control loops at each level of the hierarchy. In Section 5.1, unsafe control actions are comprehensively identified based on the four different types of unsafe control actions introduced in Section 2.1.4. In Section 5.2, the specific causal factors leading to the unsafe control are analyzed in detail. In Section 5.3, some of the key risks identified in Section 5.2 are further analyzed with System Dynamics.

5.1 Unsafe Control Actions Identification (STPA-1)

As introduced in Section 2.1.4, if there is an accident, one or more events below must have occurred, according to the STAMP theory.

Unsafe Control Actions:

1) A control action required for safety is not provided or not followed.
2) An unsafe control action is provided that leads to a hazard.
3) A potentially safe control action is provided too late, too early, or out of sequence.
4) A safe control action is stopped too soon or applied to long (for a continuous or non-discrete control action)

Failure of Controlled Process:

5) Appropriate control actions are provided, but the controlled process does not follow them.

By analyzing control loops one by one in the control models of the institutional alternatives with this framework, potential causes of hazards can be comprehensively identified. With the guidewords 1) – 4), unsafe control actions for the three alternatives are specified in Table 5.1 -5.3. In the tables, relation among “Controller,” “Controlled Process,” their “Presumed Players,” “Control Action,” “Unsafe Control Actions” are organized.

In the next section, causal factors that could lead to these identified unsafe control actions and the fifth cause of hazards, *Failure of Controlled Process*, are discussed based on STPA-2 in Section 2.1.5.

Table 5-1 Unsafe controls actions (Alternative 1: Multiple ownerships / Upgraded line)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
Regulation/certification Agency (R&D, Design, Mfg.)	FRA	System Integrator (rolling stock)	domestic or international supplier	regulation, certification	- revision of safety regulation for newly emerged safety issues is not performed. - certification that is necessary for safety-related systems is not provided but they are used in revenue operation.	- regulation or certification that does not cover all of the safety-critical conditions in the new HSR system is provided. - regulation with which regulated organization have difficulty in complying is provided. - certification is provided based on inadequate safety validation and verification of COTS products.	- safety regulation is not developed immediately after safety risks are realized, and the timing to provide it to the industry is delayed. - certification is implemented at a timing when safety-critical parts of the new HSR system cannot be adequately verified.	-
		System Integrator (infrastructure)		regulation, certification				-
		System Integrator (infrastructure)	domestic or international supplier	regulation, certification				-
System Integrator (rolling stock)	domestic or international supplier	R&D Company, Suppliers (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement designed based on inappropriate operational conditions is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but its results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
System Integrators (Infrastructure)		R&D Company, Suppliers (infrastructure)						
	domestic or international supplier	R&D Company, Suppliers (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection				
R&D Company, Suppliers (rolling stock)	domestic or international suppliers	Manufacturer (rolling stock)	domestic or international manufacturers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement designed based on inappropriate operational conditions is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
R&D Company, Suppliers (infrastructure)	domestic or international suppliers	Manufacturer (infrastructure)	domestic or international manufacturers	safety requirement, receiving inspection				

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
Regulation/certification Agency (Train operation, maintenance)	FRA	TOC	Amtrak	regulation, license, monitor	- revision of safety regulation for newly emerged safety issues is not performed. - license is not provided but TOC (IM) conducts revenue operation. - monitoring lacks a method to understand TOC (IM) 's condition in safety activities.	- regulation or certification that does not cover all of the safety-critical conditions in the new HSR system is provided. - regulation with which regulated organization has difficulty in complying is provided. - license is provided for TOC (IM) that is not capable of safety-oriented operation - monitoring method is not appropriate to understand TOC (IM) 's condition in safety activities.	- safety regulation is not developed immediately after safety risks are realized, and the timing to provide it to the industry is delayed. - license is provided too early, before capability of TOC (IM) is adequately confirmed - monitoring is not performed when TOC (IM) 's condition in safety activities is appropriately observable.	- license is not invalidated after TOC (IM) loses safe operation capability, or operational qualification - monitoring is terminated before TOC (IM) 's condition in safety activities gets worse.
		IM		regulation, license, monitor				
			regional authorities	regulation, license, monitor				
TOC	Amtrak	Train Operator	Amtrak	operational directive, operation manual, training	- operation manual or training that cover safety-critical conditions required by system changes is not provided. - safety-related operational directive is not provided when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual or training is not provided immediately after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied even after new operational manuals are provided. - safety-related operational directive is not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (rolling stock)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - monitoring lacks a method to understand financial and managerial condition that could affects safety in maintenance.	- safety requirement with which contractor has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition can be appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated. - safety requirement that is not coordinated and lacks operational condition at operational boundaries with other IMs is provided	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
IM	Amtrak	TOC	Amtrak	safety requirement	- safety requirement that covers necessary safety-related items for system operations is not provided.	- safety requirement with which TOC(s) has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided.	-	-
		Dispatcher		operational directive, operation manual, training	- operation manual or training that covers safety-critical conditions required by system changes is not provided . - safety-related operational directive is not provided when train operation has to be restricted.	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train operation has to be restricted.	- operation manual or training is not provided immediately after the system changes - safety-related operational directives are delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied after a new operational manual is provided. - safety-related operational directive is not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (infrastructure)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - financial/managerial condition that affects safety in maintenance is not monitored	- safety requirement with which contractor has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system are provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition is appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
IM	regional authorities	TOC	Amtrak	safety requirement	- safety requirement that covers necessary safety-related items for system operations is not provided.	- safety requirement with which contractors have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided.	-	-
		Dispatcher	regional authorities	operational directive, operation manual, training	- operation manual or training that cover safety-critical conditions required by system changes is not provided . - safety-related operational directive is not provided when train operation has to be restricted by the directive.	- operation manual that does not cover all of the safety-critical conditions in operation are provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train operation has to be restricted.	- operation manual or training is not provided for a while after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals are applied after new operational manuals are provided. - safety-related operational directive is not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (infrastructure)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - financial/managerial condition that affects safety in maintenance are not monitored	- safety requirement with which contractor has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition is appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated. - safety requirement that is not coordinated and lacks operational condition at operational boundaries with other IMs is provided	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
Maintenance Company (rolling stock)	contractors	Maintenance Worker (rolling stock)	contractors	maintenance directive, maintenance manual, training	- maintenance manual or training that covers safety-critical conditions required by system changes is not provided . - safety-related maintenance directive is not provided and train operation continues with the unsafe infrastructure and rolling stock.	- maintenance manual that does not cover all of the safety-critical conditions in operation are provided - training is not developed to cover all of the safety-critical conditions in maintenance at an appropriate safety level. - safety-related maintenance directive is wrong and train operation continues.	- maintenance manual or training is not provided for a while after the system changes - safety-related maintenance directive is delayed and not applied at a necessary timing.	-
Maintenance Company (infrastructure)	contractors	Maintenance Worker (infrastructure)	contractors	maintenance directive, maintenance manual, training				-

Table 5-2 Unsafe control actions (Alternative 2: Vertically separated / New line)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
Regulation/certification Agency (R&D, Design, Mfg.)	FRA	System Integrator (rolling stock)	domestic or international supplier	regulation, certification	- revision of safety regulation for newly emerged safety issues is not performed. - certification that is necessary for safety-related systems is not provided but they are used in revenue operation.	- regulation or certification that does not cover all of the safety-critical conditions in the new HSR system is provided. - regulation with which regulated organization have difficulty in complying is provided. - certification is provided based on inadequate safety validation and verification of COTS products.	- safety regulation is not developed immediately after safety risks are realized, and the timing to provide it to the industry is delayed. - certification is implemented at a timing when safety-critical parts of the new HSR system cannot be adequately verified.	-
		System Integrator (infrastructure)	domestic or international supplier	regulation, certification				-
System Integrator (rolling stock)	domestic or international supplier	R&D Company, Suppliers (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement designed based on inappropriate operational conditions is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but its results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
System Integrators (Infrastructure)	domestic or international supplier	R&D Company, Suppliers (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection			-	
R&D Company, Suppliers (rolling stock)	domestic or international suppliers	Manufacturer (rolling stock)	domestic or international manufacturers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement designed based on inappropriate operational conditions is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
R&D Company, Suppliers (infrastructure)	domestic or international suppliers	Manufacturer (infrastructure)	domestic or international manufacturers	safety requirement, receiving inspection			-	

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
Regulation/certification Agency (Train operation, maintenance)	FRA	TOC	Amtrak	regulation, license, monitor	- revision of safety regulation for newly emerged safety issues is not performed. - license is not provided but TOC (IM) conducts revenue operation. - monitoring lacks a method to understand TOC (IM) 's condition in safety activities.	- regulation or certification that does not cover all of the safety-critical conditions in the new HSR system is provided. - regulation with which regulated organization has difficulty in complying is provided. - license is provided for TOC (IM) that is not capable of safety-oriented operation - monitoring method is not appropriate to understand TOC (IM) 's condition in safety activities.	- safety regulation is not developed immediately after safety risks are realized, and the timing to provide it to the industry is delayed. - license is provided too early, before capability of TOC (IM) is adequately confirmed - monitoring is not performed when TOC (IM) 's condition in safety activities is appropriately observable.	- license is not invalidated after TOC (IM) loses safe operation capability, or operational qualification - monitoring is terminated before TOC (IM) 's condition in safety activities gets worse.
		IM	new public agency	regulation, license, monitor				
TOC	Amtrak	Train Operator	Amtrak	operational directive, operation manual, training	- operation manual or training that covers safety-critical conditions required by system changes is not provided. - safety-related operational directive is not provided when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual or training is not provided immediately after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied even after new operational manuals are provided. - safety-related operational directive is not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (rolling stock)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - monitoring lacks a method to understand financial and managerial condition that could affects safety in maintenance.	- safety requirement with which contractor has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition can be appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
IM	new public agency	TOC	Amtrak	safety requirement	- safety requirement that covers necessary safety-related items for system operations is not provided.	- safety requirement with which TOC(s) has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided.	-	-
		Dispatcher	Amtrak	operational directive, operation manual, training	- operation manual or training that covers safety-critical conditions required by system changes is not provided . - safety-related operational directive is not provided when train operation has to be restricted.	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train operation has to be restricted by them.	- operation manual or training is not provided for a while after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied after new operational manual is provided. - safety-related operational directives are not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (infrastructure)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - financial/managerial condition that affects safety in maintenance is not monitored	- safety requirement with which contractor has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition is appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
Maintenance Company (rolling stock)	contractors	Maintenance Worker (rolling stock)	contractors	maintenance directive, maintenance manual, training	- maintenance manual or training that covers safety-critical conditions required by system changes is not provided . - safety-related maintenance directive is not provided and train operation continues with the unsafe infrastructure and rolling stock.	- maintenance manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in maintenance at an appropriate safety level. - safety-related maintenance directive is wrong and train operation continues.	- maintenance manual or training is not provided for a while after the system changes - safety-related maintenance directive is delayed and not applied at a necessary timing.	-
Maintenance Company (infrastructure)	contractors	Maintenance Worker (infrastructure)	contractors	maintenance directive, maintenance manual, training				

Table 5-3 Unsafe control actions (Alternative 3: Open access / New line)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
Regulation/certification Agency (R&D, Design, Mfg.)	FRA	System Integrator (rolling stock)	domestic or international supplier	regulation, certification	- revision of safety regulation for newly emerged safety issues is not performed. - certification that is necessary for safety-related systems is not provided but they are used in revenue operation.	- regulation or certification that does not cover all of the safety-critical conditions in the new HSR system is provided. - regulation with which regulated organization has difficulty in complying is provided. - certification is provided based on inadequate safety validation and verification of COTS products.	- safety regulation is not developed immediately after safety risks are realized, and the timing to provide it to the industry is delayed. - certification is implemented at a timing when safety-critical parts of the new HSR system cannot be adequately verified.	-
		System Integrator (rolling stock)	domestic or international supplier	regulation, certification				-
		System Integrator (infrastructure)		regulation, certification				-
System Integrator (rolling stock, for private TOCs)	domestic or international supplier(for Private TOCs)	R&D Company, Suppliers (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement designed based on inappropriate operational conditions is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but its results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
System Integrator (rolling stock, for Amtrak)	domestic or international supplier(for Amtrak)	R&D Company, Suppliers (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection				
System Integrators (Infrastructure)		R&D Company, Suppliers (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection				
R&D Company, Suppliers (rolling stock)	domestic or international suppliers	Manufacturer (rolling stock)	domestic or international manufacturers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement designed based on inappropriate operational conditions is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
R&D Company, Suppliers (infrastructure)	domestic or international suppliers	Manufacturer (infrastructure)	domestic or international manufacturers	safety requirement, receiving inspection				
Regulation/certification Agency (Train operation, maintenance)	FRA	TOC (Private)	private operator(s)	regulation, license, monitor	- revision of safety regulation for newly emerged safety issues is not performed. - license is not provided but TOC (Infrastructure Owner or IM) conducts revenue operation. - monitoring lacks a method to understand TOC (Infrastructure Owner or IM) 's condition in safety activities.	- regulation or certification that does not cover all of the safety-critical conditions in the new HSR system is provided. - regulation with which regulated organization has difficulty in complying is provided. - license is provided for TOC (Infrastructure Owner or IM) that is not capable of safety-oriented operation - monitoring method is not appropriate to understand TOC (Infrastructure Owner or IM) 's condition in safety activities.	- safety regulation is not developed immediately after safety risks are realized, and the timing to provide it to the industry is delayed. - license is provided too early, before capability of TOC (Infrastructure Owner or IM) is adequately confirmed - monitoring is not performed when TOC (Infrastructure Owner or IM) 's condition in safety activities is appropriately observable.	- license is not invalidated after TOC (Infrastructure Owner or IM) loses safe operation capability, or operational qualification - monitoring is terminated before TOC (Infrastructure Owner or IM) 's condition in safety activities gets worse.
		TOC (Public)	Amtrak	regulation, license, monitor				
		Infrastructure Owner	new public agency	regulation, license, monitor				
		IM	Amtrak	regulation, license, monitor				

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
TOC (Private)	private operator(s)	Train Operator (Private)	private operator(s)	operational directive, operation manual, training	- operation manual or training that covers safety-critical conditions required by system changes is not provided. - safety-related operational directive is not provided when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train is not automatically controlled and has to be restricted by the directive. (e.g., emergency operation).	- operation manual or training is not provided immediately after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied even after new operational manuals are provided. - safety-related operational directive is not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (rolling stock)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - monitoring lacks a method to understand financial and managerial condition that could affects safety in maintenance.	- safety requirement with which contractor has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition can be appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system are provided. - receiving inspection is conducted but their results are inadequately evaluated. - safety requirements that are not coordinated among TOCs are provided.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
TOC (Public)	Amtrak	Train Operator (Public)	Amtrak	operational directive, operation manual, training	- operation manual or training that covers safety-critical conditions required by system changes is not provided. - safety-related operational directive is not provided when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train is not automatically controlled and has to be restricted by the directive.(e.g., emergency operation).	- operation manual or training is not provided immediately after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied even after new operational manuals are provided. - safety-related operational directive is not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (rolling stock)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - monitoring lacks a method to understand financial and managerial condition that could affects safety in maintenance.	- safety requirement with which contractors have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition can be appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (rolling stock)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system are provided. - receiving inspection is conducted but their results are inadequately evaluated. - safety requirement that is not coordinated among TOCs are provided.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
Infrastructure Owner	new public agency	IM	Amtrak	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for train operations is not provided. - monitoring lacks a method to understand financial and managerial condition of IM that could affects safety in maintenance.	- safety requirement with which IM has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand IM's condition in safety activities.	- monitoring is not performed when IM's financial/managerial condition is appropriately observable.	- monitoring is terminated before IM's financial/managerial condition gets worse.

(continued)

Controllers	Presumed Players	Controlled Process	Presumed Players	Control Action	Unsafe Control Actions			
					Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped Too Soon / Applied too long
IM	Amtrak	TOC (Private)	private operator(s)	safety requirement	- safety requirement that covers necessary safety-related items for system operations is not provided.	- safety requirement with which TOC(s) has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided.	-	-
		TOC (Public)	Amtrak	safety requirement	- safety requirement that covers necessary safety-related items for system operations is not provided.	- safety requirement with which TOC(s) has difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided.	-	-
		Dispatcher	new public agency	operational directive, operation manual, training	- operation manual or training that covers safety-critical conditions required by system changes is not provided . - safety-related operational directive is not provided when train operation has to be restricted.	- operation manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in operation at an appropriate safety level. - safety-related operational directive is wrong when train operation has to be restricted by them.	- operation manual or training is not provided immediately after the system changes - safety-related operational directive is delayed and not applied at a necessary timing.	- training is terminated before trainee acquires adequate skills. - old operational manuals keep applied even after new operational manuals are provided. - safety-related operational directives are not terminated when the operational condition changes and can be unsafe due to the directive.
		Maintenance Company (infrastructure)	contractors	safety requirement, monitor financial/managerial condition	- safety requirement that covers safety-related items necessary for maintenance is not provided. - financial/managerial condition that affects safety in maintenance are not monitored	- safety requirement with which contractors have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system is provided. - monitoring method is not appropriate to understand contractors' condition in safety activities.	- monitoring is not performed when contractors' financial/managerial condition is appropriately observable.	- monitoring is terminated before contractors' financial/managerial condition gets worse.
		System Integrator (infrastructure)	domestic or international suppliers	safety requirement, receiving inspection	- safety requirement that covers safety-related items necessary for system operations is not provided. - receiving inspection necessary for safety-related systems is not conducted but the systems are used in revenue operation.	- safety requirement with which suppliers have difficulty in complying is provided. - safety requirement that does not cover all of the safety-critical conditions in the new HSR system are provided. - receiving inspection is conducted but their results are inadequately evaluated.	-	- when receiving inspection is incomplete, the developed system is applied to the revenue operation.
Maintenance Company (rolling stock)	contractors	Maintenance Worker (rolling stock)	contractors	maintenance directive, maintenance manual, training	- maintenance manual or training that covers safety-critical conditions required by system changes is not provided . - safety-related maintenance directive is not provided and train operation continues with the unsafe infrastructure and rolling stock.	- maintenance manual that does not cover all of the safety-critical conditions in operation is provided - training is not developed to cover all of the safety-critical conditions in maintenance at an appropriate safety level. - safety-related maintenance directive is wrong and train operation continues.	- maintenance manual or training is not provided for a while after the system changes - safety-related maintenance directive is delayed and not applied at a necessary timing.	-
Maintenance Company (infrastructure)	contractors	Maintenance Worker (infrastructure)	contractors	maintenance directive, maintenance manual, training				-

5.2 Causal Analysis (STPA-2)

In this causal analysis, complex causal factors for the identified unsafe control actions as well as failures of controlled processes are analyzed. These causal factors can be regarded as "scenarios" in which these types of unsafe control happen. As described in Section 2.1.5, this research uses guide words introduced in Figure 5-1 (same as Figure 2-10) to develop possible scenarios, focusing on control actions/feedback interaction of each controller and controlled process, process model of the controller, and external input to both the controller and controlled process. The scenarios are analyzed and developed, taking into account the information given from the current HSR operational and managerial issues in the NEC and the ongoing HSR project design. Generic risks generated from this framework that can also be true for non-US HSRs are not discussed in detail, so identified risks in this analysis, importantly, are not collectively exhaustive.

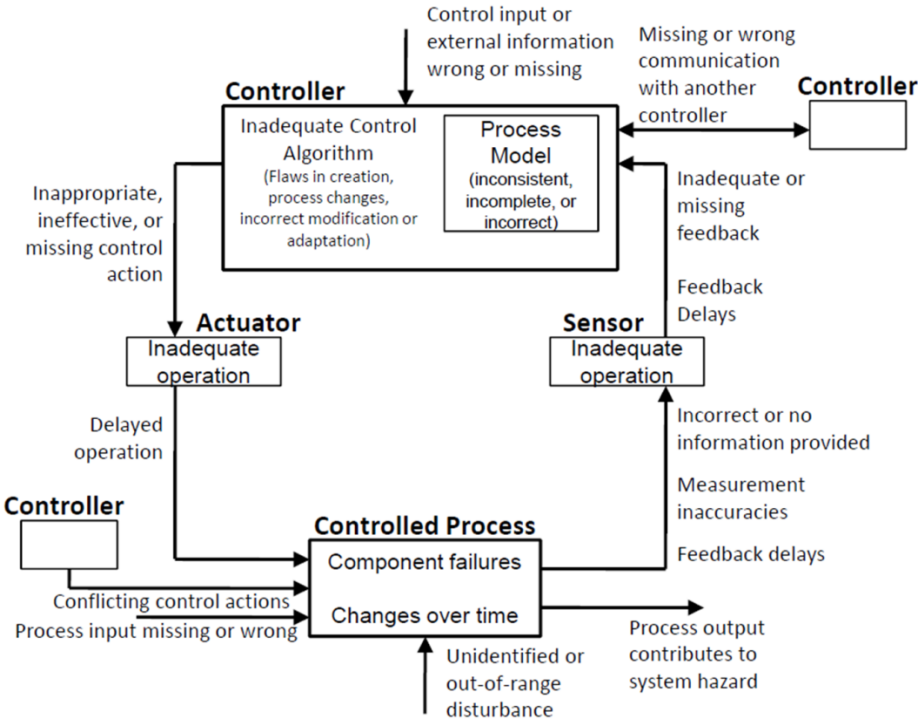

Figure 5-1 Guide words for causal scenario identification (same as Figure 2-10)

The identified risks are categorized into two types according to their "time-to-effect": *immediate risks* and *general risks*. *Immediate risks* represent unsafe events that can come out at relatively quickly after the launch of commercial operation, which can be mitigated over time. *General risks*, on the other hand, cannot be mitigated for a long-term period or could come out after a while. Some of the key general risks identified in this section are analyzed by SD in Section 5.3.

For each identified risk, "Controller" and "Controlled process" that create the risk, "Type of Causal Factor" discussed in Section 2.1.5, "Time-to-effect," and institutional alternatives that could have the risk are organized in Table 5-4. Although more than half of the risks are true for all of the three alternatives, the rests are applicable only to one or two of the alternatives. The detailed description of causal relations for each risk is described in Section 5.2.1. Based on these identified risks, weaknesses of the *System Safety Program* (*49 CFR Part 270 proposed rule in 2012*) are discussed in Section 5.2.2, as a case study of regulation analysis.

Table 5-4 Identified risks and types of their causal factors

Controller	Controlled Process	Risk	Type of Causal Factor	Time to effect	Alt. 1	Alt. 2	Alt. 3
Regulation/certification Agency	System Integrators (rolling stock, infrastructure)	1	Inadequate process model	General	x	x	x
		2	Inadequate control algorism	Immediate	x	x	x
		3	Inadequate control algorism	General	x	x	x
		4	Inadequate process model	Immediate	x	x	x
		5	Inadequate inputs to the controller	General	x	x	x
		6	Inadequate control algorism	General	x	x	x
		7	Inadequate control algorism	General	x	x	x
		8	Inadequate control algorithm/process model	General	x	x	x
System Integrators (rolling stock, infrastructure)	R&D Company/Suppliers (rolling stock or infrastructure)	9	Inadequate inputs to the controller	Immediate	x	x	x
		10	Inadequate inputs to the controller	Immediate	x	x	x
		11	Inadequate process model	Immediate	x	x	x
		12	Inadequate process model	General	x	x	x
		13	Inadequate inputs to the controller	Immediate	x	x	x
		14	Inadequate process model	General	x	x	x
		15	Inadequate control algorism	General	x	x	x
R&D Company/Suppliers (rolling stock or infrastructure)	Manufacturers (rolling stock or infrastructure)	16	Inadequate process model	General	x	x	x
		17	Inadequate inputs to the controller	General	x	x	x
		18	Failure of the control process	Immediate	x	x	x
Regulation/certification Agency	TOC and IM (or Infrastructure Owner and IM)	19	Inadequate control algorism	General	x	x	x
		20	Inadequate control algorism	General	x	x	x
		21	Inadequate control algorithm/process model	General	x	x	x
TOC	Train Operator	22	Inadequate process model	General	x	x	x
		23	Inadequate process model	General	x	x	x
		24	Conflicting control action	General	x		
	Maintenance Company (rolling stock)	25	Inadequate process model	Immediate	x	x	x
		26	Inadequate process model	Immediate	x	x	x
		27	Inadequate control algorism	General			x
	System Integrator (rolling stock)	28	Inadequate control algorithm/process model	Immediate	x	x	x
		29	Inadequate control algorithm/process model	Immediate	x	x	x
		30	Inadequate inputs to the controller	General	x	x	x
		31	Failure of the control process	Immediate	x	x	x
		32	Inadequate control algorithm/process model	General	x	x	x
		33	Inadequate control algorism	General			x
		34	Inadequate inputs to the controller	General			x
IM	TOC	35	Inadequate process model	Immediate	x	x	x
		36	Conflicting control action	Immediate	x		
		37	Inadequate process model	General	x	x	x
		38	Conflicting control action	General		x	x
		39	Inadequate control algorithm/process model	General			x
	Dispatcher	40	Inadequate process model	Immediate	x	x	x
		41	Inadequate control algorism	Immediate	x		
		42	Inadequate process model	General	x		x
	Maintenance Company (infrastructure)	43	Inadequate process model	Immediate	x	x	x
		44	Inadequate process model	General	x		
		45	Inadequate control algorism	General	x		
		46	Inadequate process model	General	x	x	x
		47	Inadequate control algorithm/process model	General		x	x
	System Integrators (infrastructure)	48	Inadequate control algorithm/process model	Immediate	x	x	x
		49	Inadequate control algorithm/process model	Immediate	x	x	x
		50	Inadequate inputs to the controller	General	x		
		51	Failure of the control process	Immediate	x	x	x
		52	Inadequate process model	General	x	x	x
		53	Inadequate control algorism	General	x	x	x
		54	Inadequate control algorithm/process model	General	x	x	x
Infrastructure Owner	IM	55	Conflicting control action	General			x
Maintenance Companies (rolling stock, infrastructure)	Maintenance Workers (rolling stock, infrastructure)	56	Inadequate process model	Immediate	x	x	x
		57	Inadequate process model	Immediate	x	x	x
		58	Inadequate control algorithm/process model	Immediate		x	x

5.2.1 Risks of the NEC HSR

The identified 58 risks are explained one by one, below.

