ADDIS ABABA UNIVERSITY
ADDIS ABABA INSTITUTE OF TECHNOLOGY
SCHOOL OF MECHANICAL AND INDUSTRIAL ENGINEERING
UNDER RAILWAY MECHANICAL ENGINEERING
STREAM

DEVELOPMENT OF SAFETY CONTROL STRUCTURE OF ADDIS ABABA LIGHT RAIL TRANSIT, USING SYSTEM – THEORETIC APPROACH

A Thesis Submitted to the Graduate School of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Masters of Science

In

Railway Mechanical Engineering

By:

Gemta Kedjela

ID NO. GSR/3806/05

Advisor:

DR.Gulelat Gatew

March, 2015

Addis Ababa University

Addis Ababa Institute of Technology

School Of Mechanical and Industrial Engineering

Under Railway Mechanical Engineering

Stream

DEVELOPMENT OF SAFETY CONTROL STRUCTURE OF ADDIS ABABA LIGHT RAIL TRANSIT, USING SYSTEM –THEORETIC APPROACH

By: Gemta Kedjela

Approved by: Board of Examiners

_____	_____	_____
Chairman of Department	Signature	Date
Graduate Committee (DGC)		
Dr. Gulelat Gatew.	_____	_____
Advisor	Signature	Date
Internal examiner	_____	_____
	Signature	Date
External examiner	_____	_____
	Signature	Date
Associate Dean,	_____	_____
Research and graduate program	Signature	Date

DECLARATION

I hereby declare that the work which is being presented in this thesis entitled, **"DEVELOPMENT OF SAFETY CONTROL STRUCTURE OF ADDIS ABABA LIGHT RAIL TRANSIT, USING SYSTEM –THEORETIC APPROACH "** is original work of my own, has not been presented for a degree of any other university and all the resource of materials uses for this thesis have been duly acknowledged.

_____ _____

Gemta Kedjela Date

This is to certify that the above declaration made by the candidate is correct to the best of my knowledge.

_____ _____

Dr.Gulelat Gatew Date

ACKNOWLEDGEMENT

First of all, I would like to thank my almighty God, for what he has done to me, during those hard times.

I would like to express my sincere gratitude to my thesis advisor, Doctor Gulelat Gatew, who has supported this thesis work and has kept me inspired with his novel, insightful, and immense views on safety and engineering systems. Without his excellent guidance, creative suggestion and critical comments and persistent help, I would not fulfill my academic goal at the AAIT of AAU.

During my study, special cooperation and continual support has given by Ato Zalalem Asemu Design Team Leader at Ethiopian Railway Corporation Company, Ato Birhane Haileyesus Mechanical Engineer at ERC, Mr. Guo Yi Human Resource Manager at Shenzhen Metro Group Ltd Company and ato Neway Genene civil Engineer at AA LRT. Thus, I need to express my deep appreciation to all of them and many thanks for their positive and prompt cooperation.

I would like to thank all who responded to my interviews, which helped me in a great deal in my study.

Finally, I thank my father Kedjela Weyessa, my mother Tsehaynesh Mekonen , my brothers Sirika Kedjela, Amanuel Kedjela, Iyasu Kedjela and Israel Kedjela for their unreserved encouragement, continual support and love during my study.

ABSTRACT

Light Rail Transit 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 Ethiopia, the Ethiopian Railway Corporation (ERC) released a strategic vision to develop new LRTs in 2008, specifically focusing on two corridors, Ayat Adababay to Torhailoch and from Piazza (Areda Georgis) to Kaliti. With such rapid growth, safety is a growing concern in LRT projects; in fact, there have been two accidents over the past three years. In developing a new LRT 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 LRT 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 Control 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 LRT project in the AA is analyzed by this methodology. This methodology includes steps of conducting STAMP-based accident analysis, developing a safety control model of the LRT system in the AA based on lessons learned from the analyzed accidents, with a specific focus on the institutional structure. Thus, this thesis research concludes with specific recommendations about safety management in the project in the LRT, making a point that the proposed methodology can be valuable for the actual project processes as a "safety-guided institutional design" tool.

Table of Contents

Contents ***Page***

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABREVETIONS

AA	Addis Ababa
AA LRT	Addis Ababa Light Rail Transit
BR	British Railway
CAST	Causal Analysis based on STAMP
CFR	Code of Federal Regulations
CMS RA	Common Safety Methods for Risk Assessment
CNR	China National Research
CREC	China Railway Engineering Corporation
CRSC	China Railway Signal & Communication Corporation
CRSDC	Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.
CTC	Centralized Train Control
DVT	Driving Van Trailer
ERA	European Railway