- **Risk 1-8: *Regulation/certification Agency* [FRA] → *System Integrators (rolling stock or infrastructure)* [domestic or international suppliers][28]**

    - **Risk 1 (Inadequate process model, General, Alternative 1-3):** One of the causal factors that cause unsafe control actions is an inappropriate process model of the controller. (Figure 5-2). FRA's inappropriate notion about the new HSR system might cause unsafe controls in their regulatory activities. FRA often referred to the new HSR system being applied to the US as a "service-proven" technology [7][23]; FRA has been revising various regulations to allow introduction of mature international HSR technologies, which have an approximately 50-year history, to the US corridors. However, this notion is not necessarily true for what is going on in reality in the US, from a system perspective. Specifically, the following points cast doubt on the notion of "service proven."
        - The newly developed (or being developed) safety-related federal regulations are basically developed by revising the currently-used regulations with a strict consensus approach among related key stakeholders such as FRA, APTA and international suppliers, and labor unions. Therefore, there are few international, European, or Japanese safety standards being directly applied to the US's new regulations. For example, *49 Code of Federal Regulations 238* [108], which has a significantly strict requirement about the crashworthiness, is now being mitigated as of May 2014, but the new description of the regulation is said to be US-specific, which would require suppliers to change a mechanical structure of their train nose to comply with the new regulation [109].
        - Although HSR systems seem to procure their trainsets from international suppliers, the train control system called PTC, which is one of the safety-critical technologies, is currently being developed by the US railroads. Thus, the HSR physical system can be regarded as the integration of a domestic-quality signal system and international-quality rolling stock, as the Chinese HSR case can be. From a total system perspective, it is definitely inappropriate to call this integrated HSR system as "service proven." Additionally, under *Rail Safety Improvement Act* (RSIA) issued in 2008, railroads are required to equip PTC that can meet the functional requirements by 2015; in other words, each railroad is allowed to design its

[28] Risk 1 and 5-8 are also applicable to the interaction "Regulatory/certification Agency → TOCs and IMs.'

original PTC as long as the system meets the requirements. Therefore, interoperability has to be incorporated into all of the systems of the related TOCs and IMs [21][77]. The more these institutions are fragmented, the more potential risks would exist.

- The operational condition on the NEC is presumed to be unique, compared to other countries. According to the discussion in RSAC [109], the future HSR operation will be comprised of three different types of operations: Tier 1 (up to 125 mph), Tier 2 (up to 160 mph), and Tier 3 (up to 220 mph). Also, Tier 1 involves co-operation with freight rails. HSR technologies would have to comply with operational requirements for one or more of them.
- Passengers are also one component of the total system. Their behavior on trains or at stations, their cultural view to railway, or the purposes of their ride, could be the aspects taken into account in the system design process. Different countries or even corridors have different types of passengers.
- Operators of the system are also factors differentiating US's HSR from other HSRs. TOCs, IMs, and *Maintenance Company* are in the operation. Those of which have responsibilities for the current railway operation in the US would apply their experience or know-how to the new HSR operation.
- According to FRA's latest press releases [102][103], statutes about *Buy America* (PRIIA's *Buy America* provision *49 USC §24405(a)* [113] and *Buy American Act 41 USC §8301-§8305* [114]) are planned to be applied to HSR projects.[29] If these acts are applied to HSRs in the US, there are strict requirements for suppliers in system development. For example, final assemblies of HSR trainsets would have to be conducted in the US. Additionally, the manufacturers would have to use domestically manufactured components for the trainsets. Thus, it is presumed that international suppliers would face unexpected difficulties meeting these requirements in their system development processes. In this sense, the new HSR system is far from "service proven" HSR systems in other countries.
- There are several other factors that differentiate HSR systems in the US from others such as difference in geography, climate, required security levels, etc.

[29] Conditions for waiving these requirements are still being discussed. When Amtrak and CHSRA issued RFP (*Request For Proposal*) for high-speed train sets in Jan. 2014 [124], they specifically mentioned "this RFP encourages international rolling stock suppliers to build manufacturing factories in the US," but, at the same time, they submitted a waiver request to FRA, claiming "applying FRA's Buy America requirement to the purchase of the manufactured goods – four high-quality, service-proven prototype HSR trainsets – would be inconsistent with the public interest, and the manufactured goods cannot be bought and delivered in the United States within a reasonable time." [125]

If FRA has these inadequate notions about the new system, FRA's risk analysis could be inadequate, leading to its unsafe regulatory activities. According to Goodman, who analyzed safety risks in incorporating COTS (*Commercial Off The Shelf*) products into complex systems in space industries [115], when a COTS product is applied to a different system for which the COTS product was not designed, the application should be treated as a system development, rather than as a "plug and play" under a fixed-price/schedule contract. Similarly, Leveson discusses risks of reusing embedded application software for a different system, specifically suggesting specific requirements for successful reuse by introducing a system-based specification called *intent specifications* [80][81]. A key shared idea by these two researchers is that system integration requires as much risk awareness as system development from scratch even though some of the components in the system are "service proven."

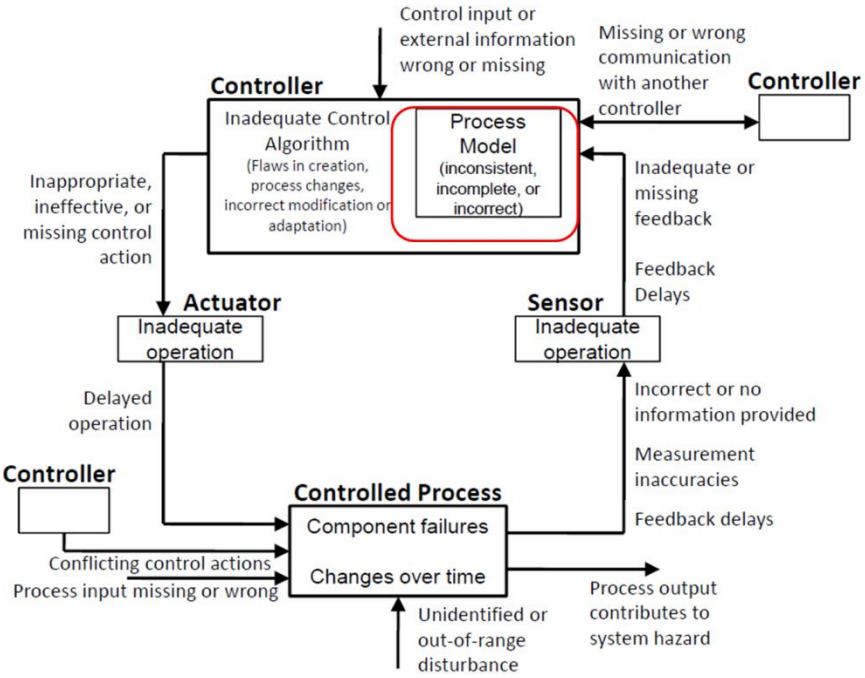

Figure 5-2 Type of causal factor (Inadequate process model)

- **Risk 2 (Inadequate control algorithm, Immediate, Alt. 1-3):** Inadequate control algorithm could be driven by FRA's limited experience in managing HSRs (Figure 5-3). For example, according to the current regulation, *49 CFR part 288.111*[30], FRA is responsible for certifying passenger equipment that has not yet been used for commercial operation in the US, inspecting

[30] As of May 2014, FRA is in the process of revising *49 CFR part 238.111*. The specific procedure for the certification is being discussed to be applicable to Tier 3 operation as well as the current Tier 1 and Tier 2 operation, and to accommodate international suppliers [109].

pre-revenue testings [108]. If this certification process is implemented with limited capabilities, unsafe certification could be provided to *System Integrators*. FRA has to clarify and take into consideration technical, operational, and managerial risks and future uncertainties in the new HSR development and operation, and needs to incorporate them into FRA's risk analysis and regulatory activities, with adequate support from experienced professionals. It should also be discussed whether FRA is capable of certification activities and whether third parties can be in charge of these activities.

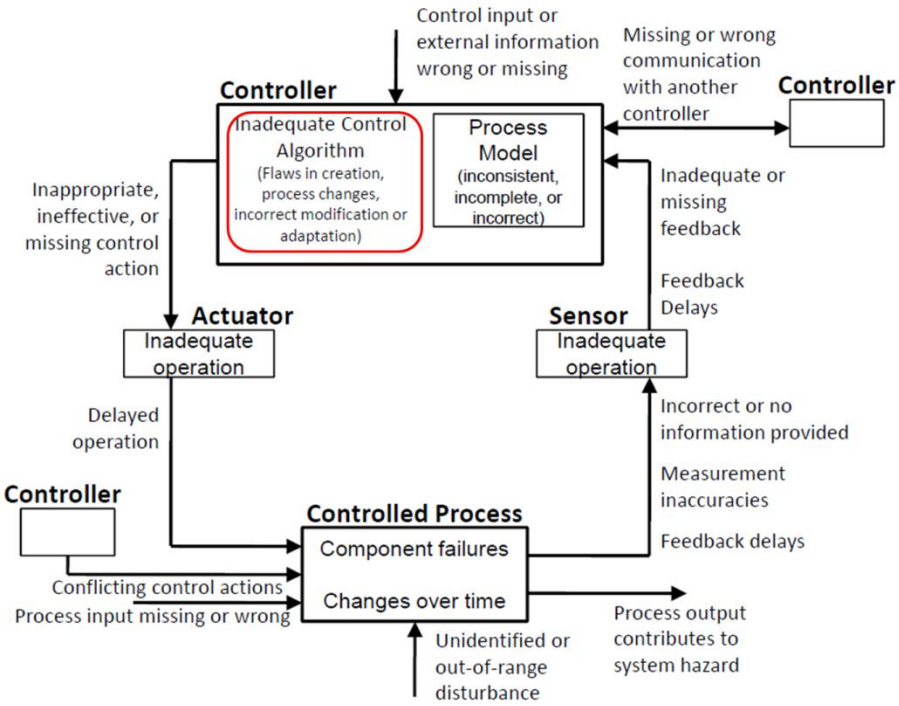

Figure 5-3 Type of causal factor (Inadequate control algorithm)

- **Risk 3 (Inadequate control algorithm, General, Alt. 1-3):** The current regulations about certification such as *49 CFR 238.111* might not be appropriate for the new HSR systems. Due to inadequate timing and order of certification processes, the identification of unsafe parts of the system in the certification might fail. Specifically, *49 CFR 238.111* requires FRA to inspect testing of a developed system only at a handover stage, just before starting revenue operation. However, this is not compatible with an international trend. For example, in Germany, the authority published a handbook on a certification process of rolling stock for suppliers, and this new certification process includes multiple "quality gates," in which authorities conduct inspections about safety and interoperability [118]. According to Kefer [119], these multi-phased inspections would help handle problems in system development, most of which arose earlier in

the design phase. Figure 5-4 presents the specific process to be followed for production and certification. Although the place of responsibility for train qualities had been unclear in Germany for many years, this handbook clearly defined the entity that has this responsibility as rolling stock manufacturers. While certifications are implemented by authorities in Germany, railroads in Japan have a unique certification system: most of the railroads themselves are in charge of actual inspections of developed systems.[31] Traditionally, Japanese railroads play roles of *System Integrator*, working closely with suppliers throughout the development process, and certification activities can be regarded to be implemented virtually in multiple stages of system development [120], similarly to the German case. For FRA, it is important to develop an sufficient certification process that can fit US rail industry and the new HSR system, identifying appropriate timings of certification activities in system development and evolution process of both rolling stock and infrastructure, and clarifying places and boundaries of safety responsibilities in the process among FRA (or other certification authorities), railroads, and suppliers. For these purposes, current regulations about certification processes such as *49 CFR 238.111* clearly need a drastic revision.[32]

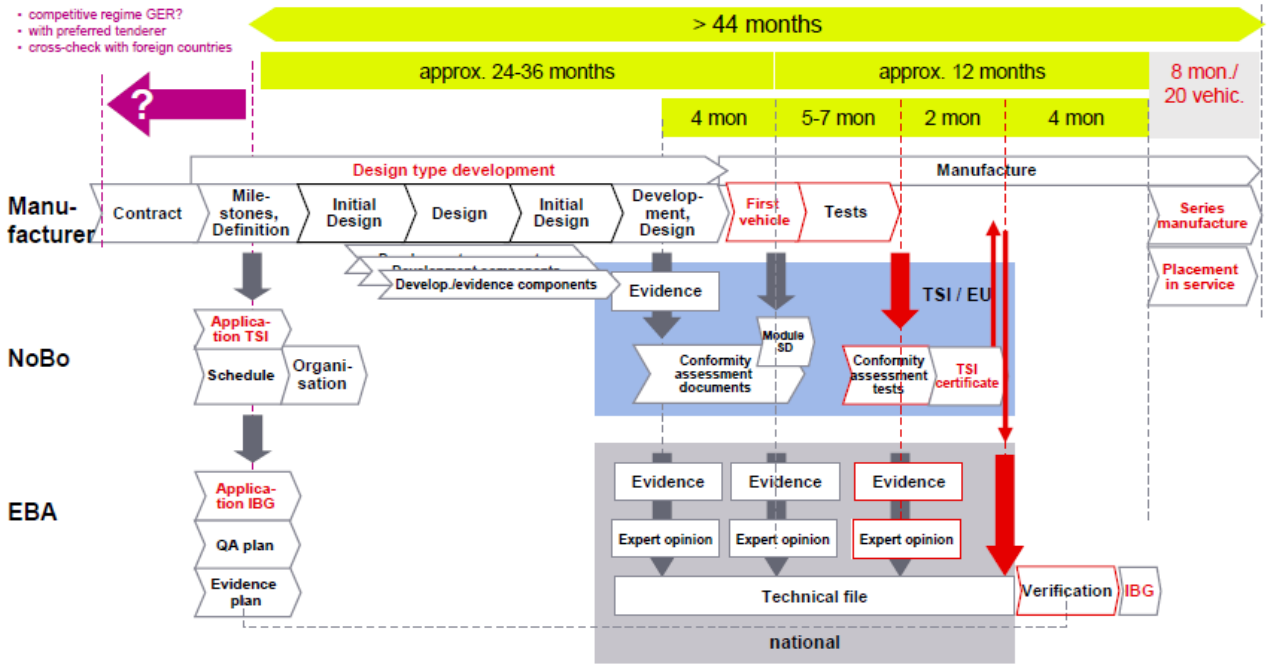

Figure 5-4 Multi-phased certification process in Germany [118]

[31] Ministry of Economy, Trade, and Industry of Japan trying to change this structure by establishing a governmental certification agency called Railway Certification Center in 2012, which is capable of performing certification about key international standards such as *IEC 62278* and *IEC 62280*, for improving compatibility of Japanese railway technologies with international markets.

[32] Other certification-related regulations such as for PTC or Infrastructure should be similarly analyzed.

- **Risk 4 (Inadequate process model, Immediate, Alt. 1-3):** FRA makes safety-related decision based on feedback from *System Integrators (rolling stock, infrastructure)*. If this feedback is wrong or missing, FRA's regulatory decisions could be hazardous (Figure 5-5). Basically, *System Integrators* will be international suppliers, some of which might be with limited business experience in the US. They could have difficulty in integrating information required for certification because they might have to cope with new partners in the US, some of which might not have adequate experience, due to *Buy America*. The documents required by regulation could be inadequate, which might not be recognized by either FRA or *System Integrators*, leading to FRA's unsafe control action (unsafe action provided or action required but not provided).

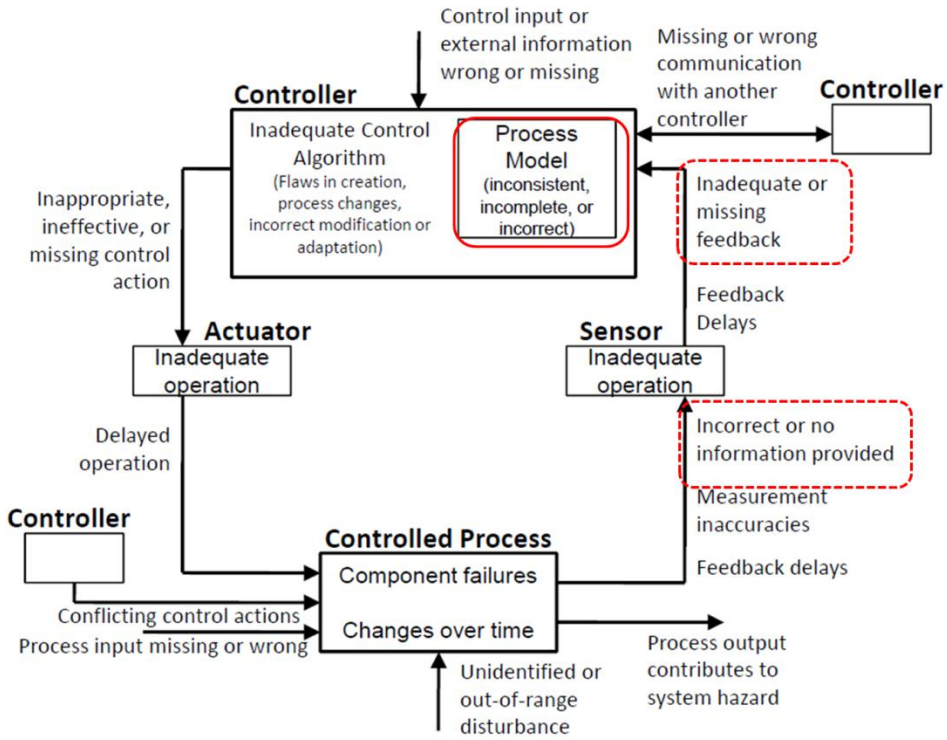

Figure 5-5 Type of causal factor (Inadequate process model due to inadequate feedback)

- **Risk 5 (Inadequate inputs to the controller, General, Alt. 1-3):** Similarly to Risk 4, FRA makes safety-related decision based on input information from interaction with other components in the model (Figure 5-6). If this input is wrong or missing, FRA's regulatory decisions could be hazardous. For example, FRA also has interaction with TOC(s) and IMs, as shown in Figure 4-8, 4-9, and 4-10. Having fragmented industry could cause delay of input and require FRA to take significant time to make a safety-related decision and implement it for system evolution. Thus,

this non-timely decision making could delay implementation of necessary safety regulatory actions.

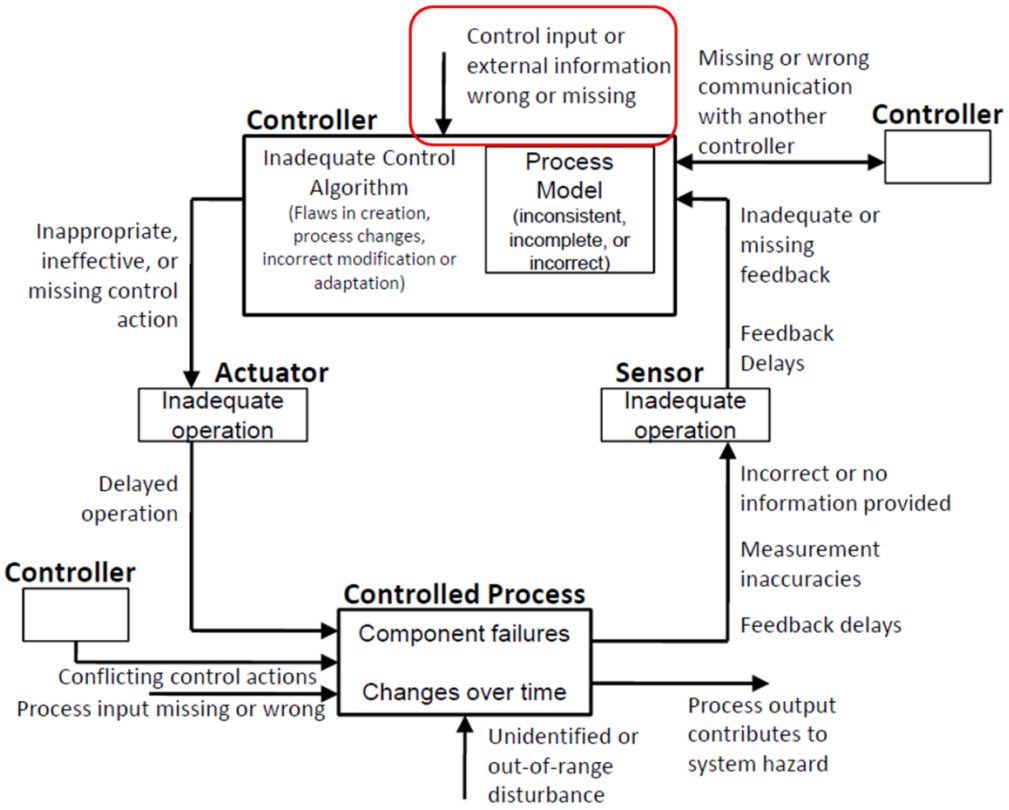

Figure 5-6 Type of causal factor (Inadequate inputs to the controller)

- **Risk 6 (Inadequate control algorithm, General, Alt. 1-3):** Although it is not described in the control structure in Figure 4-8, 4-9, and 4-10, there are many stakeholders involved in the decision making process of safety regulation, such as labor unions, APTA, Volpe (*The National Transportation Research Center* in DOT), international/domestic suppliers, and international railroads. Any decision is made based on a strict consensus approach among the government, labor unions, and industry [109]. FRA has to handle several risks that could be caused by this consensus approach; it might not be easy that regulatory decision making in system evolution is done immediately after its necessity comes out, or that safety becomes the first priority for all of the agencies involved in the decision making processes due to conflict of their interests.

- **Risk 7 (Inadequate control algorithm**, **General, Alt. 1-3):** Due to a pressure from the Congress about safety accountability, FRA's regulatory decision making might be too conservative and

necessary actions might not be taken timely, especially if FRA does not have clear criteria in decision making based on risk analysis.

- **Risk 8 (Inadequate control algorithm/process model, General, Alt. 1-3):** FRA has a responsibility to perform cost-benefit analysis and evaluate a financial impact of new safety regulations. Due to future uncertainties, lack of capability, or lack of understanding of the industry, FRA could overestimate the financial impact of regulatory decision on the US rail industry, which could delay the implementation or could implement an inadequate regulation.

- **Risk 9–15: *System Integrators (rolling stock or infrastructure)* [domestic or international suppliers] → *R&D Company/Suppliers (rolling stock or infrastructure)* [domestic or international suppliers]**

  - **Risk 9 (Inadequate inputs to the controller, Immediate, Alt. 1-3):** International *System Integrators* might not have adequate knowledge about railway operation and maintenance in the US, which contains different customs and rules from other countries'. Or TOC(s) and IM(s) might not provide adequate information about operation and maintenance. Thus, *System Integrators* could provide wrong requirements to *R&D companies or suppliers*, or inadequate requirements missing safety-related operation/maintenance information.

  - **Risk 10 (Inadequate inputs to the controller, Immediate, Alt. 1-3):** Similarly to Risk 9, TOC(s) and IM(s) might not provide adequate information about operation and maintenance, because their business partnership with *System Integrators* might not be well-developed, especially at the initial stage of system development. By this, *System Integrators* could provide wrong requirements to *R&D companies or suppliers*, or inadequate requirements missing safety-related operation/maintenance information.

  - **Risk 11 (Inadequate process model, Immediate, Alt. 1-3):** *Buy America* would require international *System Integrators* to cope with domestic suppliers, which are presumably not well experienced as HSR suppliers. If *System Integrators* are overconfident about the capabilities of the domestic suppliers, *System Integrators* could not identify their unsafe work. Thus, inadequate process model of the controlled process could lead to conducting inadequate receiving inspection.

- **Risk 12 (Inadequate process model, General, Alt. 1-3):** Having too many TOCs and IMs causes fragmentation of design responsibilities of *System Integrators.* This situation could cause their inadequate understanding about the total system and interfaces of the responsibilities (i.e., inadequate control algorithm), which could lead to providing inadequate safety requirements to *R&D companies and suppliers*. This risk might be mitigated in Alternative 2, which has single TOC and single IM, but still, if they have *System Integrators* for rolling stock and Infrastructure separately due to its vertically separated structure, the responsibility for their system boundary must be clarified to avoid unsafe development.

- **Risk 13 (Inadequate inputs to the controller, Immediate, Alt. 1-3):** International *System Integrators* might not adequately understand rationales of safety regulation due to the lack of business experience in the US, thus providing incomplete or inappropriate safety requirements to *R&D companies and suppliers*. FRA has to make these rationales available to any of *System Integrators* and *R&D companies and suppliers.*

- **Risk 14 (Inadequate process model, General, Alt. 1-3):** Due to *Buy America, System Integrators* might need to work with unexperienced domestic suppliers, and they might not provide products with adequate qualities constantly. If *System Integrators* do not monitor the capability of *R&D Company and Suppliers* over time, *System Integrators'* receiving inspections could be conducted inadequately due to *System Integrators'* overconfidence.

- **Risk 15 (Inadequate control algorism, General, Alt. 1-3):** Due to *Buy America, System Integrators* might need to work with unexperienced domestic suppliers and to integrate a new supply chain. As Boeing experienced in the Boeing 787 project, a newly created supply chain with unfamiliar suppliers could cause cost overrun and schedule delay in the project, which could reduce resources that *System Integrators* can use for safety-related activities. Thus, their control algorithm could become less safety-oriented, thereby providing inadequate safety requirements or conducting inadequate safety inspections.

- **Risk 16–18: *R&D Company/Suppliers (rolling stock or infrastructure)* [domestic or international suppliers] → *Manufacturers (rolling stock or infrastructure)* [domestic or international manufacturers]**

  - **Risk 16 (Inadequate process model, General, Alt. 1-3):** There might be some newly involved domestic suppliers that pursue only short-term profits and do not keep involved in the supply chain for long periods. Unstable industrial structure in system development could impede system evolution, which requires continuous efforts for improvement from any of the industrial members. Thus, the controller's inadequate process model of the unstable industrial structure could provide unsafe control actions.

  - **Risk 17 (Inadequate inputs to the controller, General, Alt. 1-3):** If *System Integrators* do not provide adequate information about operation or maintenance, *R&D Company and Suppliers* could provide unsafe requirements to manufacturers.

  - **Risk 18 (Failure of the controlled process, Immediate, Alt. 1-3):** *Buy America* might require final assemblies of rolling stock to take place in the US. If *R&D Company and Suppliers* overestimate the capability of local manufacturers unfamiliar to them, they might overlook the local manufacturers' unsafe performance in manufacturing (Figure 5-7). Thus, safe control actions are provided but the controlled process does not follow them.

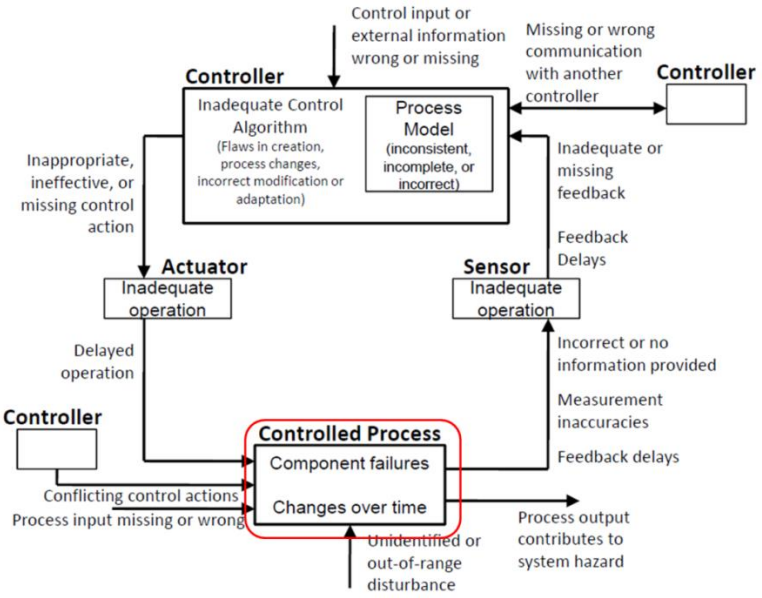

Figure 5-7 Type of causal factor (Failure of the controlled process)

- **Risk 19–21: *Regulation/certification Agency* [FRA] → TOC(s) [Amtrak, private operators], IM(s) [Amtrak, Regional authorities, New public agency], *Infrastructure Owner* [New public agency][33]**

  - **Risk 19 (Inadequate control algorism, General, Alt. 1-3):** As mentioned in Risk 2, incorrect control algorithm could be driven by FRA's limited experience in managing HSRs. Due to the lack of experience, risk analysis about train operation and maintenance might be inadequate, which could lead to providing inadequate regulations.

  - **Risk 20 (Inadequate control algorism, General, Alt. 1-3):**
    - **Alternative 1**: Even if the current institutional structure is applied, FRA has to appropriately evaluate the operational capabilities of TOC and IMs (Amtrak and regional authorities) for the new HSR, because of the drastic system change described in Risk 1. If FRA overestimates their capabilities and does not monitor them adequately, they could provide unsafe operation. It is necessary to establish appropriate managerial and technical performance metrics to monitor their condition over time and clear criteria for FRA's decision making. SSP is expected to facilitate FRA in this issue, but specific metrics or criteria are not yet clearly defined in its NPRM published in 2012 [25].
    - **Alternative 2**: Similarly to Alternative 1, FRA has to evaluate the capabilities of Amtrak (TOC) and the new public infrastructure owner appropriately. In particular, the new public agency, owning a significant amount of assets, has a responsibility to manage them, although it has no experience in taking this responsibility. If FRA overestimates their capability and does not monitor them adequately, they could provide unsafe operation, or the new public agency could provide unsafe requirement to TOC. It is necessary to establish appropriate managerial and technical performance metrics to monitor their condition over time and clear criteria for FRA's decision making.
    - **Alternative 3**: Similarly to Alternative 1 and 2, FRA has to appropriately evaluate the capabilities of TOCs (Amtrak and private TOCs) and the new public infrastructure owner. In particular, the new public agency, which would own a significant amount of assets, has a responsibility to manage them cooperating with IM, although it has no experience of taking this responsibility. Additionally, the newly involved public private TOCs could have less operational experience in the US or even anyplace in the world. It might also be a concern that those private agencies are more strongly fixated on their operational profits than public

[33] Risk 1 and 5-8 are also true for this interaction.

agencies would be. If FRA overestimates their capability and does not monitor them adequately, they could provide unsafe operation, or the new public agency could provide unsafe requirement to IM. It is necessary to establish appropriate managerial and technical performance metrics to monitor their condition over time and clear criteria for FRA's decision making.

- **Risk 21 (Inadequate control algorithm/process model, General, Alt. 1-3):** FRA has a responsibility to perform cost-benefit analysis and evaluating financial impact of new regulations. Due to future uncertainties, lack of capability, or lack of understanding of the industry, FRA could underestimate the financial impact of regulatory decision on the industry, which could provide financial problems for TOC(s) or IM(s) and make them comply with the regulation untimely or inadequately.

- **Risk 22–24: TOC [Amtrak, private TOCs] → *Train Operator* [Amtrak, private TOCs]**

  - **Risk 22 (Inadequate process model, General, Alt. 1-3):** TOC (Amtrak) could have inadequate understanding of the new HSR system, especially about emergency operation, which could lead to unsafe training or unsafe manual development for train operators.

  - **Risk 23 (Inadequate process model, General, Alt. 1-3):** Operation manual needs to be improved with the feedback from operators after the introduction of the new system based on what the operators actually experiences, but this process might not be performed well due to the lack of adequate communication between management-level people and operators in TOC(s). This issue can also be seen in the current Amtrak's operation. To solve this issue, *Confidential Close Call Reporting System* (C3RS) [34]is being introduced in the US. At any rate, there is a need for effective and speedy information sharing system between management-level people and operators, especially immediately after starting the new HSR operation.

  - **Risk 24 (Conflicting control actions, Genera, Alt. 1)**: This risk is applicable only to Alternative 1. Although it is not described in the safety control model in Figure 4-8, 4-9, and 4-10, *Train Operator* has other control interactions with multiple dispatchers with respect to routing. IM(s)

[34] C3RS (Confidential Close Call Reporting System) is an FRA-funded project to improve rail safety by collecting information about potentially unsafe conditions or close call events. Operators can voluntarily and confidentially report close calls without fear of discipline or punishment.(http://www.closecallsrail.org/faq_about.aspx)

are segmented according to operational areas, but their directives might have a "control" conflict with one another and with TOC's control, which could lead to inadequate operational directives from TOC to Train Operator (Figure 5-8). TOC and IM must clarify possible operational conflicts in interfaces and create coordinated procedures.

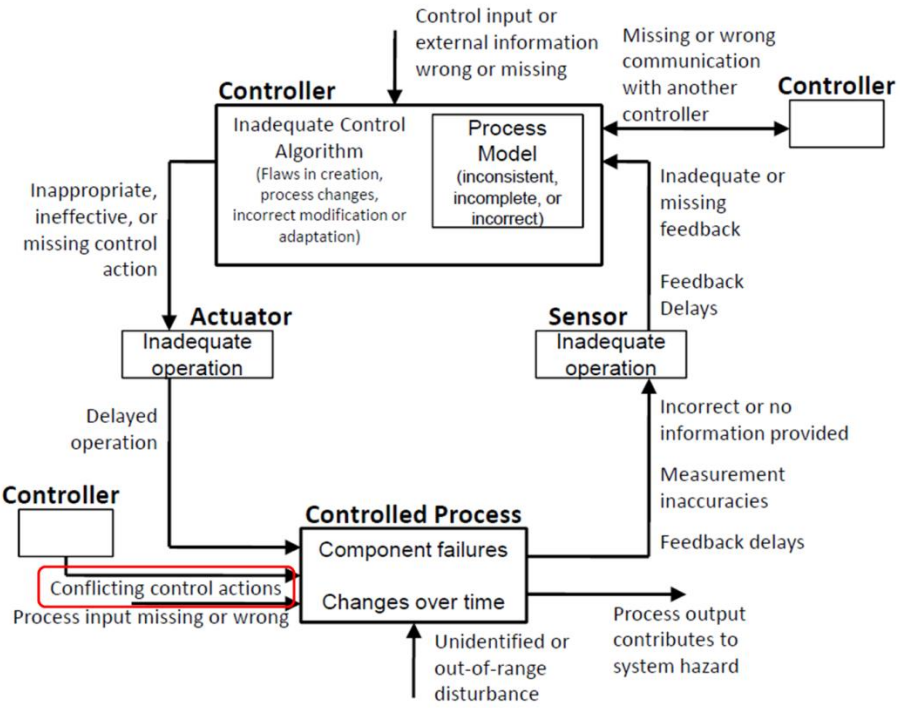

Figure 5-8 Type of causal factor (Conflicting control actions)

- **Risk 25–27: TOC(s) [Amtrak, private operators] → *Maintenance Company (rolling stock)* [contractors]**

  - **Risk 25 (Inadequate process model, Immediate, Alt. 1-3)**: TOC(s) might take main responsibility for frontline maintenance work, but some of the tasks are generally outsourced to contractors. Maintenance requirements could need continuous improvement especially at the initial stage of the new HSR operation, and for this, feedback report about safety-related issues from the contractors are crucial. If TOC(s) underestimate the risk of this initial phase of operation and did not appropriately manage maintenance contractors, TOC(s) would perform an unsafe control action, providing inadequate maintenance requirements.

- **Risk 26 (Inadequate process model, Immediate, Alt. 1-3)**: *System Integrators, R&D Company*, or *Suppliers* could be in charge of maintenance as well. TOC(s) might inadequately understand maintenance capabilities of those companies, which might not be well experienced due to *Buy America*, and TOC(s) could have inadequate communication with them about maintenance requirements and results, which leads to providing inadequate safety requirements with which the maintenance contractors have difficulty complying.

- **Risk 27 (Inadequate control algorithm, General, Alt. 3):** This risk is applicable only to Alternative 3. Some of the TOCs could have financial issues due to market competition with other TOCs, thereby lowering the priority of safety in their decision making processes about maintenance management and providing unsafe maintenance requirement to *Maintenance Companies*, as Railtrack in the UK did (see Section 3.1).

- **Risk 28-34: TOC [Amtrak, private operators] → *System Integrator (rolling stock)* [domestic or international suppliers]**

  - **Risk 28 (Inadequate control algorithm/process model, Immediate, Alt. 1-3)**: TOC(s) might fail to comprehensively integrate operational safety requirement that are not stipulated in safety regulation due to an inadequate hazard analysis or understanding of the new operation. Especially in Alternative 3, this risk would become higher if private TOCs, some of which could be unexperienced, unskilled, or incapable if FRA's monitoring is inadequate, are involved in the operation. Thus, inadequate control algorithm and process model of TOS(s) could lead to providing inadequate safety requirements.

  - **Risk 29 (Inadequate control algorithm/process model, Immediate, Alt. 1-3)**: It is desirable that TOC(s) is constantly involved in system development processes to incorporate operation/maintenance perspectives, and check if these objectives are met appropriately. In the new HSR system development, TOC(s) would have to work with International *System Integrators* that TOC(s) has had less business experience with, or TOC(s) would have difficulty in having fluent communication with them due to a language gap. Insufficient involvement of TOC(s) to the development could cause an unsafe situation in which TOC(s) provides inadequate safety requirements that international *System Integrators* do not sufficiently understand, or in which TOC(s) does not realize possible safety issues in the receiving inspection process. Especially in Alternative 3, this risk would become higher if private TOCs, some of which could be

unexperienced, unskilled, or incapable if FRA's monitoring is inadequate, are involved in the operation.

- **Risk 30 (Inadequate inputs to the controller, General, Alt. 1-3)**:
  - **Alternative 1:** The operation/maintenance issues to be reflected to the system evolution might not adequately be provided to Amtrak (TOC) from *Maintenance Companies (infrastructure)* due to the vertically separated responsibilities between Amtrak (TOC) and the regional authorities (IMs) and fragmented infrastructure ownership, and thereby Amtrak (TOC) might not provide appropriate safety requirement to *System Integrator (rolling stock)* in the system evolution process.
  - **Alternative 2:** Compared to Alternative 1, Alternative 2 has a higher risk of having inadequate system evolution due to its completely vertically separated institutional structure. Amtrak (TOC) might not provide appropriate safety requirement to *System Integrator (rolling stock)* in the system evolution process due to inadequate feedback from the new public agency (IM) about maintenance issues related to train operation.
  - **Alternative 3:** Similarly to Alternative 1 and 2, Alternative 3 has a risk of having inadequate system evolution due to its partially vertically separated institutional structure and fragmented TOCs. The private TOCs might not provide appropriate safety requirement to *System Integrator (rolling stock)* in the system evolution process due to inadequate feedback from Amtrak (IM) about maintenance issues related to train operation.

- **Risk 31 (Failure of the controlled process, Immediate, Alt. 1-3)**: Initial system development or following system evolution might take longer time than planned due to the immature domestic supply chain that could be caused due to *Buy America*, which could lead to unsafe system development caused by programmatic performance pressure or lead to slow system evolution.

- **Risk 32 (Inadequate control algorithm/process model, General, Alt. 1-3):** There is a possibility that TOC(s) takes a responsibility for system integration, instead of *System Integrator*, as some Japanese railroads do. In this case, if the TOC(s) has inadequate understanding about the new system and are not capable of designing the interfaces among subsystems, their safety requirement to *System Integrator* could be unsafe. Especially in Alternative 3, this risk would become higher if private TOCs, some of which could be unexperienced, unskilled, or incapable if FRA's monitoring is inadequate, are involved in the operation.

- **Risk 33 (Inadequate control algorithm, General, Alt. 3):** This risk is applicable only to Alternative 3. There might be some private TOCs that are not motivated to commit system evolution because different private TOCs have different financial conditions, management policies, or contents of hazard analyses. This diversity of management in the industry could cause imperfect system evolution or delay of system evolution.

- **Risk 34 (Inadequate inputs to the controller, General, Alt. 3):** This risk is applicable only to Alternative 3. The operation/maintenance issues to be reflected to system evolution might not adequately be shared among the fragmented TOCs, and thereby, they might provide uncoordinated, unsafe requirement to each *System Integrator (rolling stock)* in the system evolution.

- **Risk 35-39: IM(s) [Amtrak, regional authorities, a new public agency] → TOC(s) [Amtrak, private operators]**

  - **Risk 35 (Inadequate process model, Immediate, Alt. 1-3):** IM(s) could have inadequate understanding of the new HSR system, which could make them not provide safety requirements about train operation, especially about emergency situations, to TOC(s).

  - **Risk 36 (Conflicting control actions, Immediate, Alt. 1):** This risk is applicable only to Alternative 1. If there is any inadequate coordination among IMs (Amtrak and regional authorities), operational requirement to TOC (Amtrak) could be inconsistent at the boundaries of the infrastructure ownerships, leading to TOC's unsafe operation.

  - **Risk 37 (Inadequate process model, General, Alt. 1-3):** The (partially) vertically separated industrial structure could cause inefficient communication between TOC(s) and IM(s), thereby delaying safety requirement provided from the IM(s) to the TOC(s).

  - **Risk 38 (Conflicting control actions, General, Alt. 2-3):** This risk is applicable only to Alternative 2 and 3. TOC(s) needs to comply with both safety regulations from FRA and operational safety requirements from the IM (and *Infrastructure Owner* in the case of Alternative 3). If the IM, as Railtrack in the UK did, sets safety-related rules and they are not compatible with FRA's regulation, the conflicting controls could cause TOC(s) to conduct unsafe train operation.

- **Risk 39 (Inadequate control algorithm/process model, General, Alt. 3):** This risk is applicable only to Alternative 3. Having multiple TOCs could create technical and managerial complexity in coordinating their operations based on their operational plans and types of fleet. If IM (Amtrak) has inadequate planning and operational capabilities managing these complexities, especially in emergency situations, if the IM (Amtrak) does not have adequate communication with the TOCs about operational procedure, especially of emergency situations, or if IM (Amtrak) has inadequate hazard analysis, IM's safety requirement to TOCs about train operation could be inadequate.

- **Risk 40-42: IM(s) [Amtrak, regional authorities, a new public agency] → *Dispatcher* [Amtrak, regional authorities, a new public agency]**

  - **Risk 40 (Inadequate process model, Immediate, Alt. 1-3):** IM(s) could have inadequate understanding of the new HSR system and could not perform comprehensive hazard analysis, which could lead to inadequate operational directive, operational manual design, or training.

  - **Risk 41 (Inadequate control algorithm, Immediate, Alt. 1):** This risk is applicable only to Alternative 1. There might be some regional authorities (IMs) that do not have adequate technical or financial capabilities of performing hazard analysis, which could lead to inadequate operational directive, training or operational manual design.

  - **Risk 42 (Inadequate process model, General, Alt. 1&3):** This risk is applicable only to Alternative 1 and 3. Due to the organizational boundary between *Dispatchers* and *Train Operator*s, anomalies of the infrastructure that could be discovered by *Train Operators* in the operation might not be reported to the IM(s), which could make IM(s) have an inadequate process model and miss an opportunity to improve the safety level of infrastructure.

- **Risk 43-47: IM(s) [Amtrak, regional authorities, a new public agency] → *Maintenance Company (infrastructure)* [contractors]**

  - **Risk 43 (Inadequate process model, Immediate, Alt. 1-3):** IM(s) could have inadequate understanding of the new HSR system and might not perform comprehensive hazard analysis, which could lead to inadequate maintenance safety requirement to Maintenance Companies.

- **Risk 44 (Inadequate process model, General, Alt. 1):** This risk is applicable only to Alternative 1. The newly updated HSR line could require IMs to have additional infrastructure maintenance contractors. Some of IMs might fail to adequately monitor the managerial condition especially of these new contractors over time. Overconfidence in its own management capability due to its operation experience on the NEC or inadequate realization about contractors' capabilities could lead to this inadequate contractor management.

- **Risk 45 (Inadequate control algorithm, General, Alt. 1):** This risk is applicable only to Alternative 1. There might be some regional authorities that do not have adequate technical or financial capabilities of performing hazard analysis, which could lead to inadequate maintenance safety requirement to *Maintenance Companies*.

- **Risk 46 (Inadequate process model, General, Alt. 1-3):** Due to the organizational boundary between IM(s) and TOC (s), anomalies of the infrastructure that could be discovered by *Train Operator* in the operation might not be reported to regional authorities, which could make IM(s) have an inadequate process model and miss an opportunity to improve the safety level of infrastructure maintenance.

- **Risk 47 (Inadequate control algorithm/process model, General, Alt. 2-3):** This risk is applicable only to Alternative 2 and 3. IM would have to manage multiple maintenance contractors to maintain the extensive ROW (right-of -way), and some of the contractors could be relatively less experienced. If the IM overestimates contractors' skills, it might fail to adequately monitor the managerial condition especially of these less-capable contractors over time, which could lead to unsafe maintenance. It is necessary for the public agency to have appropriate managerial and technical performance metrics to monitor contractors' condition over time and to have clear criteria for the agency's decision making.

- **Risk 48-54: IM(s) [Amtrak, regional authorities, a new public agency] → *System Integrators (infrastructure)* [domestic or international suppliers]**

  - **Risk 48 (Inadequate control algorithm/process model, Immediate, Alt. 1-3):** IM(s) might fail to comprehensively integrate operational safety requirement that are not stipulated in safety regulation due to an inadequate hazard analysis or understanding of the new infrastructure

operation. Thus, inadequate control algorithm and process model of TOS(s) could lead to providing inadequate safety requirements.

- **Risk 49 (Inadequate control algorithm/process model, Immediate, Alt. 1-3):** It is desirable that IM(s) are constantly involved in system development process to incorporate operation/maintenance perspectives, and check if these objectives are met appropriately. In the new HSR system development, IM(s) would have to work with international *System Integrators* that have had less business experience with them, or they would have difficulty in having fluent communication with *System Integrators* due to a language gap. Insufficient involvement of IM(s) to the development could cause an unsafe situation in which IM(s) provides inadequate safety requirements that international *System Integrators* do not sufficiently understand, or in which IM(s) do not realize possible safety issues in the receiving inspection process.

- **Risk 50 (Inadequate inputs to the controller, General, Alt. 1):** This risk is applicable only to Alternative 1. The operation/maintenance issues to be reflected to system evolution might not adequately be shared among the fragmented IM(s), and thereby, they might provide uncoordinated, unsafe requirement to each *System Integrator (infrastructure)* in the system evolution.

- **Risk 51 (Failure of the controlled process, Immediate, Alt. 1-3):** Initial system development or following system evolution might take longer time than planned due to the immature domestic supply chain that could be caused due to *Buy America*, which could lead to slow system evolution.

- **Risk 52 (Inadequate process model, General, Alt. 1-3):** Due to the organizational boundary between IM(s) and TOC(s), anomalies of the infrastructure that could be discovered by *Train Operator(s)* in the operation might not be appropriately reported to regional authorities, which could make IM(s) have an inadequate process model and miss an opportunity to improve the safety level of infrastructure in system evolution.

- **Risk 53 (Inadequate control algorithm, General, Alt. 1-3)**: There might be some IM(s) that do not have adequate technical or financial capabilities of performing hazard analysis for system development, which could lead to providing inadequate safety requirement to *System Integrator (Infrastructure)*.

- **Risk 54 (Inadequate control algorithm/process model, General, Alt. 1-3):** There is a possibility that some of the IM(s) have responsibility for system integration, instead of *System Integrator(s)*, as some Japanese railroads do. In this case, if the IM(s) playing as *System Integrator(s)* have inadequate understanding about the new system and are not capable of designing the interfaces among subsystems, their safety requirement to *System Integrators* could be unsafe.

- **Risk 55: *Infrastructure Owner* [new public agency] → IM [Amtrak]**

  - **Risk 55 (Conflicting control actions, General, Alt. 3):** This risk is applicable only to Alternative 3. If *Infrastructure Owner* and IM are separate agencies, the roles of FRA and *Infrastructure Owner* in safety management of the IM must be clearly defined without any overlapping. If this definition is unclear, they could have conflicting controls, which could lead to unsafe performance of the IM.

- **Risk 56-58: *Maintenance Companies (rolling stock, infrastructure)* [contractors] → *Maintenance Workers (rolling stock, infrastructure)* [contractors]**

  - **Risk 56 (Inadequate process model, Immediate, Alt. 1-3):** If *Maintenance Companies* have limited understanding about the new HSR system, or if they do not receive adequate information about maintenance requirement from IM(s) or TOC(s), maintenance directives, manuals, and training to *Maintenance Workers* could be inadequate.

  - **Risk 57 (Inadequate process model, Immediate, Alt. 1-3):** *Maintenance Companies* could overestimate maintenance skills of *Maintenance Workers* that have the current maintenance experience in the Acela operation, which could lead to providing inadequate maintenance requirement.

  - **Risk 58 (Inadequate control algorithm/process model, Immediate, Alt. 2-3):** This risk is applicable only to Alternative 2 and 3. The introduction of the new system could cause frequent technical problems in an early phase of the revenue operation. Inappropriate management of the data acquired from these problems or inadequate feedback from the *Maintenance Workers* could cause delay of maintenance timing or lead to unsafe maintenance.

5.2.2 Evaluation of the System Safety Program (SSP)

The identified risks can be applied to evaluate and design regulation. In this research, SSP is evaluated as an example [25]. SSP consists of the following four subparts: subpart A – *General* (§270.1 - §270.9), subpart B – *System Safety Program Requirements* (§270.101 - §270.105), subpart C – *Review, Approval, and Retention of System Safety Program Plans* (§270.201 - §270.203), and subpart D – *System Safety Program Internal Assessments and External Auditing* (§270.301 - §270.305). Specifically, subpart A describes purposes and scopes of SSP, specifying the definition of terminologies in SSP, entities to which SSP is applied, and penalties when they do not comply with SSP. Subpart B describes the requirements for SSP plans, which railroads[35] must develop in this program. Description about specific safety risk management[36] is included in this subpart. Subpart C describes tasks in review, approval, and retention of SSP plans. FRA is supposed to review and approve SSP plans proposed by railroads. Lastly, subpart D describes internal and external safety audits. The excerpts of these four subparts are shown in Appendix B. For each subpart, possible weaknesses of SSP are discussed below.

- **Weaknesses related to Subpart A - General**
  - SSP is planned to be applied to "*(1) railroads that operate intercity or commuter passenger train service on the general railroad system of transportation, and (2) railroads that provide commuter or other short-haul rail passenger train service in a metropolitan or suburban area*." Therefore, the main focus of SSP plans is how to implement operation management safely from railroads' perspectives; i.e., SSP does not deal with safety interactions in the system development domain or those between a regulator and regulated organizations. Specifically, risk 1to 21 identified in 5.2.1 are not tackled in SSP. Thus, in light of multi-angled discussion in this research, SSP is not a sufficient tool for system safety management in the NEC HSR.

- **Weaknesses related to Subpart B – SSP Requirements**
  - According to the description in §270.102 *Consultation requirements*, railroads are not necessarily required to enforce all employees, e.g. non-profit employee labor organization, to comply with SSP, which could be a significant hole in SSP implementation. Risk 23, 24, 25, and 42 could be a possible outcome of this inadequate, unorganized safety management among labors.

[35] In SSP, "*Railroad*" is defined as "*any form of non-highway ground transportation that runs on rails or electromagnetic guideways, including (i) commuter or other short-haul rail passenger service in a metropolitan or suburban area and commuter railroad service that was operated by the Consolidated Rail Corporation on Jan.1, 1979; and (ii) high speed ground transportation systems that connect metropolitan areas, without regard to whether those systems use new technologies not associated with traditional railroads, but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation.*"
[36] In SSP, safety risk management is referred to as "Risk-based hazard management."

- Although railroads need detailed understanding of the physical system to perform adequate risk analysis, SSP does not adequately mention the importance of communication between suppliers and railroads. Thus, the risk analysis might not appropriately evaluate risks related to issues in the physical system, possibly causing risk 22, 35, 40, 43, and 56.
- Due to the operation-oriented scope of SPP, perspectives of system evolution based on lessons in maintenance and operation are not adequately described, which could cause risk 23, 25, 42, 49, 50, 52, and 58.
- SSP mentions that railroads should communicate with other entities that are related to any part of SSP, specifically with respect to emergency management, technology analysis, and hazard analysis, but SSP does not ensure adequate coordination of this communication. This coordination issue could be a significant safety risk, especially when the NEC HSR has a complex institutional structure. Risk 24, 36, 38, and 55 could be caused by this issue.
- Analytic tools for risk identification and evaluation are not specified in SPP in order to allow railroads to conduct their management flexibly, but this could lead to inconsistent quality of safety management in the industry if FRA does not review and approve SSPs in a consistent way. Risk 41 and 45 could be caused by this issue.

- **Weaknesses related to Subpart C - Review, Approval, and Retention and subpart D –Auditing**
  - FRA has a significant responsibility to overarch diverse SSP plans implemented by various organizations in the industry on the same basis, consistently over time even if the system changes. Additionally, FRA needs to comprehensively manage risks created at the institutional level that could not be identified by any individual SSP. Specifically, the following is requirements for this overarching activity.

    - Need to define a procedure for harmonizing all of the individual system safety approach.
    - Need to define consistent criteria about risk evaluation and risk acceptance.
    - Need to manage weaknesses of underlying system safety activities.
    - Need to incorporate flexibility to adapt all system safety activities to any future changes of the industry (e.g., privatization, open access, technology innovation)

    In light of these significant responsibilities of FRA, overseeing FRA's activities could be an important aspect of system safety management of the NEC HSR, which is not mentioned in SSP.

In the next section, the identified risks in Section 5.2 are further analyzed with SD models.

5.3 Detailed Causal analysis (System Dynamics)

In the previous sections, various modes of causal relations are analyzed based on the STPA guidewords, and NEC-specific 58 risks are identified. Some of the identified risks are described with similar causal reasoning because their causal factors are interrelated. For further understanding of the risk creation mechanism, it is necessary to analyze causal factors further in detail from a broader perspective. While STPA focuses on each control loop that include a controller, controlled process, and their interactions one by one, the causal analysis with System Dynamics (SD) expands the causal relation to the entire system level by connecting causal factors for multiple risks related to one another. Thus, SD can incorporate indirect causal factors into the primitive causal relations identified by STPA, in a visually-understandable way. Furthermore, SD is an appropriate tool to analyze a dynamic behavior of safety levels of systems; e.g., SD can consider the dynamic impact of multiple changes within the entire safety control structure, which would be difficult to analyze by STPA.

This research discusses applicability of SD modeling for risk analysis, applying SD to two specific issues "Coordination in train operation" in Section 5.3.1 and "Open access" in Section 5.3.2. For each topic, multiple risks and their causal factors identified in Section 5.2.1 are integrated as SD models.[37] Impact of the difference of the institutional structures among Alternative 1, 2, and 3 are also organized in one model for each issue. With these results, possible applications of SD modeling for safety risk management are discussed in Section 5.3.3.

5.3.1 Coordination in Train Operation and Safety

In train operation that involves multiple organizations, coordination of operational rules and processes, including ones in emergency operation, among them are crucial for safety. At a front-line operation level, sharing consistent *process models* among all of the *Train Operators* and *Dispatchers* is important. At an institutional level, which this research focuses on, appropriate operational coordination among TOC(s) and IM(s) and appropriate corporate management within each organization are important, as discussed in Risk 23, 24, 36, 37, 39, and 42 in Section 5.2.1.

As a first step, a SD model representing the interaction between TOC and *Train Operator* is developed in Figure 5-9.

[37] For simplicity, mathematical descriptions of the models are not necessarily accurate in this research; e.g., some of the "variables" in the models should be represented with "stock" and "flow." The purpose of this System Dynamics analysis is to clarify complex causal relations of risks, and this mathematical simplification does not change the causal relations.

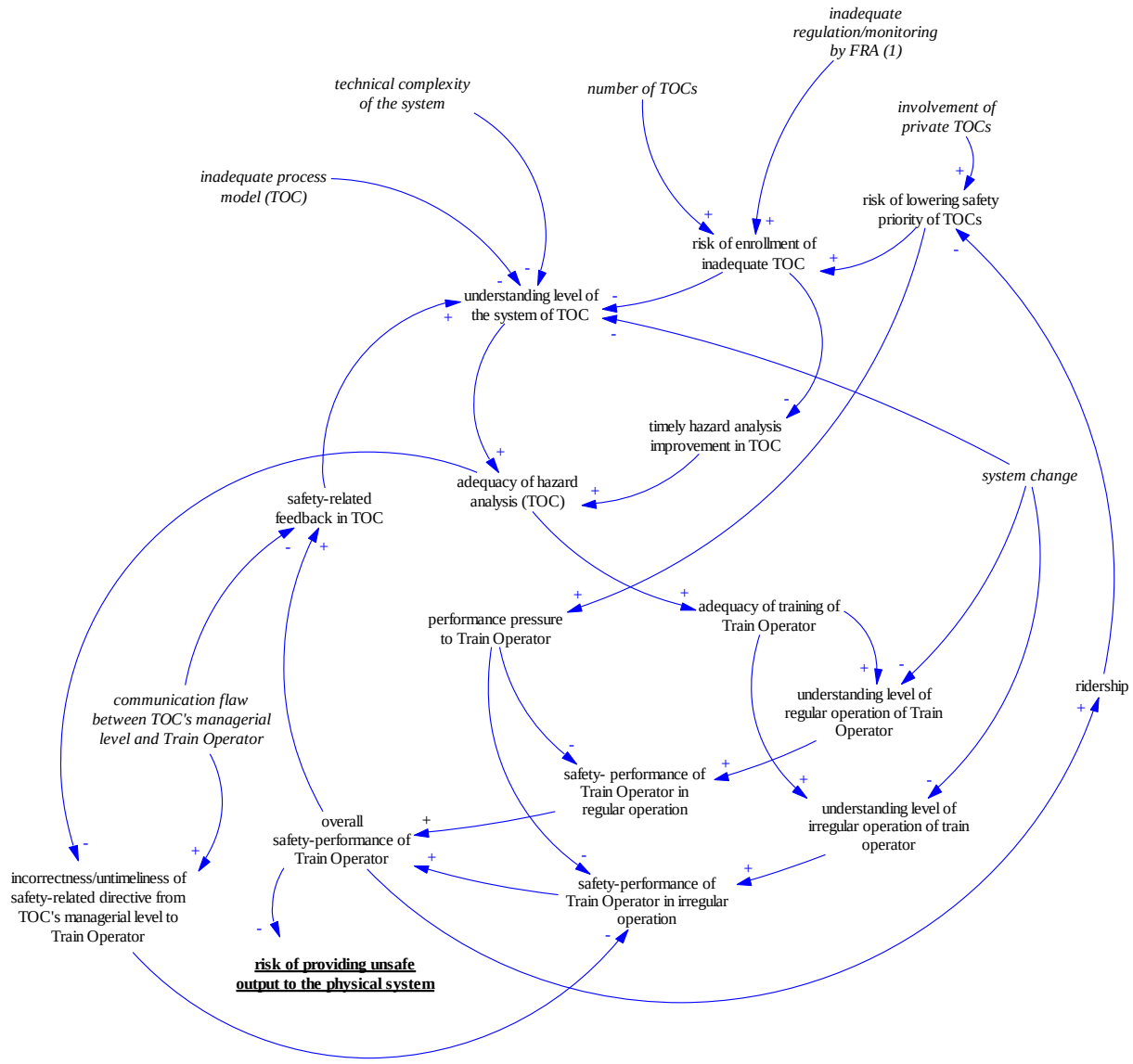

Figure 5-9 Causal model about coordination in train operation (TOC and *Train Operator*)

Variables represented by Italic letters means system input that could increase safety risks of the system, which are discussed in Section 5.2.1. There may be a large number of additional variables that could be connected to some of the variables in the model, but they are not considered in this analysis to narrow down the focus.

At the top right of the model, "risk of enrollment of inadequate *TOC*" is driven by involvement of multiple TOCs, FRA's inadequate regulation or monitoring, or private TOCs' inadequate safety priority. This leads to inadequate hazard analysis or its slow improvement. Technical complexity and inadequate process model of TOC could exacerbate this situation. This hazard analysis of TOC is related to the

"adequacy of training of *Train Operator*" and their understanding and safety-performance in train operation. Train operation is comprised of regular operation and irregular operation in this model. "System change," which is described on the right hand side of the model, would lower the understanding of the system of both TOC (i.e., managerial level) and *Train Operator*. "Overall safety-performance" of *Train Operator* is linked to the risk of providing unsafe output to the physical system. The overall performance is also related to ridership and operational revenues, which could affect safety priority of TOCs, which is presumed to come out especially in Alternative 3. This priority could affect safety-performance of *Train Operator* if management level of TOC(s) imposes excessive performance pressure about punctuality on *Train Operator*. Additionally, the overall performance is related to "safety-related feedback in TOC" from *Train Operator* to TOC's managerial level. This feedback is important to improve hazard analysis continuously, but it could be impaired due to inadequate communication between *Train Operator* and TOC's managerial level. This inadequate communication could affect the quality of safety-related directives from TOC's managerial level to *Train Operator*, especially in irregular operations.

There are mainly two types of feedback loops regarding the overall safety-performance in the model: "ridership" and "safety-related feedback about the operation," as shown with bold arrows in Figure 5-10 and 5-11. The first loop about ridership has an even number of negative arrows denoted by "-" for any routes and, therefore, can be regarded as a positive feedback loop,[38] in which a change of variable reinforces the change of the same variable in the same direction. This implies the importance of developing economically sustainable industry, developing industrial structure or rules in which impact of ridership on safety management is low, or developing a way of operation resilient to change of the economic condition, by, for example, enhancing cost efficiency of the operation. The other feedback is also a positive feedback, bolstering understanding of the system and safety-performance by safety-related feedback about operation. As can be seen in the model, there are several negative inputs that weaken the reinforcement, such as "system change" and "inadequate process model of TOC." To overcome these risks, continuous system improvement activities are crucial.

[38] The basics of SD, including the definition of "positive feedback loop," are explained in Appendix A.

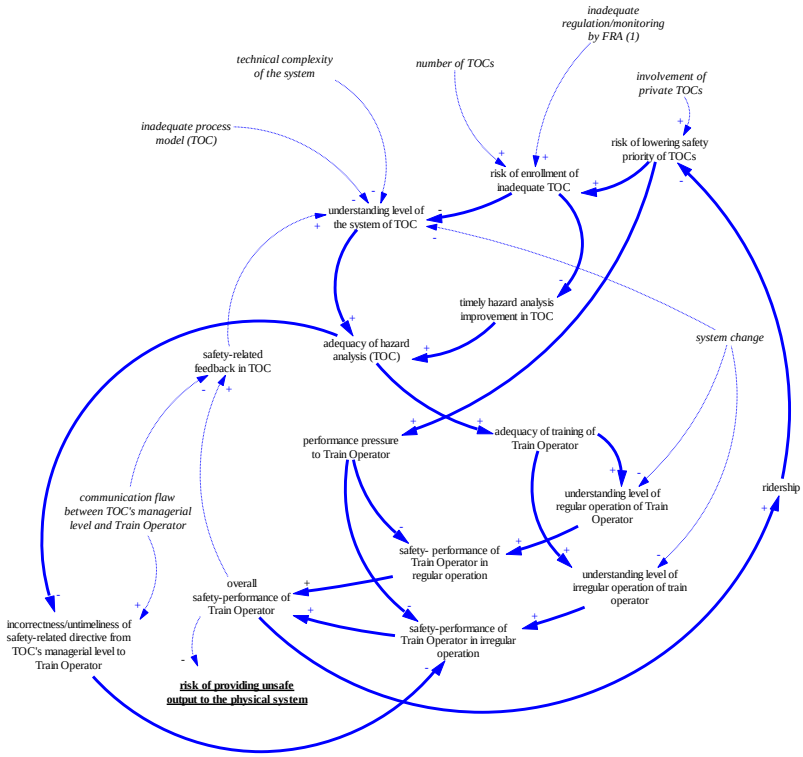

Figure 5-10 Positive feedback loop (ridership)

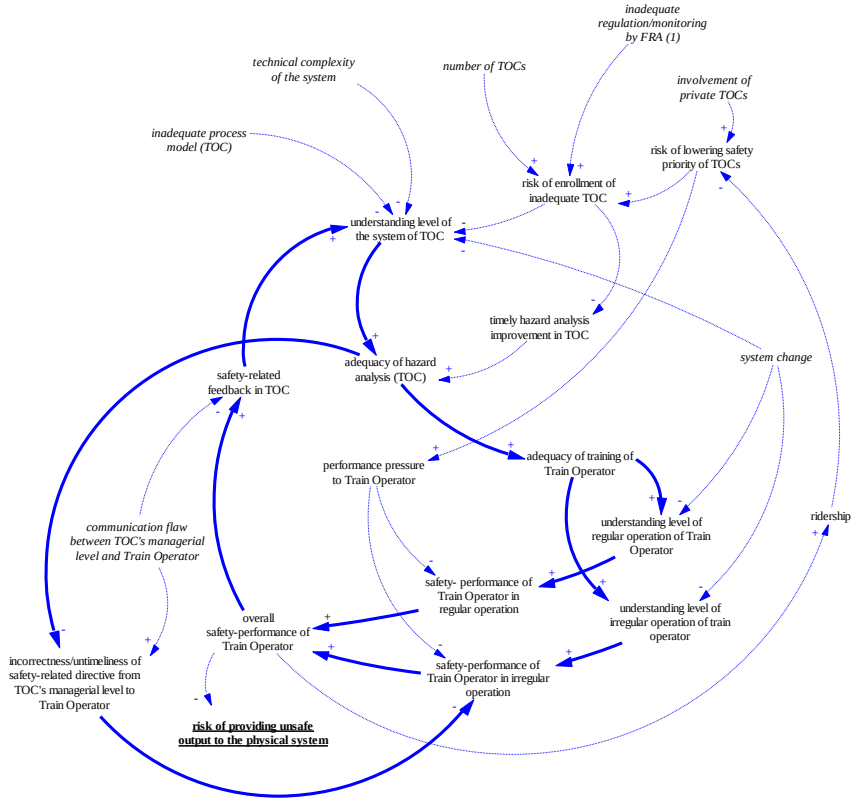

Figure 5-11 Positive feedback loop (safety-related feedback)

As a next step, a system dynamics model representing the interaction between IM and *Dispatcher* is developed in Figure 5-12.

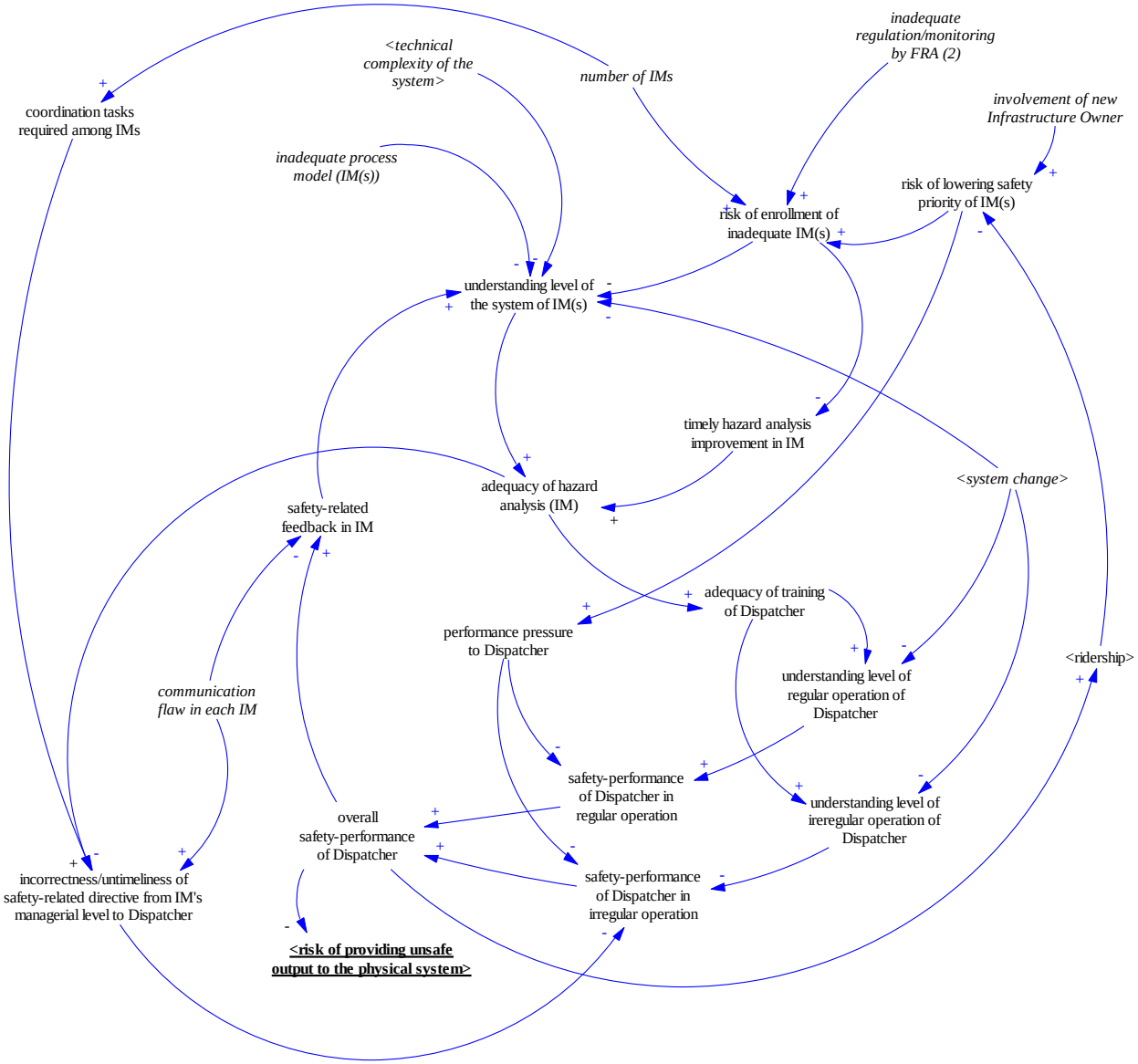

Figure 5-12 Causal model about coordination in train operation (IM and *Dispatcher*)

The causal structure of this model is same as that of the model in Figure 5-9. The variables described in pointy brackets "< >" represent the common ones in both models. One of the largest differences between them is that this model has "coordination tasks required among IMs" as an additional driver of "incorrectness/untimeliness of safety-related directive from IMs' management level to *Dispatcher*."

Additionally, “risk of lowering safety-priority” at the top left of the model is discussed in the context of involvement of new IM, which can be seen in Alternative 2.

The two models (Figure 5-9 and 5-12) are combined with a variable “risk of lowering adequacy of safety requirement or operational communication between IM(s) and TOC(s),” which could be affected by vertical structure of the industry, coordination level among IM(s), and the adequacies of their hazard analyses, as shown in Figure 5-13. Thus, causal factors representing multiple risks, specifically risk 23, 24, 36, 37, 39, and 42 in Section 5.2.1, are incorporated in this model, and various indirect causal relations can be analyzed from this model; for example, the influence of “inadequate process model of IM” on “safety-related feedback in TOC,” which seems unapparent in STPA, can be analyzed with this approach.

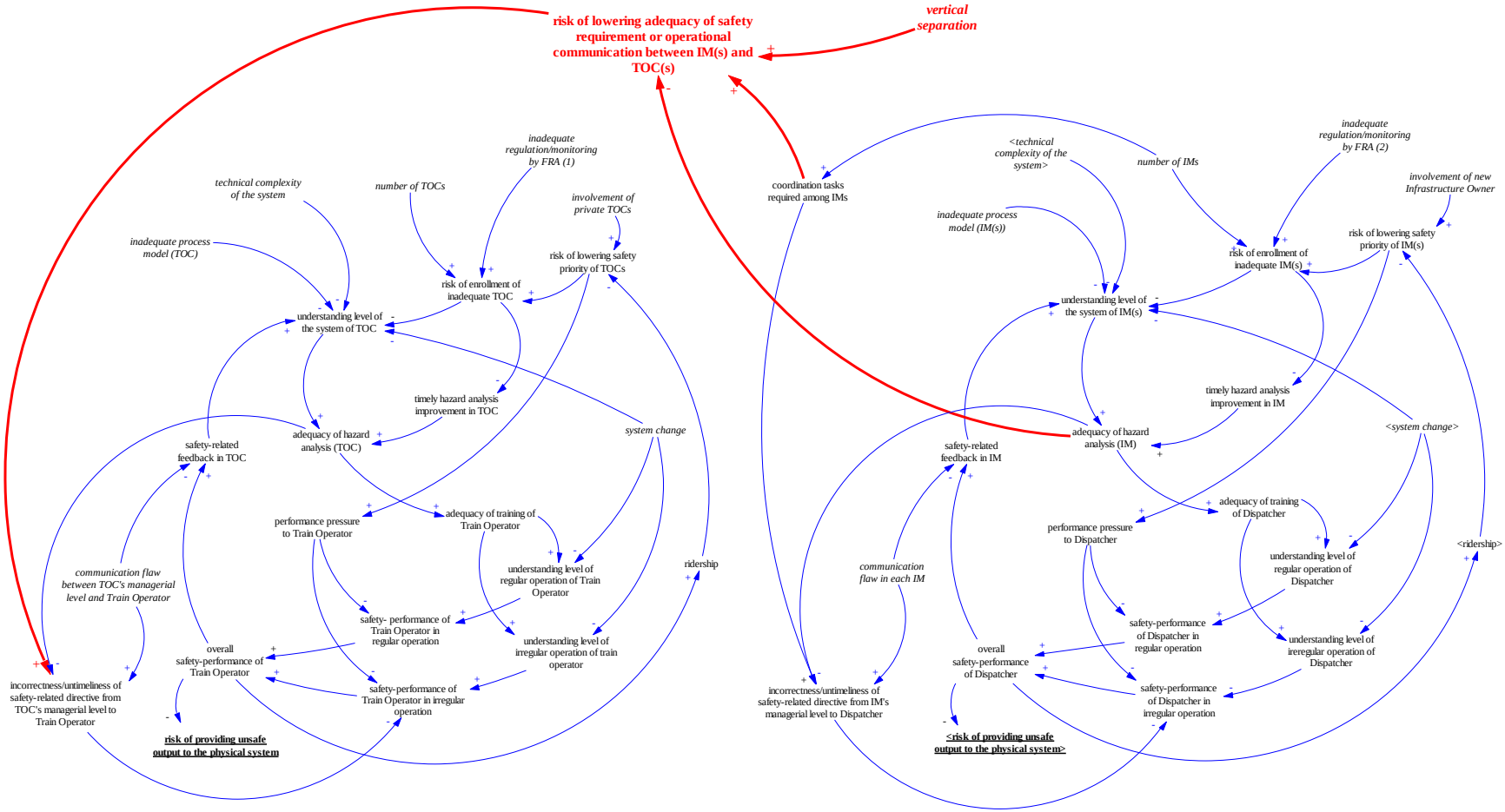

Figure 5-13 Causal model about coordination in train operation (combined model)

5.3.2 Market Competition and Safety

This analysis focuses on a causal relation among maintenance management, system evolution, and market competition. As discussed in Risk 27, 44, and 47, risks in maintenance management have complex causal factors. Operational revenue is one of the factors that could affect maintenance management; e.g., in the case of *Hatfield Derailment*, maintenance management, which generally involves many contractors and subcontractors, became a target of cost reduction of Railtrack. Also, lessons learned from maintenance are keys to system improvement, which is essential to achieve persistent safety of the system.

The model in this section is based on the structure in Alternative 3, incorporating two TOCs and clarifying their mutual interactions. As mentioned in Section 4.3.2, this research assumes that the type of market competitive interaction in the NEC HSR is "Intra-modal competition for the market" defined in Table 1-2. In addition to this focus, this analysis also aims to acquire an insight about the impact of having "Intra-modal side-by-side competition" defined in Table 1-2 between new and upgraded HSR operations on the NEC, which is not analyzed in the STPA of this research.

The first model focuses on one TOC, describing causal relations among ridership, maintenance quality, and system evolution, as shown in Figure 5-14.

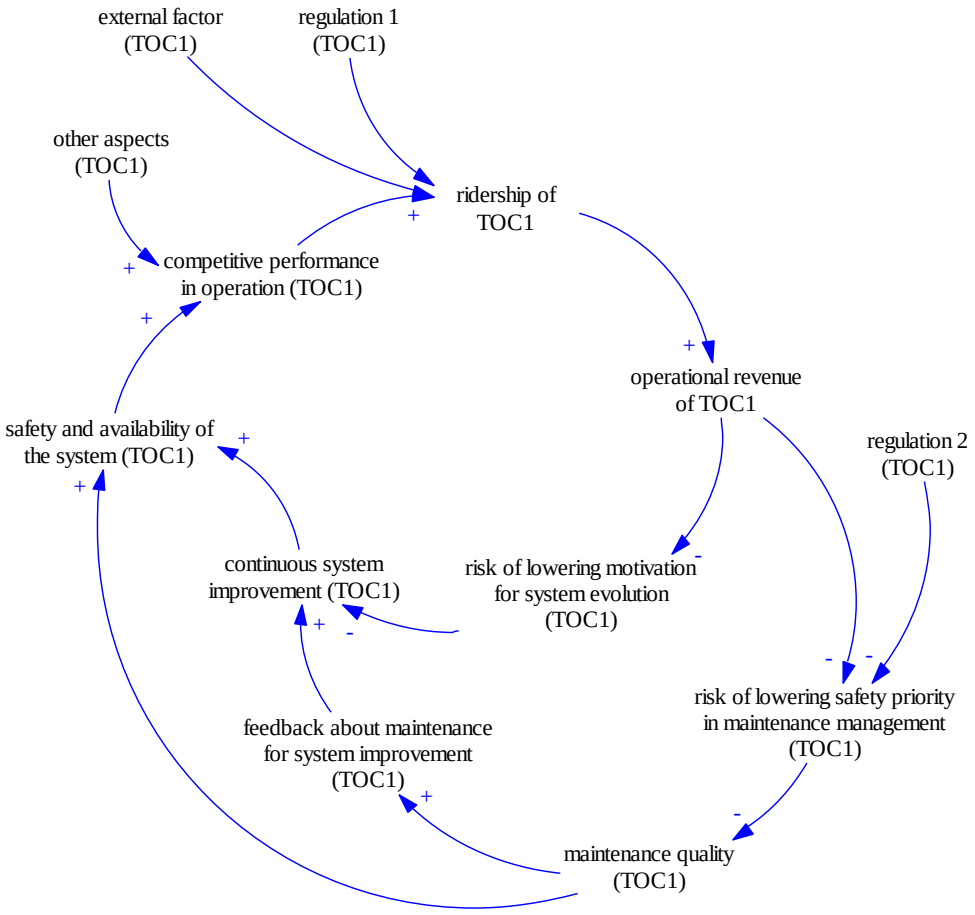

Figure 5-14 Causal model about market competition

Decrease in "ridership" and "operational revenue" could boost two types of risks in this model: "risk of lowering motivation for system evolution" and "risk of lowering safety priority in maintenance management." Low safety priority that is not adequately regulated could lead to inadequate maintenance management and to an unsafe state of rolling stock. Additionally, poor maintenance management would lose an opportunity for system improvement, lacking safety-related feedback from contractors. With "risk of lowering motivation for system evolution," this situation could lead to a failure in the improvement of the system's safety or *availability*.[39] Thus, losing competitiveness to other TOCs would result in lowering ridership.

[39] Availability is one of the essential system characteristics to represent the rolling stock's performance, which is mainly used in Europe. It is defined as a ration of up time of a system to the summation of uptime and downtime [59].

This model can be defined as a positive feedback loop. From a safety perspective, it is important that TOCs have a continuously increasing ridership. Even if it decreases, there is a necessity for actions to disconnect the positive feedback loop to avoid accumulating the two risks. For example, regulation that could excessively affect ridership should be mitigated, and "risk of lowering safety priority in maintenance management" of TOC should be appropriately monitored by a regulator. Furthermore, "other aspects" that could enhance competitive performance of the TOC should be applied. The examples of "other aspects" could be a quality of service, frequency of operation, operational speed, or punctuality. Also, "external factors" connected to ridership such as economic condition of the TOC or surrounding societies, population growth, and business policies of other transportation modes could have a strong influence on ridership. Uncertainties such as fluctuation of ridership expected at the initial stage of commercial operation could be regarded as one of the external factors, as well.

As a next step, this model is combined with another TOC's model with arrows that represent market interaction. The combined model is shown in Figure 5-15. The models of two different TOCs are connected with two negative arrows that represent market competition; an increase in ridership of TOC1 would decrease that of TOC2, and vice versa. To the contrary, there is a symbiotic relation in which one's ridership increase could contribute to the other's ridership increase by enhancing NEC HSR's competency to other transportation modes and thereby acquiring new customers. When competitive relation is stronger than symbiotic relation, this market competition could affect the safety of a TOC losing market share.

Considering uncertainties of demand or the new system's performance at the initial phase of commercial operation, this model gives an insight in which market competition should not be applied at first to avoid a situation in which one of the TOCs has an unsafe feedback loop, and a timing of entry of following TOC(s) is crucial for this purpose. Specifically, after TOC1 develops a resilient positive feedback loop, and constructs a foundation of HSR's market competitiveness to Air and Auto industries, and when negative intensive "external factors" cannot be seen or expected for a *certain* amount of time, TOC2 should enter the market. And most importantly, all of the involved TOCs in the market must establish a resilient operation continuously disconnecting unsafe positive feedback loops, thereby having a healthy competition with other TOCs.

These perspectives can be applied to the case in which NEC HSR adopts both updating the current infrastructure and constructing a new track; the two parallel lines --that might be parallel partially-- could be a competitive market if they are operated by different TOCs.

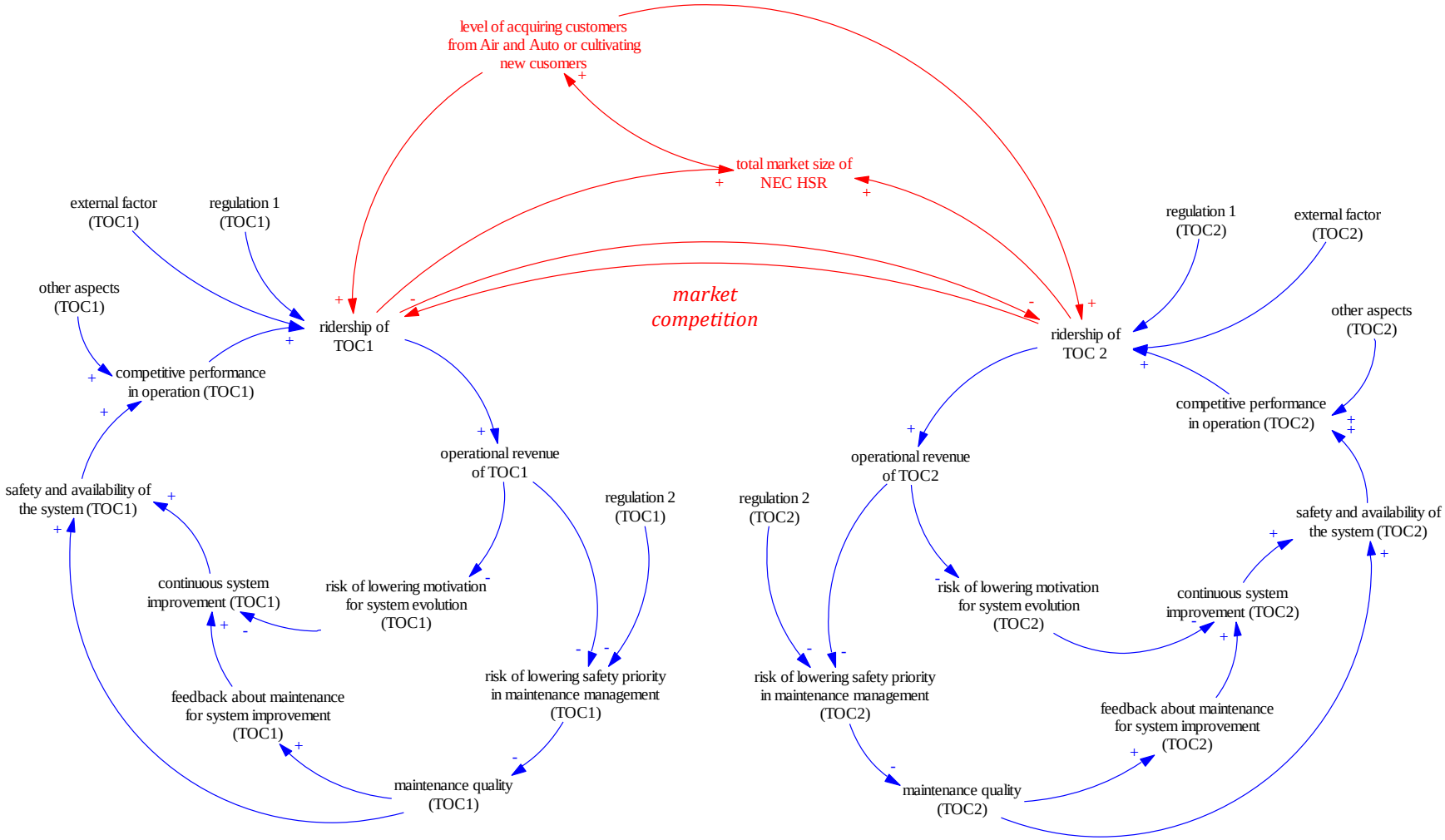

Figure 5-15 Causal model about market competition

5.3.3 System Dynamics and Risk Management

As these two examples have demonstrated, SD models help understanding complex indirect causal factors visually, integrating indirect causal factors that STPA does not necessarily address. Also, difference of institutional structures can be represented as additional variables that could strengthen or weaken positive feedback of the models. One of the potential usages of this SD in risk management is the identification of leading indicators representing that the safety level of the system is changing; e.g., monitoring dynamic changes of key variables in positive feedback loops that involves risk-related variables could provide useful information to capture emergence of system hazards timely [11][67]. Thus, SD models could be applied to dynamic risk management as well as detailed causal analysis.

CHAPTER 6. FINDINGS, CONCLUSION, AND RECOMMENDATIONS

Findings, conclusion, and recommendations are described in this chapter. The recommendations are organized for project planers and implementers of the NEC HSR based on the weaknesses that this research identified in its safety risk management.

6.1 Findings

The findings in this research are as follows.

- This thesis research has shown usefulness of STAMP-based analyses (CAST and STPA) in many domains. This thesis proved the value of this new systems-theoretic approach in HSR applications.

- The following is the findings from CAST of *Wenzhou Train Crash* and *Hatfield Derailment*.
  - In developing a new HSR project or changing the current organizational structure, the institutional structure must be carefully designed from system safety perspectives: different structures may lead to different safety performance, and therefore, different structures require different safety constraints.
  - Corporate boundaries could provide communication and coordination risks; the UK's accident case represents a risk of horizontally-fragmented contractor management, and the Chinese case represents a risk of vertically-multilayered system development. Risks on these boundaries must be identified at the institutional design process, and managed with carefully designed safety constraints.
  - One of the key ideas in the STAMP theory is continuous *system evolution*; adequate *feedback* from *controlled process* enables the *controller* to have an adequate *process model* about the dynamic system, leading to the adequate bridging between *system development* and *system operations*. As the Chinese accident case shows, a structural mechanism for *system evolution* has to be incorporated into the institutional structure.
  - As the Chinese case shows, even if most of the components are introduced from service-proven systems outside, integrating the components as a system must be considered as challenging as developing the system from scratch; the introduced components would have new safety-related interfaces with endogenous domains such as a domestically developed physical system[40],

[40] E.g., in the Chinese case, the control system is developed by CRSCD, a domestic company.

corporate cultures, nationality character, regulations, etc. Safety risks related to these interfaces must be adequately identified.

- The following is the findings from the case study of the NEC HSR with the proposed methodology.
  - The proposed methodology models the NEC HSR with a hierarchical control structure, which enabled us to
    - expand risk analysis domain from the physical system, which is a main focus of typical conventional risk analyses, to the institutional level,
    - clarify safety responsibilities of all safety-related organizations involved in the NEC HSR, including their interactions,
    - incorporate system-based lessons from past accidents,
    - compare different institutional alternatives for the NEC HSR in a consistent way,
    - identify required safety constraints and system requirements comprehensively,
    - and identify causes of hazards comprehensively.
  - The STAMP-based approach has shown that different institutional alternatives of the NEC HSR could produce different safety risks. Specifically, this research took into account three specific institutional alternatives, and identified 44 risks that are commonly true for the three alternatives and 14 risks that are true for one or two specific alternatives among the three.
  - These risks must be managed with appropriate regulations. Therefore, safety-related regulations for the NEC HSR must be designed from an institutional-structure-neutral standpoint. For this "neutral", all of the possible institutional structures must be taken into consideration to incorporate safety constraints required for them into the regulations. Based on this perspective, this research identified several weaknesses of some of the current (or currently developed) regulations such as SSP.
  - This research has discussed potential usage of System Dynamics in risk management. Specifically, this research analyzed two different safety issues with SD, and demonstrated that SD models could help understanding complex causal relations visually and could be used to identify leading indicators representing that the safety level of the system is changing.

6.2 Conclusion

The conclusion of this research is as follows.

- It is widely recognized that a physical system is regarded as a fundamental safety-critical part of the total system. In complex sociotechnical systems such as the NEC HSR, a holistic approach focusing on not only physical systems but also institutional levels is essential for risk analysis.
- The risk analysis must incorporate lessons adequately from past accidents as system-based safety constraints, not just as a countermeasure for so-called "root cause." This research has developed a STAMP-based risk analysis methodology that can meet these requirements. The case study of the HSR project in the NEC has shown the usage of this methodology, identifying 58 NEC-specific risks. This research strongly recommends that the project planers of the NEC HSR adopt the proposed methodology as a "safety-guided institutional design" tool. Specific recommendations for the NEC HSR are described in Section 6.3.1.
- Safety-related regulations should be developed from a neutral standpoint about the institutional structure; any possible institutional alternative should be taken into account in their design process. The STAMP-based approach that this research proposes enables this by clarifying the structural difference among these alternatives and safety constraints required for each alternative. Specifically, this research discussed *Buy America* (PRIIA's *Buy America* provision *49 USC §24405(a)* and *Buy American Act 41 USC §8301-§8305*), Certification Procedure (*49 CFR 238.111*), and the *System Safety Program* (SSP, *49 CFR 270 Part 270 proposed rule*) from the neutral standpoint. Several weaknesses of SSP are identified.
- Although this research analyzed three specific institutional alternatives of the NEC HSR, this research does not suggest one specific institutional structure as an optimal one among the three; in reality, system complexities at an institutional level could be intentionally introduced for non-safety purposes such as an economic benefit. Having more structural complexities does not necessarily mean that the complex institutional structure is less safe than simple ones: importantly, a safety level of systems depends on whether safety constraints are adequately designed and implemented according to the system structures. Therefore, what risks these complexities could produce and what safety constraints should be designed to manage these risks are rather important perspectives. From this perspective, we propose that the outcomes of this thesis research can be valuable for the actual institutional design process.
- As this research has shown, the STAMP-based approach can provide new views and valuable supports for designing regulations and institutional structures. However, STAMP is a new approach,

and the number of research applying STAMP-based analysis to institutional levels is still limited. Especially in the rail sector, there are only a few cases that apply STAMP to safety analysis or design. The STAMP-based approach and proposed methodology in this thesis need to be further evolved by continuous studies and applications in practice.

6.3 Recommendations

Based on the performed analyses, recommendations for project planers and implementers of the NEC HSR are organized in Section 6.3.1. Future work of this thesis research is also described in Section 6.3.2.

6.3.1 NEC HSR Recommendations

- **Recognize that HSR systems are not yet service proven in the US:**
  System integration requires as much risk awareness as system development from scratch even though some of the components in the system are "service-proven" for other markets.

- **Focus on both the physical and institutional levels of the project and implement a holistic system safety approach in the safety management:**
  From a system safety perspective, it is essential to implement a holistic approach in safety management. In the NEC HSR, its total system has to be defined as a domain that comprehensively includes any entities that have safety responsibilities and interactions with others, as this research does; e.g., regulators, maintenance companies, suppliers, R&D companies, and manufacturing companies should be included in the total system as system components.

- **Leverage this methodology, incorporate diverse perspectives, and design safety constraints:**
  Project planners that are responsible for designing safety-related regulations or the institutional structure for the NEC HSR should use the proposed methodology. This research has performed risk analysis on the NEC HSR as a case study using this methodology, but the entire processes need to be further refined from more varied and pragmatic perspectives. For example, this research only analyzed two accidents with CAST, but there might be other beneficial lessons provided by conducting additional accident analyses. Also, hazard analysis could be performed more rigorously if safety actions in the safety control structures are defined in more specific manners; e.g., control actions provided by FRA to *System Integrator* could each be a detailed certification process, instead of simply "certify developed technology." As next steps of the tasks discussed in this research, the project planners should analyze and prioritize risks, design safety constraints based on the evaluation, and design the way to monitor them over time based on SD-based analysis, cooperatively working with experts from diverse organizations involved in the project, such as regulators, suppliers, TOCs, IMs, and maintenance companies. This thesis does not provide or suggest a specific risk evaluation method or a definition of acceptable/unacceptable risk, but importantly, these decisions must be implemented in a consistent way, which is not adequately established in the US rail sector.

- **Design regulations from an institutional-structure-neutral, system-based standpoint**
  Safety-related regulations should be developed by taking into consideration potential alternatives for the institutional structure. Recommendations for regulations that are applied to the NEC HSR are organized as follows:

  - **Establish an appropriate waiver rule of Buy America**
    Buy America could provide enormous safety concerns in the initial system development process and the following system evolution process, causing many inefficiencies and uncertainties. It is desirable that an exception rule that enables HSR developments to manage potential safety risks provided by *Buy America* is appropriately developed. (Discussed in detail in Risk 1 in Section 5.2.1)

  - **Establish a new certification procedure compatible with global supply chains**
    Regulations about certification procedure of the physical systems such as *49 CFR 238.111* need to be revised: it has to be compatible with globally spread, new supply chains, incorporating appropriate safety-oriented multiphase verification processes. (Discussed in detail in Risk 3 in Section 5.2.1)

  - **Refine SSP and establish an integrative system safety approach**
    System safety approaches are essential to manage safety in complex sociotechnical systems, especially when they drastically change their technologies, industrial structures, and rules as the NEC HSR is doing. The currently proposed rule, SSP, is a managerial program mainly focusing on train operation and management, from each railway company's standpoint in the industry, not from a holistic industrial viewpoint. Therefore, in light of the holistic system safety perspective, SSP could have weaknesses in the following points. (Discussed in detail in Section 5.2.2)

    1) SSP does not deal with all of the safety interactions in the total system; e.g., safety-related activities in the system development domain and those among a regulator and regulated organizations are not SSP's focuses. Therefore, to implement a holistic system safety approach, it is necessary to establish additional SSP to cover those domains.
    2) Risk analysis in SSP might not appropriately evaluate risks related to issues in the physical system due to lack of the adequate understanding of it.
    3) Coordination risk might not be adequately handled; specifically, emergency management, technology analysis, and hazard analysis parts state that railroads should communicate with

other entities related to any part of SSP, but SSP does not ensure adequate coordination of this communication.

4) Analytic tools for risk identification and evaluation are not specified, which could lead to inconsistent quality of risk management in the industry.
5) Perspectives of system evolution based on lessons in maintenance and operation are not adequately incorporated.

With respect to 1), although there is no regulation requiring system developers to implement a system safety approach, CHSRA is requiring suppliers to implement a system safety approach called *Safety and Security Management Plan* (SSMP) that are compatible with SSP in system development processes, according to the RFP for the California HSR system [63]. This research recommends that FRA establishes a regulation to require any suppliers for HSR systems to implement a system safety approach that is harmonized with SSP to ensure their consistencies throughout the total system. Furthermore, FRA needs to overarch this additional system safety approach and SSPs implemented by various organizations in the total system on the same basis over time, and needs to comprehensively manage risks created at the institutional level that could not be identified by any of the individual system safety approach. Specifically, the following is requirements for this overarching activity.

- Need to define a procedure for harmonizing all of the individual system safety approach.
- Need to have consistent criteria about risk evaluation and risk acceptance.
- Need to manage weaknesses of underlying system safety activities such as above-mentioned SSP's weaknesses 2) – 5).
- Need to incorporate flexibility to adapt all system safety activities to any future system changes (e.g., privatization, open access, technology innovation)

6.3.2 Future Work

This thesis is the first research case to apply the STAMP-based approach to risk analysis of railway projects. Also, the system-based "safety-guided institutional design" introduced in this thesis is a new approach in safety management. These approaches need be further discussed and advanced in the future research. Additionally, the proposed methodology should be applied to different projects of other transportation modes, and its applicability, limitation, and potential of further improvement need to be discussed. In terms of the HSR in the NEC HSR, *System Safety Program* (49 CFR part 270), which is still in the development process, should be further analyzed from STAMP-based perspectives. The integrative system safety management proposed in Section 6.3.1 and its regulatory structure for the NEC HSR could be interesting future research focuses.

The NEC is one of the world-leading corridors in terms of its economic and cultural influence. Doubtless, the NEC HSR will be a symbolic infrastructure in the US, as HSRs in other countries are. Safety is one of the crucial attributes for this project's success, yet its management is complex and challenging, as this research has shown. We ardently hope that this thesis illuminates the right future direction for this project and other projects to come. We also thank you, the reader of this thesis, for your engagement, and hopefully this thesis will interest you in the future development of the NEC, safe HSR, and similar developments around the world.

BIBLIOGRAPHY

[1] UIC, “High Speed Lines in the world,” 2013.

[2] State Administration of Work Safety, “Official Accident Report of Wenzhou Derailment (Chinese),” 2011. [Online]. Available: http://www.chinasafety.gov.cn/newpage/Contents/Channel_5498/2011/1228/160577/content_160577.htm?COLLCC=485100271&.

[3] BBC, “Spain train driver ‘on phone’ at time of deadly crash,” 2013. [Online]. Available: http://www.bbc.com/news/world-europe-23507348.

[4] A. Dong, “Application of CAST and STPA to Railroad Safety in China,” 2012.

[5] D. Suo, “A System Theoretic Analysis of the ‘ 7 . 23 ’ Yong-Tai-Wen Railway Accident,” 2012.

[6] UIC, “High speed rail -faxt track to sustainable mobility-,” 2012.

[7] CNN, “Why high-speed rail is safe , smart,” 26-Jul-2013. [Online]. Available: http://www.cnn.com/2013/07/26/opinion/freemark-high-speed-trains/index.html.

[8] OECD, “Structural Reform in the Rail Industry,” no. February, 2005.

[9] F. Kurosaki, “An Analysis of Vertical Separation of Railways,” 2008.

[10] N. G. Leveson, “A new accident model for engineering safer systems,” *Saf. Sci.*, vol. 42, no. 4, pp. 237–270, Apr. 2004.

[11] N. G. Leveson, *Engineering a Safer World*. MIT Press, 2011.

[12] N. G. Leveson, *SafeWare : System Safety and Computers*. Addison-Wesley Professional, 1995.

[13] UIC, “General Definition of Highspeed.” [Online]. Available: http://www.uic.org/spip.php?article971.

[14] Reuters, “U.S. yanks high-speed rail funds for Wisconsin and Ohio,” 2010. [Online]. Available: http://www.reuters.com/article/2010/12/09/us-usa-infrastructure-highspeedrail-idUSTRE6B860B20101209.

[15] Railway Gazette, “Governor halts Orlando - Tampa high speed rail project,” 2011. [Online]. Available: http://www.railwaygazette.com/news/single-view/view/orlando-tampa-hsr-project-halted.html.

[16] California High-Speed Rail Authority, “California High-Speed Rail Authority (Website).” [Online]. Available: http://www.hsr.ca.gov/.

[17] FRA (NEC FUTURE), “Scoping Package,” no. June, 2012.

[18] FRA (NEC FUTURE), “Preliminary Alternatives Report,” 2013.

[19] APTA, “APTA High-Speed Train Survey,” 2012.

[20] Federal Railroad Administration, “Vision for High-speed Rail in America (Strategic Plan),” 2009.

[21] GAO, “RAIL SAFETY -Preliminary Observations on Federal Rail Safety Oversight and Positive Train Control Implementation-,” 2013.

[22] FRA, “High-speed Passenger Rail Safety Strategy,” 2009.

[23] FRA, “Advisory Committee Recommends Passenger Rail Crashworthiness Standards to Accommodate HSR,” 2013. [Online]. Available: http://www.fra.dot.gov/eLib/details/L04638#.

[24] United States Government Accountability Office (GAO), “Positive Train Control: Additional Authorities Could Benefit Implementation,” 2013.

[25] FRA, *49 CFR part 270 System Safety Program*, vol. 77, no. 174. 2012.

[26] FAA, “Safety Management System.” [Online]. Available: https://www.faa.gov/about/initiatives/sms/.

[27] OECD, “Railways : Structure , Regulation and Competition Policy,” 1997.

[28] World Bank, “Transport for development: An Update of the World Bank’s Transport Sector Priorities for the Period 2007-2015,” 2006.

[29] OECD, “Working Party No.2 on Competition and Regulation: Structural Reform in the Rail Industry,” 2005.

[30] World Bank, “Railway reform : vertical integration and separation,” 2006.

[31] J. Hearsch, “Structural Change in Railway Organisations-An Assessment of Recent Experience of Privatisation, Vertical and Horizontal Separation and Intra-Modal Competition,” *Rep. to South African Railw.*, 2001.

[32] EU Business, “Fourth Railway Package,” 2013. [Online]. Available: http://www.eubusiness.com/topics/transport/rail-package-4/?searchterm=None.

[33] International Railway Journal, “Germany rewrites the Fourth Railway Package,” 2013. [Online]. Available: http://www.railjournal.com/index.php/blogs/tony-berkeley/germany-rewrites-the-fourth-railway-package.html?channel.

[34] CALPIRG, “High-Speed Rail : Public , Private or Both ?,” 2011.

[35] A. W. Evans, “Rail safety and rail privatisation in Britain.,” *Accid. Anal. Prev.*, vol. 39, no. 3, pp. 510–23, May 2007.

[36] A. W. Evans, “Rail safety and rail privatisation in Japan.,” *Accid. Anal. Prev.*, vol. 42, no. 4, pp. 1296–301, Jul. 2010.

[37] OECD, “Recent Developments in Rail Transportation Services,” 2013.

[38] DOD, “Department of Defence Standard Practice -System Safety- (MIL-STD-882E),” 2012.

[39] IEC, “IEC 60300 Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems.” 1995.

[40] ISO, “ISO 31000 Risk management - Principles and guidelines.” 2009.

[41] ISO/IEC, “ISO/IEC 31010 Risk Management – Risk Assessment Techniques,” vol. 2009. 2009.

[42] R. Koivisto, N. Wessberg, A. Eerola, T. Ahlqvist, S. Kivisaari, J. Myllyoja, and M. Halonen, “Integrating future-oriented technology analysis and risk assessment methodologies,” *Technol. Forecast. Soc. Change*, vol. 76, no. 9, pp. 1163–1176, Nov. 2009.

[43] J. Tixier, G. Dusserre, O. Salvi, and D. Gaston, “Review of 62 risk analysis methodologies of industrial plants,” *J. Loss Prev. Process Ind.*, vol. 15, no. 4, pp. 291–303, Jul. 2002.

[44] P. Patel, “Review of Available System Safety Assessment Tools and Techniques-Integrated Approaches for Accident Prevention in Process Industry,” vol. 2, no. 4, pp. 251–258, 2013.

[45] IEC, “IEC 61025 Fault Tree Analysis (FTA).” 2006.

[46] “ARP4761 Guidelines and Methos for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.” 1996.

[47] NASA, “Fault Tree Analysis with Aerospace Applications,” 2002.

[48] DOD, “Military Handbook: Electronic Reliability Design Handbook,” 1998.

[49] IEC, “IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).” 2006.

[50] G. Apostolakis, “The concept of probability in safety assessments of technological systems.,” *Science*, vol. 250, no. 4986, pp. 1359–64, Dec. 1990.

[51] NASA, “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,” 2011.

[52] N. Dulac, “A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems,” 2007.

[53] J. Samadi, “l ’ École nationale supérieure des mines de Paris Development of a Systemic Risk Management Approach for CO 2 Capture , Transport and Storage Projects,” 2012.

[54] J. Thomas, “Extending and Automating STPA for Requirements Generation and Analysis,” 2013.

[55] H. W. Heinrich, *Industrial accident prevention; a scientific approach*. McGraw-Hill book company, 1931.

[56] E. Hollnagel, *Barriers and Accident Prevention*. Ashgate publishing company, 2004.

[57] J. Reason, *Human Error*. Cambridge University Press, 1990.

[58] J. Reason, *Human Errors: Models and Management*. BMJ Group, 2000.

[59] IEC, "IEC62278 (EN50126) Railway Applications -- Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)." International Electrotechnical Commission, 2002.

[60] California High-Speed Rail Authority, "Request For Proposal: Reliability , Availability and Maintainability," 2012.

[61] ERA, "Safety Management System (ERA)." [Online]. Available: http://www.era.europa.eu/tools/sms/Pages/default.aspx.

[62] European Union, "COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009," *Off. J. Eur. Union*, vol. 3, p. P.8, 2013.

[63] California High-Speed Rail Authority, "Safety and Security Management Plan." 2013.

[64] N. G. Leveson, "An STPA Primer (Versioin 1)," 2013.

[65] T. Tao and N. Ru, "A Systematic Accident Analysis Approach for Chinese Railway," 2013.

[66] J. Samadi and M. Paristech, "Prepared & presented by: Jaleh SAMADI MINES ParisTech, CRC," 2013.

[67] N. G. Leveson, N. Dulac, B. Barrett, J. Carroll, and J. Cutcher-gershenfeld, "Risk Analysis of NASA Independent Technical Authority," 2005.

[68] N. Dulac, B. Owens, and N. G. Leveson, "Demonstration of a New Dynamic Approach to Risk Analysis for NASA ' s Constellation Program," 2007.

[69] J. D. Sterman, *Business Dynamics*. New York: McGraw-Hill, 2000.

[70] T. P. Dunn, "The Geography of Strategy: An Exploration of Alternative Frameworks for Transportation Infrastructure Strategy Development," 2010.

[71] D. R. Miller, R. and Lessard, *Evolving strategy: risk management and shaping of mega-projects in Decision-Making On Mega-Projects: Cost-Benefit Analysis, Planning and Innovation.* UK: Edward Elgar, 2008.

[72] J. Santos-Reyes and a N. Beard, "A Systemic Analysis of the Paddington Railway Accident," *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit*, vol. 220, no. 2, pp. 121–151, Jan. 2006.

[73] R. Lawton and N. J. Ward, “A systems analysis of the Ladbroke Grove rail crash.,” *Accid. Anal. Prev.*, vol. 37, no. 2, pp. 235–44, Mar. 2005.

[74] J. Santos-Reyes, a N. Beard, and R. a Smith, “A systemic analysis of railway accidents,” *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit*, vol. 219, no. 2, pp. 47–65, Jan. 2005.

[75] Office of Railway Regulation, “Train Derailment at Hatfield: A Final Report byt hte Independent Investigation Board,” 2006.

[76] C. Wolmar, *Broken Rails*. London: Aurum Press, 2001.

[77] T. Song, D. Zhong, and H. Zhong, “A STAMP Analysis on the China-Yongwen Railway STAMP Model of Accidents,” pp. 376–387, 2012.

[78] H. Qiao, “Wenzhou crash report blames design flaws and poor management,” *Int. Railw. J.*, vol. January 30, pp. 8–10, 2013.

[79] P. Booth, D. Shouts, D. Comment, A. Davidson, J. Cassidy, A. Borowitz, R. Brody, and T. N. Yorker, “How a High-Speed Rail Disaster Exposed China’s Corruption,” *New Yorker*, vol. 10/29, pp. 1–15, 2012.

[80] Boeing Co., “Boeing Press Release (787-related).” [Online]. Available: http://boeing.mediaroom.com/news-releases-statements?category=797.

[81] The Seattle Times, “Boeing celebrates 787 delivery as program’s costs top $32 billion,” 24-Sep-2011. [Online]. Available: http://seattletimes.com/html/businesstechnology/2016310102_boeing25.html.

[82] The Seattle Times, “Boeing’s Fastener Problems,” 20-Nov-2008. [Online]. Available: http://seattletimes.com/flatpages/businesstechnology/boeing787fastenerproblems.html?syndication=rss.

[83] Chicago Tribute, “Behind Boeing ’ s 787 delays,” 08-Dec-2007. [Online]. Available: http://articles.chicagotribune.com/2007-12-08/news/0712070870_1_dreamliner-boeing-spokeswoman-suppliers.

[84] N. York, N. Corridor, W. D. C. Under, U. States, S. Security, Y. Amtrak, U. Kingdom, L. Angeles, S. Francisco, R. Yaro, and B. Allen, “High-speed Railways : Worth Their Hefty Price Tag ?,” pp. 1–3, 2012.

[85] Lincoln Institute of Land Policy, *High-Speed Rail International Lessons for U . S . Policy Makers*. 2011.

[86] The NEC Mater Plan Working Group, “The Northeast Corridor Infrastructure Master Plan,” 2010.

[87] Regional Plan Association, “Northeast Corridor Now,” 2013.

[88] California High-speed Rail Authority, “Implementation Plan,” 2008.

[89] California High-Speed Rail Authority, “Implementation Plan,” 2012.

[90] California High-Speed Rail Authority, “California High-Speed Rail Program Revised 2012 Business Plan,” no. April, 2012.

[91] California High-Speed Rail Authority, “Connecting California: Draft 2014 Bussines Plan,” 2014.

[92] FRA, “Preliminary National Rail Plan,” 2009.

[93] FRA, “National Rail Plan Moving Forward,” 2010.

[94] NEC Commission, “Critical Infrastructure Needs on the Northeast Corridor,” 2013.

[95] NEC Commission, “The Northeast Corridor and the American Economy,” 2014.

[96] Amtrak, “A Vision for High-Speed Rail in the Northeast Corridor,” 2010.

[97] Amtrak, “The Amtrak Vision for the Northeast Corridor (2012 Update Report),” 2012.

[98] America 2050, “Where High-Speed Rail Works Best,” 2009.

[99] America 2050, “High Speed Rail in America,” 2011.

[100] Pennsylvania University Design School, “Making High-Speed Rail Work in the Northeast Megaregion,” 2010.

[101] Pennsylvania University Design School, “High Speed Rails in the Northeast Megaregion - from vision to reality -,” 2011.

[102] Pennsylvania University Design School, “Early Actions for High Speed Rail,” 2012.

[103] RSAC, “Railroad Safety Advisory Committee Website.” [Online]. Available: https://rsac.fra.dot.gov/home.php.

[104] J. M. Sussman, M. Pena-Alcaraz, A. F. Archila, S. J. Carlson, and N. Stein, “Transportation in the Northeast Corridor of the U . S .: A Multimodal and Intermodal Conceptual Framework .,” 2012.

[105] L. S. Thompson, “Options for Federal Ownership of the Northeast Corridor (NEC) Infrastructure,” 2005.

[106] L. S. Thompson and Y. Tanaka, “High Speed rail Passenger Services: World Experience and US Applications,” 2011.

[107] TNEM, “The Northeast Maglev Website.” [Online]. Available: http://northeastmaglev.com/.

[108] FRA, “49 Code of Federal Regulations PART 238 - PASSENGER EQUIPMENT SAFETY STANDARDS -,” pp. 797–902, 2011.

[109] RSAC, “RSAC committee documents.” [Online]. Available: https://rsac.fra.dot.gov/meetings/.

[110] J. C. Peters and J. Frittelli, “Positive Train Control (PTC): Overview and Policy Issues,” 2012.

[111] FRA, “FRA Buy America and Related Requirements,” 2013.

[112] FRA, “Buy america & FRA’s High-seped Intercity Passenger Rail Program: Answers To Frequently Asked Questions,” 2013.

[113] *49 USC section 24405 (a) Buy America (PRIIA)*, vol. 2012. 2012, pp. 1–4.

[114] *41 USC section 83 Buy American Act*, vol. 2012. 1933.

[115] J. L. Goodman, “Lessons Learned From Flights of ‘ Off the Shelf ’ Aviation Navigation Units on the Space Shuttle,” pp. 1–16, 2002.

[116] N. G. Leveson and K. A. Weiss, “Making embedded software reuse practical and safe,” *ACM SIGSOFT Softw. Eng. Notes*, vol. 29, no. 6, pp. 171–178, Nov. 2004.

[117] N. G. Leveson, “Intent specifications: an approach to building human-centered specifications,” *IEEE Trans. Softw. Eng.*, vol. 26, no. 1, pp. 15–35, 2000.

[118] and U. D. Federal Ministory of Transport, Builing, “Manual on Rolling Stock: Guideline for Manufacture and Approval,” 2011.

[119] V. (Railway G. I. Kefer, “Rebuilding the Reputation of Germany’s Railways,” Sep-2012.

[120] Japan Association of Rolling Stock Industries, *Railway Engineerin Business (written in Japanese)*. 2010.

[121] J. W. Forrester, *Industrial Dynamics*. Pegasus Communications, 1961.

[122] J. M. Sussman, C. Process, J. B. Mcconnell, and A. Mostashari, “THE ‘ CLIOS PROCESS ’: a User’s Guide,” 2009.

[123] C. A. Drew, J. Nash, “Vertical separation of railway infrastructure - does it always make sense?,” pp. 1–17, 2011.

[124] International Railway Journal, “Amtrak and California issue RFP for high-speed trains,” 2014. [Online]. Available: http://www.railjournal.com/index.php/high-speed/amtrak-and-california-issue-rfp-for-high-speed-trains.html?channel=523.

[125] FRA, “Amtrak / California High Speed Rail Authority High Speed Rail Prototype Trainsets Waiver Request (FRA press),” 2014. .

APPENDIX A: BASICS OF SYSTEM DYNAMICS

While STPA is a static approach to analyze causal factors of system, System Dynamics (SD) is a dynamic approach to analyze complex causal relations and their dynamic changes. This research adopted SD to analyze detailed causal relations of system risks, based on the causal analysis in STPA. In 5.3, two possible problems are modeled by SD, and their dynamic behaviors are qualitatively analyzed.

The theory of System Dynamics was developed at Massachusetts Institute of Technology (MIT) in the 1950s by Jay Forrester [121], aiming to help decision makers understand structures and dynamics of complex systems. Similarly to STAMP, it can be regarded as a non-linear theory using feedback controls. SD models consist of *variables* that represent system attributes and *arrows* that represent causal relations of the two connected variables. In SD models, variables and arrows construct two types of feedback loops that are basic elements of the models: positive feedback loops and negative feedback loops [69]. The feedback loop in Figure A1 represents a structure of a positive feedback loop, which presents a self-reinforcing relation; e.g., an increase in variable 1 leads to an increase in variable 2 (as indicated by the "+" sign), which drives a further increase in variable 1. The "+" represents that variable 1 and variable 2 change synchronously; i.e., if variable 1 decreases, variable 2 will decrease, leading to a further decrease in variable 1. If there is no external influence, both variable 1 and variable 2 will grow (or decline) exponentially. Thus, systems with positive feedback loops could have aspects of generating growth, amplifying deviations, and reinforcing change of system variables. On the other hand, the feedback loop in Figure A2 is a negative feedback loop that mitigates system changes and seeks system equilibrium. A "-" sign represents that the two connected values change in opposite directions. In the case of the structure in Figure A2, the difference between the current value and the desired value is perceived as an error. An action proportional to the error is taken to decrease the error so that, over time, the current value approaches the desired value [52][11].

Precisely speaking, variables in SD models are classified into three types: flow, stock, and auxiliary variables. Flow and stock are necessary to define time-dependent differential relations quantitatively in models, but, for simplicity, this research does not distinguish them, and uses SD only for qualitative analysis of causal relations among variables.

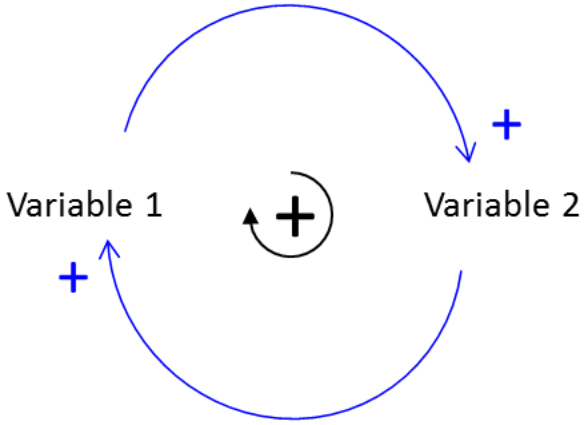

Figure A1 Positive feedback loop

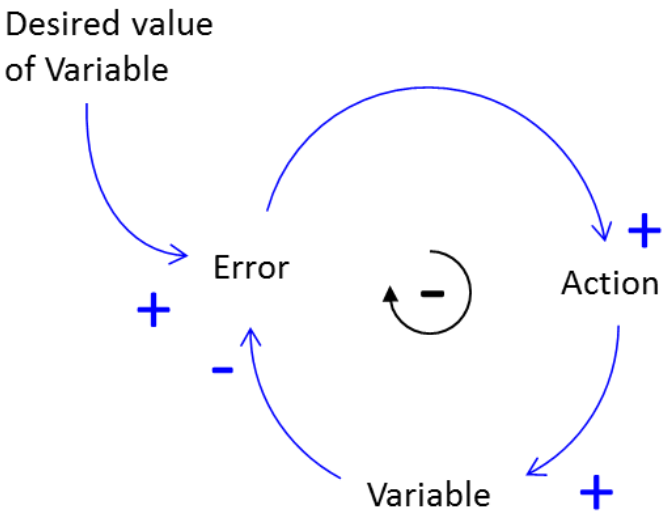

Figure A2 Negative feedback loop

APPENDIX B: SYSTEM SAFETY PROGRAM (49 CFR PART 270)

In 2012, DOT released the *System Safety Program* as a *proposed rule*. This regulation is designed to require passenger railroads to develop and implement a *System Safety Program plan*. This thesis research has analyzed its weaknesses from a STAMP-based perspective in 5.2.2. Excerpts of its executive summary (P.55372 – P.55374) and proposed list of subjects for 49 CFR Part 270 (P.55402 – P.55408) are shown as Appendix B.

DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

49 CFR Part 270

[Docket No. FRA–2011–0060, Notice No. 1]

RIN 2130–AC31

System Safety Program

AGENCY: Federal Railroad Administration (FRA), Department of Transportation (DOT).

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: FRA proposes to require commuter and intercity passenger railroads to develop and implement a system safety program (SSP) to improve the safety of their operations. An SSP would be a structured program with proactive processes and procedures developed and implemented by commuter and intercity passenger railroads to identify and mitigate or eliminate hazards and the resulting risks on each railroad's system. A railroad would have a substantial amount of flexibility to tailor an SSP to its specific operations. An SSP would be implemented by a written SSP plan and submitted to FRA for review and approval. A railroad's compliance with its SSP would be audited by FRA.

DATES: Written comments must be received by November 6, 2012. Comments received after that date will be considered to the extent possible without incurring additional expense or delay.

FRA anticipates being able to resolve this rulemaking without a public, oral hearing. However, if FRA receives a specific request for a public, oral hearing prior to October 9, 2012, one will be scheduled and FRA will publish a supplemental notice in the **Federal Register** to inform interested parties of the date, time, and location of any such hearing.

ADDRESSES: *Comments:* Comments related to Docket No. FRA–2011–0060, Notice No. 1, may be submitted by any of the following methods:

- *Web site:* The Federal eRulemaking Portal, *www.regulations.gov.* Follow the Web site's online instructions for submitting comments.
- *Fax:* 202–493–2251.
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE., Room W12–140, Washington, DC 20590.
- *Hand Delivery:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE., Room W12–140 on the Ground level of the West Building, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

Instructions: All submissions must include the agency name, docket name, and docket number or Regulatory Identification Number (RIN) for this rulemaking (2130–AC31). Note that all comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided. Please see the Privacy Act heading in the **SUPPLEMENTARY INFORMATION** section of this document for Privacy Act information related to any submitted comments or materials.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* at any time or visit the Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE., Room W12–140 on the Ground level of the West Building, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: Daniel Knote, Staff Director, Passenger Rail Division, U.S. Department of Transportation, Federal Railroad Administration, Office of Railroad Safety, Mail Stop 25, West Building 3rd Floor, 1200 New Jersey Avenue SE., Washington, DC 20590 (telephone: 631–965–1827), *Daniel.Knote@dot.gov;* or Matthew Navarrete, Trial Attorney, U.S. Department of Transportation, Federal Railroad Administration, Office of Chief Counsel, Mail Stop 10, West Building 3rd Floor, 1200 New Jersey Avenue SE., Washington, DC 20590 (telephone: 202–493–0138), *Matthew.Navarrete@dot.gov.*

SUPPLEMENTARY INFORMATION:

Table of Contents for Supplementary Information

I. Executive Summary

This proposal would require commuter and intercity passenger railroads to develop and implement a system safety program (SSP). An SSP is a structured program with proactive processes and procedures developed and implemented by commuter and intercity passenger railroads (passenger railroads) to identify and mitigate or eliminate hazards and the resulting risks on the railroad's system. An SSP encourages a railroad and its employees to work together to proactively identify hazards and to jointly determine what, if any, action to take to mitigate or eliminate the resulting risks. The proposed rule would provide each railroad with a substantial amount of flexibility to tailor its SSP to its specific operations. FRA is proposing the SSP rule as part of its efforts to continuously improve rail safety and to satisfy the statutory mandate contained in sections 103 and 109 of the Rail Safety Improvement Act of 2008 (RSIA), Public Law 110–432, Division A, 122 Stat. 4848 *et seq.,* codified at 49 U.S.C. 20156, and 20118–20119.

Section 103 of RSIA directs the Secretary of Transportation (Secretary) to issue a regulation requiring certain railroads, including passenger railroads, to develop, submit to the Secretary for review and approval, and implement a railroad safety risk reduction program. The proposed rule would implement this safety risk mandate for passenger railroads. Section 109 of RSIA authorizes the Secretary to issue a regulation protecting from discovery and admissibility into evidence in litigation documents generated for the purpose of developing, implementing, or evaluating a SSP. The proposed rule would implement section 109 with respect to the system safety program covered by part 270 and a railroad safety

risk reduction rule required by FRA for Class I freight railroads and railroads with an inadequate safety performance. The Secretary has delegated the responsibility to carry out his responsibilities under both sections 103 and 109 of RSIA, as well as the general responsibility to conduct rail safety rulemakings, codified at 49 U.S.C. 20103, to the Administrator of FRA. 49 CFR 1.49(m) and (oo). The proposed SSP rule is a performance-based rule and FRA seeks comments on all aspects of the proposed rule.

An SSP would be implemented by a written system safety program plan (SSP plan). The proposed regulation sets forth various elements that a railroad's SSP plan would be required to contain to properly implement an SSP. The main components of an SSP would be the risk-based hazard management program and risk-based hazard analysis. A properly implemented risk-based hazard management program and risk-based hazard analysis would identify the hazards and resulting risks on the railroad's system, develop methods to mitigate or eliminate, if practicable, these hazards and risks, and set forth a plan to implement these methods. As part of its risk-based hazard analysis, a railroad would consider various technologies that may mitigate or eliminate the identified hazards and risks, as well as consider the role of fatigue in creating hazards and risks.

As part of its SSP plan, a railroad would also be required to describe the various procedures, processes, and programs it has in place that support the goals of the SSP. These procedures, processes, and programs include, but are not limited to, the following: a maintenance, inspection, and, repair program; rules compliance and procedures review(s); SSP employee/contractor training; and a public safety outreach program. Since most of these are procedures, processes, and programs railroads should already have in place, the railroads would most likely only have to identify and describe such procedures, processes, and programs to comply with the regulation.

An SSP can be successful only if a railroad engages in a robust assessment of the hazards and resulting risks on its system. However, a railroad may be reluctant to reveal such hazards and risks if there is the possibility that such information may be used against it in a court proceeding for damages. Congress directed FRA to conduct a study to determine if it was in the public interest to withhold certain information, including the railroad's assessment of its safety risks and its statement of mitigation measures, from discovery and admission into evidence in proceedings for damages involving personal injury and wrongful death. *See* 49 U.S.C. 20119. FRA contracted with an outside organization to conduct this study and the study concluded that it was in the public interest to withhold this type of information from these types of proceedings. *See* FRA, *Study of Existing Legal Protections for Safety-Related Information and Analysis of Considerations for and Against protecting Railroad Safety Risk Reduction Program Information,* docket no. FRA–2011–0025–0031, Oct. 21, 2011, available at *http://www.fra.dot.gov/Downloads/FRA-Final-Study-Report.pdf.* Furthermore, Congress authorized FRA, by delegation from the Secretary, to prescribe a rule, subject to notice and comment, to address the results of the study. 49 U.S.C. 20119(b). The proposed rule addresses the study's results and sets forth protections of certain information from discovery, admission into evidence, or use for other purposes in a proceeding for damages.

An SSP will affect almost all facets of a railroad's operations. To ensure that all employees directly affected by an SSP have an opportunity to provide input on the development, implementation, and evaluation of a railroad's SSP, a railroad would be required to consult in good faith and use its best efforts to reach agreement with all of its directly affected employees on the contents of the SSP plan and amendments to the plan. In an appendix, the proposed rule provides guidance regarding what constitutes ''good faith'' and ''best efforts.''

FRA anticipates the rule would become effective 60 days after the publication of the final rule. However, by statute, the protection of certain information from discovery, admission into evidence, or use for other purposes in a proceeding for damages will not become applicable until one year after the publication of the final rule. A railroad would be required to submit its SSP plan to FRA for review not more than 90 days after the applicability date of the discovery protections, i.e., 395 days after the effective date of the final rule, or not less than 90 days prior to commencing operations, whichever is later. Within 90 days of receipt of the SSP plan, or within 90 days of receipt of an SSP plan submitted prior to the commencement of railroad operations, FRA would review the plan and determine if it meets all the requirements set forth in the regulation. If, during the review, FRA determines that the railroad's SSP plan does not comply with the requirements, FRA would notify the railroad of the specific points in which the plan is deficient. The railroad would then have 60 days to correct these deficient points and resubmit the plan to FRA. Whenever a railroad amends its SSP, it would be required to submit an amended SSP plan to FRA for approval and provide a cover letter describing the amendments. A similar approval process and timeline would apply whenever a railroad amends its SSP.

A railroad's submission of its SSP plan to FRA would not be FRA's first interaction with the railroad. FRA plans on working with the railroad throughout the development of its SSP to help the railroad properly tailor the program to its specific operation. To this end, shortly after publication of the final rule, FRA would publish a guidance manual to assist a railroad in the development, implementation, and evaluation of its SSP.

Most of the passenger railroads affected by this proposal already participate in the American Public Transportation Association (APTA) System Safety Program, which also has a triennial audit program. FRA currently provides technical assistance to new passenger railroads for the development and implementation of system safety programs and conduct of preliminary hazard analyses in the design phase. Thus, the economic impact of the proposed rule is generally incremental in nature for documentation of existing information and inclusion of certain elements not already addressed by railroads in their programs. Total estimated twenty-year costs associated with implementation of the proposed rule, for existing passenger railroads, range from $1.8 million (discounted at 7%) to $2.5 million (discounted at 3%).

FRA believes that there will be new, startup, passenger railroads, that will be formed during the twenty-year analysis period. FRA is aware of two passenger railroads that intend to commence operations in the near future. FRA assumed that one of these railroads would begin developing its SSP in Year 2, and that the other would begin developing its SSP in Year 3. FRA further assumed that one additional passenger railroad would be formed and develop its SSP every other year after that, in Years 5, 7, 9, 11, 13, 15, 17 and 19. Total estimated twenty-year costs associated with implementation of the proposed rule, for startup passenger railroads, range from $270 thousand (discounted at 7%) to $437 thousand (discounted at 3%).

Total estimated twenty-year costs associated with implementation of the proposed rule, for existing passenger

railroads and startup passenger railroads, range from $2.0 million (discounted at 7%) to $3.0 million (discounted at 3%).

Properly implemented SSPs are successful in optimizing the returns on railroad safety investments. Railroads can use them to proactively identify potential hazards and resulting risks at an early stage, thus minimizing associated casualties and property damage or avoiding them altogether. Railroads can also use them to identify a wide array of potential safety issues and solutions, which in turn allows them to simultaneously evaluate various alternatives for improving overall safety with available resources. This results in more cost effective investments. In addition, system safety planning helps railroads maintain safety gains over time. Without an SSP plan railroads could adopt countermeasures to safety problems that become less effective over time as the focus shifts to other issues. With SSP plans, those safety gains are likely to continue for longer time periods. SSP plans can also be instrumental in addressing casualties resulting from hazards that are not well-addressed through conventional safety programs, such as slips, trips and falls, or risks that occur because safety equipment is not used correctly, or routinely.

During the course of daily operations, hazards are continually discovered. Railroads must decide which hazards to address and how to do so with the limited resources available. Without a SSP plan in place, the decision process might become arbitrary. In the absence of the protections provided by the NPRM against discovery in legal proceedings for damages, railroads might also be reluctant to keep detailed records of known hazards. With a SSP plan in place, railroads are able to identify and implement the most cost effective measures to reduce casualties.

Railroad operations and maintenance activities have inherent safety critical elements. Thus, every capital expenditure is likely to have a safety component, whether for equipment, right-of-way, signaling or infrastructure. SSPs can increase the safety return on any investment related to the operation and maintenance of the railroad. FRA believes a very conservative estimate of all safety-related expenditures by all passenger railroads affected by the NPRM is $11.6 billion per year. In the first twenty years of the proposed rule, SSP plans can result in improved cost effectiveness of investments totaling between $92 billion (discounted at 7%) and $139 billion (discounted at 3%). Through anecdotal evidence, FRA is aware of situations where railroads unknowingly introduced hazards because they did not conduct hazard analyses. If the cost to remedy such situations is $100,000 on average and five remedies are avoided per year, railroads can save $500,000 per year and the proposed rule would be justified. FRA believes that it is reasonable to expect higher savings when considering there are 30 existing passenger rail operators impacted. The impact on the effectiveness of investments by startup railroads would likely be greater than for existing railroads, as more of their expenses are for new infrastructure or other systems that can have safety designed in from the start at little or no marginal cost.

Another way to look at the benefits that might accrue from implementing the proposed rule is based on potential accident prevention. Between 2001 and 2010, on average, passenger railroads had an average of 3,723.2 accidents, resulting in 207 fatalities, 3,543 other casualties, and $21.1 million in damage to railroad track and equipment each year. Total quantified twenty-year accident costs total between $24 billion (discounted at 7%) and $36 billion (discounted at 3%). Of course, these accidents also resulted in damage to other property, delays to both railroads and highway users, emergency response and clean-up costs, and other costs not quantified in this analysis. FRA estimated the accident reduction benefits necessary for the NPRM benefits to at least equal the implementation costs and found that a reduction of approximately 0.007% would suffice. FRA believes that such risk reduction is more than attainable.

FRA also believes that the SSP Plans will identify numerous unnecessary risks that are avoidable at no additional cost but simply through the selection of the most appropriate safety measure to address a hazard. For instance, railroads may mitigate or eliminate hazards that cause or contribute to slips, trips and falls, such as through measures that ensure the proper use of safety equipment. FRA believes that railroads will make additional investments to mitigate or eliminate many risks identified through the SSPs. FRA cannot reasonably predict the kinds of measures that may be adopted or the additional costs and benefits that will result from these. Nonetheless, FRA believes that such measures will not be undertaken unless the benefits exceed the costs and the funding is available.

In conclusion, FRA is confident that the accident reduction and cost effectiveness benefits together would justify the $2.0 million (discounted at 7%) to $3.0 million (discounted at 3%) implementation cost over the first twenty years of the proposed rule.

II. Background

III. System Safety Program—Generally

Railroads operate in a dynamic, fast-paced environment that at one time posed extreme safety risks. Through concerted efforts by railroads, labor organizations, the U.S. DOT, and many other entities, railroad safety has vastly improved. But even though FRA has issued safety regulations and guidance that address many aspects of railroad operations, gaps in safety exist, and hazards and risks may arise from these gaps. FRA believes that railroads are in an excellent position to identify some of these gaps and take the necessary action to mitigate or eliminate the arising hazards and resulting risks. Rather than prescribing the specific actions the railroads need to take, FRA believes it would be more effective to allow the railroads to use their knowledge of their unique operating environment to identify the gaps and determine the best methods to mitigate or eliminate the hazards and resulting risks. An SSP would provide a railroad with the tools to systematically and continuously evaluate its system to identify the hazards and risks that result from gaps in safety and to mitigate or eliminate these hazards and risks.

There are many programs that are similar to the SSP proposed by this part. Most notably, the Federal Aviation Administration (FAA) has published an NPRM proposing to require each certificate holder operating under 14 CFR part 121 to develop and implement a safety management system (SMS). 75 FR 68224, Nov. 5, 2010; and 76 FR 5296, Jan. 31, 2011. An SMS ''is a comprehensive, process-oriented approach to managing safety throughout the organization.'' 75 FR 68224, Nov. 5, 2010. An SMS includes: ''an organization-wide safety policy; formal methods for identifying hazards, controlling, and continually assessing risk; and promotion of safety culture.'' *Id.* Under FAA's proposed regulation, an SMS would have four components: Safety Policy, Safety Risk Management, Safety Assurance, and Safety Promotion. *Id.* at 68225.

The U.S. Department of Defense (DoD) has also set forth guidelines for a System Safety Program. In July 1969, DoD published ''System Safety Program Plan Requirements'' (MIL–STD–882). MIL–STD–882 is DoD's standard practice for system safety, with the most recent version, MIL–STD–882E, published on May 11, 2012. DoD, *MIL–*

received into any agency docket by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (Volume 65, Number 70; Pages 19477–78), or you may visit *http://www.dot.gov/privacy.html.*

List of Subjects in 49 CFR Part 270

Penalties; Railroad safety; Reporting and recordkeeping requirements; and System safety.

The Proposal

In consideration of the foregoing, FRA proposes to add part 270 to Chapter II, Subtitle B of Title 49, Code of Federal Regulations, to read as follows:

PART 270—SYSTEM SAFETY PROGRAM

Subpart A–General

Subpart B—System Safety Program Requirements

Subpart C—Review, Approval, and Retention of System Safety Program Plans

Subpart D—System Safety Program Internal Assessments and External Auditing

Authority: 49 U.S.C. 20103, 20106–20107, 20118–20119, 20156, 21301, 21304, 21311; 28 U.S.C. 2461, note; and 49 CFR 1.49.

Subpart A—General

§ 270.1 Purpose and scope.

(a) The purpose of this part is to improve railroad safety through structured, proactive processes and procedures developed and implemented by railroads. This part requires certain railroads to establish a system safety program that systematically evaluates railroad safety hazards on their systems and manages those risks in order to reduce the numbers and rates of railroad accidents, incidents, injuries, and fatalities.

(b) This part prescribes minimum Federal safety standards for the preparation, adoption, and implementation of railroad system safety programs. This part does not restrict railroads from adopting and enforcing additional or more stringent requirements not inconsistent with this part.

(c) This part prescribes the protection of information generated solely for the purpose of developing, implementing, or evaluating a system safety program under this part or a railroad safety risk reduction program required by this chapter for Class I railroads and railroads with inadequate safety performance.

§ 270.3 Application.

(a) Except as provided in paragraph (b) of this section, this part applies to all—

(1) Railroads that operate intercity or commuter passenger train service on the general railroad system of transportation; and

(2) Railroads that provide commuter or other short-haul rail passenger train service in a metropolitan or suburban area (as described by 49 U.S.C. 20102(2)), including public authorities operating passenger train service.

(b) This part does not apply to:

(1) Rapid transit operations in an urban area that are not connected to the general railroad system of transportation;

(2) Tourist, scenic, historic, or excursion operations, whether on or off the general railroad system of transportation;

(3) Operation of private cars, including business/office cars and circus trains; or

(4) Railroads that operate only on track inside an installation that is not part of the general railroad system of transportation (i.e., plant railroads, as defined in § 270.5).

§ 270.5 Definitions.

As used in this part—

Administrator means the Federal Railroad Administrator or his or her delegate.

Configuration management means a process that ensures that the configurations of all property, equipment, and system design elements are accurately documented.

FRA means the Federal Railroad Administration.

Fully implemented means that all elements of a system safety program as described in the SSP plan are established and applied to the safety management of the railroad.

Hazard means any real or potential condition (as identified in the railroad's risk-based hazard analysis) that can cause injury, illness, or death; damage to or loss of a system, equipment, or property; or damage to the environment.

Passenger means a person, excluding an on-duty employee, who is on board, boarding, or alighting from a rail vehicle for the purpose of travel.

Person means an entity of any type covered under 1 U.S.C. 1, including, but not limited to, the following: A railroad; a manager, supervisor, official, or other employee or agent of a railroad; any owner, manufacturer, lessor, or lessee of railroad equipment, track, or facilities; any independent contractor or subcontractor providing goods or services to a railroad; and any employee of such owner, manufacturer, lessor, lessee, or independent contractor or subcontractor.

Plant railroad means a plant or installation that owns or leases a locomotive, uses that locomotive to switch cars throughout the plant or installation, and is moving goods solely for use in the facility's own industrial processes. The plant or installation could include track immediately adjacent to the plant or installation if the plant railroad leases the track from the general system railroad and the lease provides for (and actual practice entails) the exclusive use of that trackage by the plant railroad and the general system railroad for purposes of moving only cars shipped to or from the plant. A plant or installation that operates a locomotive to switch or move cars for other entities, even if solely within the confines of the plant or installation, rather than for its own purposes or industrial processes, is not considered a plant railroad because the performance of such activity makes the operation part of the general railroad system of transportation.

Positive train control system means a system designed to prevent train-to-train collisions, overspeed derailments, incursions into established work zone limits, and the movement of a train through a switch left in the wrong position, as described in subpart I of part 236 of this chapter.

Rail vehicle means railroad rolling stock, including, but not limited to passenger and maintenance vehicles.

Railroad means—

(1) Any form of non-highway ground transportation that runs on rails or electromagnetic guideways, including—

(i) Commuter or other short-haul rail passenger service in a metropolitan or suburban area and commuter railroad service that was operated by the Consolidated Rail Corporation on January 1, 1979; and

(ii) High speed ground transportation systems that connect metropolitan areas, without regard to whether those systems use new technologies not associated with traditional railroads, but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation; and

(2) A person or organization that provides railroad transportation, whether directly or by contracting out operation of the railroad to another person.

Risk means the combination of the probability (or frequency of occurrence) and the consequence (or severity) of a hazard.

SSP plan means system safety program plan.

System safety means the application of management and engineering principles, and techniques to optimize all aspects of safety, within the constraints of operational effectiveness, time, and cost, throughout all phases of a system life cycle.

Tourist, scenic, historic, or excursion operations means railroad operations that carry passengers, often using antiquated equipment, with the conveyance of the passengers to a particular destination not being the principal purpose. Train movements of new passenger equipment for demonstration purposes are not tourist, scenic, historic, or excursion operations.

§ 270.7 Waivers.

(a) A person subject to a requirement of this part may petition the Administrator for a waiver of compliance with such requirement. The filing of such a petition does not affect that person's responsibility for compliance with that requirement while the petition is being considered.

(b) Each petition for a waiver under this section shall be filed in the manner and contain the information required by part 211 of this chapter.

(c) If the Administrator finds that a waiver of compliance is in the public interest and is consistent with railroad safety, the Administrator may grant the waiver subject to any conditions the Administrator deems necessary.

§ 270.9 Penalties and responsibility for compliance.

(a) Any person who violates any requirement of this part or causes the violation of any such requirement is subject to a civil penalty of at least $650 and not more than $25,000 per violation, except that: Penalties may be assessed against individuals only for willful violations, and, where a grossly negligent violation or a pattern of repeated violation has created an imminent hazard of death or injury to persons, or has caused death or injury, a penalty not to exceed $105,000 per violation may be assessed. Each day a violation continues shall constitute a separate offense. Any person who knowingly and willfully falsifies a record or report required by this part may be subject to criminal penalties under 49 U.S.C. 21311 (formerly codified in 45 U.S.C. 438(e)). Appendix A contains a schedule of civil penalty amounts used in connection with this part.

(b) Although the requirements of this part are stated in terms of the duty of a railroad, when any person, including a contractor or subcontractor to a railroad, performs any function covered by this part, that person (whether or not a railroad) shall perform that function in accordance with this part.

Subpart B—System Safety Program Requirements

§ 270.101 System safety program; general.

(a) Each railroad subject to this part shall establish and fully implement a system safety program that continually and systematically evaluates railroad safety hazards on its system and manages the resulting risks to reduce the number and rates of railroad accidents, incidents, injuries, and fatalities. A system safety program shall include a risk-based hazard management program and risk-based hazard analysis designed to proactively identify hazards and mitigate the resulting risks. The system safety program shall be fully implemented and supported by a written SSP plan described in § 270.103.

(b) A railroad's SSP shall be designed so that it promotes and supports a positive safety culture at the railroad.

§ 270.102 Consultation requirements.

(a) *General duty.* (1) Each railroad required to establish a system safety program under this part shall in good faith consult with, and use its best efforts to reach agreement with, all of its directly affected employees on the contents of the SSP plan.

(2) For purposes of this part, the term directly affected employees includes any non-profit employee labor organization representing a class or craft of directly affected employees of the railroad. A railroad that consults with such a non-profit employee labor organization is considered to have consulted with the directly affected employees represented by that organization.

(3) A railroad shall meet no later than (180 days after the effective date of the final rule) with its directly affected employees to discuss the consultation process. The railroad shall notify the directly affected employees of this meeting no less than 60 days before it is scheduled.

(4) Appendix B to this part contains guidance on how a railroad might comply with the requirements of this section.

(b) *Railroad consultation statements.* A railroad required to submit an SSP plan under § 270.201 must also submit, together with that plan, a consultation statement that includes the following information:

(1) A detailed description of the process the railroad utilized to consult with its directly affected employees;

(2) If the railroad was not able to reach agreement with its directly affected employees on the contents of its SSP plan, identification of any known areas of non-agreement and an explanation why it believes agreement was not reached;

(3) If the SSP plan would affect a provision of a collective bargaining agreement between the railroad and a non-profit employee labor organization, identification of any such provision and an explanation how the SSP plan would affect it; and

(4) A service list containing the names and contact information for the international/national president and general chairperson of any non-profit employee labor organization representing a class or craft of the railroad's directly affected employees; any labor organization representative who participated in the consultation process; and any directly affected employee who significantly participated in the consultation process independently of a non-profit employee labor organization. When a railroad submits its SSP plan and consultation statement to FRA, it must also send a copy of these documents to all individuals identified in the service list.

(c) *Statements from directly affected employees.* (1) If a railroad and its directly affected employees cannot reach agreement on the proposed contents of an SSP plan, then directly affected employees may file a statement with the FRA Associate Administrator for Railroad Safety/Chief Safety Officer explaining their views on the plan on which agreement was not reached. The FRA Associate Administrator for

Railroad Safety/Chief Safety Officer shall consider any such views during the plan review and approval process.

(2) A railroad's directly affected employees have 60 days following the railroad's submission of a proposed SSP plan to submit the statement described in paragraph (c)(1) of this section.

(d) *Consultation requirements for system safety program plan amendments.* As required by § 270.201(c)(1)(i), a railroad's SSP plan must include a description of the process the railroad will use to consult with its directly affected employees on any subsequent substantive amendments to the railroad's system safety program. The requirements of this paragraph do not apply to non-substantive amendments (e.g., amendments that update names and addresses of railroad personnel).

§ 270.103 System safety program plan.

(a) *General.* (1) Each railroad subject to this part shall adopt and fully implement a system safety program through a written SSP plan that, at a minimum, contains the elements in this section. This SSP plan shall be approved by FRA under the process specified in § 270.201.

(2) Each railroad subject to this part shall communicate with each railroad that hosts passenger train service for that railroad and coordinate the portions of the SSP plan applicable to the railroad hosting the passenger train service.

(b) *System safety program policy statement.* Each railroad shall set forth in its SSP plan a policy statement that endorses the railroad's system safety program. This policy statement shall:

(1) Define the railroad's authority for establishment and implementation of the system safety program; and

(2) Be signed by the chief official at the railroad.

(c) *Purpose and scope of system safety program.* Each railroad shall set forth in its SSP plan a statement defining the purpose and scope of the system safety program. The purpose and scope statement shall describe:

(1) The safety philosophy and safety culture of the railroad;

(2) The railroad's management responsibilities within the system safety program; and

(3) How host railroads, contractor operators, shared track/corridor operators, contractors who provide significant safety-related services, and any other entity or person that provides significant safety-related services as identified by the railroad pursuant to paragraph (e)(2) of this section will, as appropriate, support and participate in the railroad's system safety program.

(d) *System safety program goals.* Each railroad shall set forth in its SSP plan a statement defining the goals for the railroad's system safety program. This statement shall describe clear strategies on how the goals will be achieved and what management's responsibilities are to achieve them. At a minimum, the goals shall be:

(1) Long-term;

(2) Meaningful;

(3) Measurable; and

(4) Focused on the identification of hazards and the mitigation or elimination of the resulting risks.

(e) *Railroad system description.* (1) Each railroad shall set forth in its SSP plan a statement describing the railroad's system. The description shall include: a history of the railroad's operations, including any host operations; the physical characteristics of the railroad; the scope of service; the railroad's maintenance; and identification of the physical plant and any other pertinent aspects of the railroad's system.

(2) Each railroad shall identify the persons that provide significant safety-related services to the railroad.

(f) *Railroad management and organizational structure.* Each railroad shall set forth a statement in its SSP plan that describes the management/organizational structure of the railroad. This statement shall include:

(1) A chart or other visual representation of the organizational structure of the railroad;

(2) A description of how safety responsibilities are distributed within the railroad organization;

(3) Clear identification of the lines of authority used by the railroad to manage safety issues; and

(4) A description of the relationships and responsibilities between the railroad, host railroads, contract operators, shared track/corridor operators, and other entities or persons that provide significant safety-related services. The statement shall set forth the roles and responsibilities in the railroad's system safety program for each host railroad, contract operator, shared track/corridor operator, or other entity or person that provides significant safety-related services.

(g) *System safety program implementation plan.* Each railroad shall set forth a plan in its SSP plan that describes how the system safety program will be implemented on that railroad. This plan shall include a description of the:

(1) Roles and responsibilities of each position or job function that has significant responsibility for implementing the system safety program, including those held by employees, contractors who provide significant safety-related services, and other entities or persons that provide significant safety-related services; and

(2) Milestones necessary to be reached to fully implement the program.

(h) *Maintenance, inspection and repair program.* (1) Each railroad shall identify and describe in its SSP plan the processes and procedures used for maintenance and repair of infrastructure and equipment directly affecting railroad safety. Examples of infrastructure and equipment that directly affect railroad safety include: fixed facilities and equipment, rolling stock, signal and train control systems, track and right-of-way, and traction power distribution systems.

(2) Each description of the processes and procedures used for maintenance and repair of infrastructure and equipment directly affecting safety shall include the processes and procedures used to conduct testing and inspections of the infrastructure and equipment.

(i) *Rules compliance and procedures review.* Each railroad shall set forth a statement describing the processes and procedures used by the railroad to develop, maintain, and comply with the railroad's rules and procedures directly affecting railroad safety and to comply with the applicable railroad safety laws and regulations found in this chapter. The statement shall include:

(1) Identification of the railroad's operating and safety rules and procedures that are subject to review under this chapter;

(2) Techniques used to assess the compliance of the railroad's employees with the railroad's operating and safety rules and maintenance procedures, and applicable FRA regulations; and

(3) Techniques used to assess the effectiveness of the railroad's supervision relating to the compliance with the railroad's operating and safety rules and maintenance procedures, and applicable railroad safety laws and regulations.

(j) *System safety program employee/contractor training.* (1) Each railroad shall set forth a statement in its SSP plan that describes the railroad's system safety program training plan. A system safety program training plan shall set forth the procedures in which employees who are responsible for implementing and supporting the SSP, contractors who provide significant safety-related services, and any other entity or person that provides significant safety-related services will be trained on the railroad's system safety

program. A system safety program training plan shall help ensure that all personnel who are responsible for implementing and supporting the system safety program understand the goals of the program, are familiar with the elements of the railroad's program, and have the requisite knowledge and skills to fulfill their responsibilities under the program. The railroad shall keep a record of training conducted under this part and update that record as necessary.

(2) For each position or job function identified pursuant to paragraph (g)(1) of this section, the training plan shall describe the frequency and content of the system safety program training the position receives.

(3) If a position or job function is not identified under paragraph (g)(1) of this section as having significant responsibilities to implement and support the system safety program but the position or job function is safety related or has a significant impact on safety, personnel in those positions or performing those job functions shall receive training in basic system safety concepts and the system safety implications of their position or job function.

(4) Training under this subpart may be conducted by interactive computer-based training, video conferencing, or formal classroom training.

(5) The system safety program training plan shall set forth the process used to maintain and update the necessary training records required by this part.

(6) The system safety program training plan shall set forth the process used by the railroad to ensure that it is complying with the training requirements set forth in the training plan.

(k) *Emergency management.* Each railroad shall set forth a statement in its SSP plan that describes the processes used by the railroad to manage emergencies that may arise within its system including, but not limited to, the processes to comply with applicable emergency equipment standards contained in part 238 of this chapter and the passenger train emergency preparedness requirements contained in part 239 of this chapter.

(l) *Workplace safety.* Each railroad shall set forth a statement in its SSP plan that describes the programs established by the railroad that protect the safety of the railroad's employees and contractors. The statement shall describe any:

(1) Processes that help ensure the safety of employees and contractors while working on or in close proximity to the railroad's property as described in paragraph (e) of this section;

(2) Processes that help ensure the employees and contractors understand the requirements established by the railroad pursuant to paragraph (g)(1) of this section; and

(3) Fitness-for-duty programs, including standards for the control of alcohol and drug use contained in part 219 of this chapter, fatigue management programs established by this part, and medical monitoring programs.

(m) *Public safety outreach program.* Each railroad shall establish and set forth a statement in its SSP plan that describes its public safety outreach program that provides safety information to railroad passengers and the general public.

(n) *Accident reporting and investigation.* Each railroad shall set forth a statement in its SSP plan that describes the processes that the railroad uses to receive notification of accidents, investigate and report those accidents, and develop, implement, and track any corrective actions found necessary to address the investigation's finding(s).

(o) *Safety data acquisition.* Each railroad shall set forth a statement in its SSP plan that describes the processes used to collect, maintain, analyze, and distribute safety data in support of the system safety program.

(p) *Contract procurement requirements.* Each railroad shall set forth a statement in its SSP plan that describes the process to help ensure that safety concerns and hazards are adequately addressed during the safety-related contract procurement process.

(q) *Risk-based hazard management program.* Each railroad shall establish a risk-based hazard management program as part of the railroad's system safety program. The risk-based hazard management program shall be fully described in the SSP plan. The description of the risk-based hazard management program shall include:

(1) The identity of the individual(s) responsible for administering the risk-based hazard management program;

(2) The identities of stakeholders who will participate in the risk-based hazard management program;

(3) The structure and participants in any hazard management teams or safety committees that a railroad may establish to support the risk-based hazard management program;

(4) The process for setting goals for the risk-based hazard management program and how performance against the goals will be reported;

(5) The processes used in the risk-based hazard analysis to identify hazards on the railroad's system;

(6) The processes or procedures that will be used in the risk-based hazard analysis to analyze hazards and support the risk-based hazard management program;

(7) The methods used in the risk-based hazard analysis to determine the severity and frequency of hazards and to calculate the resulting risk;

(8) The methods used in the risk-based hazard analysis to identify actions that mitigate or eliminate hazards and corresponding risks.

(9) How decisions affecting safety of the rail system will be made relative to the risk-based hazard management program;

(10) The methods used in the risk-based hazard management program to support continuous safety improvement throughout the life of the rail system.

(11) The method used to maintain records of identified hazards and risks and mitigations throughout the life of the rail system.

(r) *Risk-based hazard analysis.* (1) Once FRA approves a railroad's SSP pursuant to § 270.201(b), the railroad shall apply the risk-based hazard analysis methodology identified in paragraph (q)(5) through (7) of this section to identify and analyze hazards on the railroad system and to determine the resulting risks. At a minimum, the aspects of the railroad system that should be analyzed include: operating rules and practices, infrastructure, equipment, employee levels and schedules, management structure, employee training, employee fatigue as identified in paragraph (s) of this section, new technology as identified in paragraph (t) of this section, and other aspects that have an impact on railroad safety not covered by railroad safety regulations or other Federal regulations.

(2) A risk-based hazard analysis shall identify and implement specific actions using the methods described in paragraph (q)(8) of this section that will mitigate or eliminate the hazards and resulting risks identified by paragraph (r)(1) of this section.

(3) A railroad shall also conduct a risk-based hazard analysis pursuant to paragraphs (r)(1) and (2) of this section when there are significant operational changes, system extensions, system modifications, or other circumstances that have a direct impact on railroad safety.

(s) *Technology analysis and implementation plan.* (1) A railroad shall conduct a technology analysis that evaluates current, new, or novel technologies that may mitigate or eliminate hazards and the resulting risks identified in the risk-based hazard analysis process. The railroad shall

analyze the safety impact, feasibility, and cost and benefits of implementing technologies that will mitigate or eliminate hazards and the resulting risks. At a minimum, the technologies a railroad shall consider as part of its technology analysis are: processor-based technologies, positive train control systems, electronically-controlled pneumatic brakes, rail integrity inspection systems, rail integrity warning systems, switch position monitors and indicators, trespasser prevention technology, and highway-rail grade crossing warning and protection technology. The railroad shall make the results of the technology analysis conducted pursuant to this paragraph available upon request to representatives of FRA upon request and States participating under part 212 of this chapter.

(2) A railroad shall establish a technology implementation plan as part of its SSP plan that contains the results of the technology analysis conducted pursuant to paragraph (s)(1) of this section. If a railroad decides to implement any of the technologies identified in the technology analysis based on the technology's safety impact, feasibility, or costs and benefits, the technology implementation plan shall describe the railroad's plan and a prioritized implementation schedule for the development, adoption, implementation and maintenance of those technologies over a 10-year period.

(3) Except as required by subpart I of part 236 of this chapter, if a railroad decides to implement positive train control systems as part of its technology implementation plan, the railroad shall set forth and comply with a schedule for implementation of the positive train control system no later than December 31, 2018.

(t) *Fatigue management plan.* A railroad shall set forth in its SSP plan a Fatigue Management Plan no later than (three years after the effective date of the final rule).

(u) *Safety Assurance*—(1) *Change management.* Each railroad shall establish and set forth a statement in its SSP plan describing processes and procedures used by the railroad to manage significant operational changes, system extensions, system modifications, or other significant changes that will have a direct impact on railroad safety.

(2) *Configuration management.* Each railroad shall establish a configuration management program and describe the program in its SSP plan. The configuration management program shall—

(i) State who within the railroad has authority to make configuration changes;

(ii) Establish processes to make configuration changes to the railroad's system; and

(iii) Establish processes to ensure that all departments of the railroad affected by the configuration changes are formally notified and approve of the change.

(3) *Safety certification.* Each railroad shall establish and set forth a statement in its SSP plan that describes the certification process used by the railroad to help ensure that safety concerns and hazards are adequately addressed prior to the initiation of operations and major projects to extend, rehabilitate, or modify an existing system or replace vehicles and equipment.

(v) *Safety culture.* A railroad shall set forth a statement in its SSP plan that describes how it measures the success of its safety culture identified in paragraph (c)(1) of this section.

§ 270.105 Discovery and admission as evidence of certain information.

(a) Any information (including plans, reports, documents, surveys, schedules, lists, or data) compiled or collected solely for the purpose of developing, implementing, or evaluating a system safety program under this part, including a railroad carrier's analysis of its safety risks conducted pursuant to § 270.103(r)(1) and its statement of the mitigation measures with which it would address those risks created pursuant to § 270.103(r)(2), shall not be subject to discovery, admitted into evidence, or considered for other purposes in a Federal or State court proceedings for damages involving personal injury, wrongful death, or property damage.

(b) This section does not affect the discovery, admissibility, or consideration for other purposes of information (including plans, reports, documents, surveys, schedules, lists, or data) compiled or collected for a purpose other than that specifically identified in paragraph (a) of this section. Such information shall continue to be discoverable and admissible into evidence if it was discoverable and admissible prior to the existence of this section. This includes such information that either:

(1) Existed prior to (365 days from the publication of the final rule);

(2) Existed prior to (365 days from the publication of the final rule) and that continues to be compiled or collected; or

(3) Is compiled or collected after (365 days from the publication of the final rule).

(c) State discovery rules and sunshine laws that could be used to require the disclosure of information protected by paragraph (a) of this section are preempted.

(d) Paragraphs (a) through (c) of this section shall apply to any railroad safety risk reduction programs required by this chapter for Class I railroads, railroads with inadequate safety performance, or any other railroad.

Subpart C—Review, Approval, and Retention of System Safety Program Plans

§ 270.201 Filing and approval.

(a) *Filing.* (1) Each railroad to which this part applies shall submit one copy of its SSP plan to the FRA Associate Administrator for Railroad Safety/Chief Safety Officer at Mail Stop 25, 1200 New Jersey Avenue SE., Washington, DC 20590, not more than (395 days after the effective date of the final rule) or not less than 90 days prior to commencing operations, whichever is later.

(2) The railroad shall not include in its SSP plan the risk-based hazard analysis conducted pursuant to § 270.103(r). The railroad shall make the results of any risk-based hazard analysis available upon request to representatives of FRA and States participating under part 212 of this chapter.

(3) The SSP plan shall include the signature, name, title, address, and telephone number of the chief safety officer who bears primary managerial authority for implementing the program for the submitting railroad. The system safety plan shall also include the name and contact information for:

(i) The primary person responsible for managing the system safety program, and

(ii) The senior representatives of host railroads, contract operators, shared track/corridor operators, and others who provide significant safety-related services.

(4) As required by § 270.102(b), each railroad must submit with its SSP plan a consultation statement describing how it consulted with its directly affected employees on the contents of its system safety program. Directly affected employees may also file a statement in accordance with § 270.102(c).

(5) The chief official responsible for safety and who bears primary managerial authority for implementing the program for the submitting railroad shall certify that the contents of the SSP plan are accurate and that the railroad

will implement the contents of the program as approved by FRA pursuant to paragraph (b) of this section.

(b) *Approval.* (1) Within 90 days of receipt of a SSP plan, or within 90 days of receipt of each SSP plan submitted prior to the commencement of railroad operations, FRA will review the proposed SSP plan to determine if the elements prescribed in this part are sufficiently addressed in the railroad's submission. This review will also consider any statement submitted by directly affected employees pursuant to § 270.102.

(2) FRA will notify the primary contact person of each affected railroad in writing whether the proposed plan has been approved by FRA, and if not approved, the specific points in which the plan is deficient. FRA will also provide this notification to each individual identified in the service list accompanying the consultation statement required under § 270.102(b).

(3) If a proposed system safety plan is not approved by FRA, the affected railroad shall amend the proposed plan to correct all deficiencies identified by FRA and provide FRA with a corrected copy of the SSP plan not later than 60 days following receipt of FRA's written notice that the proposed SSP plan was not approved.

(c) *Review of Amendments.* (1)(i) Railroads shall submit amendment(s) to the SSP plan to FRA not less than 60 days prior to the proposed effective date of the amendment(s). The railroad shall file the amended SSP plan with a cover letter outlining the changes made to the original approved SSP plan by the proposed amendment(s). The cover letter shall also describe the process it used pursuant to § 270.102(d) to consult with directly affected employees on the amendment(s).

(ii) If the amendment(s) is safety-critical and the railroad is unable to submit the amended SSP plan to FRA 60 days prior to the proposed effective date of the amendment(s), the railroad shall submit the amended SSP plan to FRA as soon as possible thereafter.

(2)(i) FRA will review the proposed amended SSP plan within 45 days of receipt. FRA will then notify the primary contact person of each affected railroad whether the proposed amended plan has been approved by FRA, and if not approved, the specific points in which the proposed amendment(s) to the SSP plan is deficient.

(ii) If FRA has not notified the railroad by the proposed effective date of the amendment(s) whether the proposed amended plan has been approved or not, the railroad may implement the amendment(s), subject to FRA's decision.

(iii) If a proposed SSP amendment is not approved by FRA, the affected railroad shall correct all deficiencies identified by FRA. The railroad shall provide FRA with a corrected copy of the amended SSP plan no later than 60 days following receipt of FRA's written notice that the proposed amendment was not approved.

(d) *Reopened Review.* Following initial approval of a plan, or amendment, FRA may reopen consideration of the plan, or amendment, for cause stated.

§ 270.203 Retention of system safety program plan.

Each railroad to which this part applies shall retain at its system headquarters and at any division headquarters, one copy of the SSP plan required by this part and one copy of each subsequent amendment to that plan. These records shall be made available to representatives of FRA and States participating under part 212 of this chapter for inspection and copying during normal business hours.

Subpart D—System Safety Program Internal Assessments and External Auditing

§ 270.301 General.

The system safety program and its implementation shall be assessed internally by the railroad and audited externally by the FRA or FRA's designee.

§ 270.303 Internal system safety program assessment.

(a) Following FRA's initial approval of the railroad's SSP plan pursuant to § 270.201, the railroad shall annually conduct an assessment of the extent to which:

(1) The system safety program is fully implemented;

(2) The railroad is in compliance with the implemented elements of the approved system safety program; and

(3) The railroad has achieved the goals set forth in § 270.103(d).

(b) As part of its system safety plan, the railroad shall set forth a statement describing the processes used to:

(1) Conduct internal system safety program assessments;

(2) Internally report the findings of the internal system safety program assessments;

(3) Develop, track, and review recommendations as a result of the internal system safety program assessment;

(4) Develop improvement plans based on the internal system safety program assessments. Improvement plans shall, at a minimum, identify who is responsible for carrying out the necessary tasks to address assessment findings and specify a schedule of target dates with milestones to implement the improvements that address the assessment findings;

(5) Manage revisions and updates to the SSP plan based on the internal system safety program assessments; and

(6) Comply with the reporting requirements set forth in § 270.201.

(c)(1) Within 60 days of completing its internal SSP plan assessment pursuant to paragraph (a) of this section, the railroad shall:

(i) Submit to FRA a copy of the railroad's internal assessment report that includes a system safety program assessment and the status of internal assessment findings and improvement plans; and

(ii) Outline the specific improvement plans for achieving full implementation of the SSP plan, as well as achieving the goals of the plan.

(2) The railroad's chief official responsible for safety shall certify the results of the railroad's internal SSP plan assessment.

§ 270.305 External safety audit

(a) FRA may conduct, or cause to be conducted, external audits of a railroad's system safety program. Each audit will evaluate the railroad's compliance with the elements required by this part in the railroad's approved SSP plan. FRA shall provide the railroad written notification of the results of any audit.

(b)(1) Within 60 days of FRA's written notification of the results of the audit, the railroad shall submit to FRA for approval, if necessary, improvement plans to address all audit findings. Improvement plans submitted shall, at a minimum, identify who is responsible for carrying out the necessary tasks to address audit findings and specify target dates and milestones to implement the improvements that address the audit findings.

(2) If FRA does not approve the railroad's improvement plan, FRA will notify the railroad of the specific deficiencies in the improvement plan. The affected railroad shall amend the proposed plan to correct the deficiencies identified by FRA and provide FRA with a corrected copy of the improvement plan no later than 30 days following receipt of FRA's written notice that the proposed plan was not approved.

(3) Upon request, the railroad shall provide to FRA and States participating under part 212 of this chapter for review

a report regarding the status of the implementation of the improvements set forth in the improvement plan established pursuant to paragraph (b)(1) of this section.

Appendix A to Part 270—Schedule of Civil Penalties [Reserved]

Appendix B to Part 270—Federal Railroad Administration Guidance on the System Safety Program Consultation Process

A railroad required to develop a system safety program under this part must in good faith consult with and use its best efforts to reach agreement with its directly affected employees on the contents of the SSP plan. *See* § 270.102(a). This appendix discusses the meaning of the terms ''good faith'' and ''best efforts,'' and provides guidance on how a railroad could comply with the requirement to consult with directly affected employees on the contents of its SSP plan. Specific guidance will be provided for employees who are represented by a non-profit employee labor organization and employees who are not represented by any such organization.

The Meaning of ''Good Faith'' and ''Best Efforts''

''Good faith'' and ''best efforts'' are not interchangeable terms representing a vague standard for the § 270.102 consultation process. Rather, each term has a specific and distinct meaning. When consulting with directly affected employees, therefore, a railroad must independently meet the standards for both the good faith and best efforts obligations. A railroad that does not meet the standard for one or the other will not be in compliance with the consultation requirements of § 270.102.

The good faith obligation requires a railroad to consult with employees in a manner that is honest, fair, and reasonable, and to genuinely pursue agreement on the contents of an SSP plan. If a railroad consults with its employees merely in a perfunctory manner, without genuinely pursuing agreement, it will not have met the good faith requirement. A railroad may also fail to meet its good faith obligation if it merely attempts to use the SSP plan to unilaterally modify a provision of a collective bargaining agreement between the railroad and a non-profit employee labor organization.

On the other hand, ''best efforts'' establishes a higher standard than that imposed by the good faith obligation, and describes the diligent attempts that a railroad must pursue to reach agreement with its employees on the contents of its system safety program. While the good faith obligation is concerned with the railroad's state of mind during the consultation process, the best efforts obligation is concerned with the specific efforts made by the railroad in an attempt to reach agreement. This would include considerations such as whether a railroad had held sufficient meetings with its employees, or whether the railroad had made an effort to respond to feedback provided by employees during the consultation process. For example, a railroad would not meet the best efforts obligation if it did not initiate the consultation process in a timely manner, and thereby failed to provide employees sufficient time to engage in the consultation process. A railroad may, however, wish to hold off substantive consultations regarding the contents of its SSP until one year after the effective date of the rule in order to ensure that information generated as part of the process is protected from discovery and admissibility into evidence under § 270.105 of the rule. Generally, best efforts are measured by the measures that a reasonable person in the same circumstances and of the same nature as the acting party would take. Therefore, the standard imposed by the best efforts obligation may vary with different railroads, depending on a railroad's size, resources, and number of employees.

When reviewing SSP plans, FRA will determine on a case-by-case basis whether a railroad has met its § 270.102 good faith and best efforts obligations. This determination will be based upon the consultation statement submitted by the railroad pursuant to § 270.102(b) and any statements submitted by employees pursuant to § 270.102(c). If FRA finds that these statements do not provide sufficient information to determine whether a railroad used good faith and best efforts to reach agreement, FRA may investigate further and contact the railroad or its employees to request additional information. If FRA determines that a railroad did not use good faith and best efforts, FRA may disapprove the SSP plan submitted by the railroad and direct the railroad to comply with the consultation requirements of § 270.102. Pursuant to § 270.201(b)(3), if FRA does not approve the SSP plan, the railroad will have 60 days, following receipt of FRA's written notice that the plan was not approved, to correct any deficiency identified. In such cases, the identified deficiency would be that the railroad did not use good faith and best efforts to consult and reach agreement with its directly affected employees. If a railroad then does not submit to FRA within 60 days a SSP plan meeting the consultation requirements of § 270.102, the railroad could be subject to penalties for failure to comply with § 270.201(b)(3).

Guidance on How a Railroad May Consult With Directly Affected Employees

Because the standard imposed by the best efforts obligation will vary depending upon the railroad, there may be countless ways for various railroads to comply with the consultation requirements of § 270.102. Therefore, FRA believes it is important to maintain a flexible approach to the § 270.102 consultation requirements, in order to give a railroad and its directly affected employees the freedom to consult in a manner best suited to their specific circumstances.

FRA is nevertheless providing guidance in this appendix as to how a railroad may proceed when consulting (utilizing good faith and best efforts) with employees in an attempt to reach agreement on the contents of an SSP plan. FRA believes this guidance may be useful as a starting point for railroads that are uncertain about how to comply with the § 270.102 consultation requirements. This guidance distinguishes between employees who are represented by a non-profit employee labor organization and employees who are not, as the processes a railroad may use to consult with represented and non-represented employees could differ significantly.

This guidance does not establish prescriptive requirements with which a railroad must comply, but merely outlines a consultation process a railroad may choose to follow. A railroad's consultation statement could indicate that the railroad followed the guidance in this appendix as evidence that it utilized good faith and best efforts to reach agreement with its employees on the contents of a SSP plan.

Employees Represented by a Non-Profit Employee Labor Organization

As provided in § 270.102(a)(2), a railroad consulting with the representatives of a non-profit employee labor organization on the contents of a SSP plan will be considered to have consulted with the directly affected employees represented by that organization.

A railroad could utilize the following process as a roadmap for using good faith and best efforts when consulting with represented employees in an attempt to reach agreement on the contents of an SSP plan.

- Pursuant to § 270.102(a)(3), a railroad must meet with representatives from a non-profit employee labor organization (representing a class or craft of the railroad's directly affected employees) within 180 days of the effective date of the final rule to begin the process of consulting on the contents of the railroad's SSP plan. A railroad must provide notice at least 60 days before the scheduled meeting.
- During the time between the initial meeting and the applicability date of § 270.105 the parties may meet to discuss administrative details of the consultation process as necessary.
- Within 60 after the applicability date of § 270.105 a railroad should have a meeting with the directed affected employees to discuss substantive issues with the SSP.
- Within 90 days after the applicability date of § 270.105, a railroad would file its SSP plan with FRA.
- As provided by § 270.102(c), if agreement on the contents of a SSP plan could not be reached, a labor organization (representing a class or craft of the railroad's directly affected employees) could file a statement with the FRA Associate Administrator for Railroad Safety/Chief Safety Officer explaining its views on the plan on which agreement was not reached.

Employees Who Are Not Represented by a Non-Profit Employee Labor Organization

FRA recognizes that some (or all) of a railroad's directly affected employees may not be represented by a non-profit employee labor organization. For such non-represented employees, the consultation process described for represented employees may not be appropriate or sufficient. For example, FRA believes that a railroad with non-represented employees must make a concerted effort to ensure that its non-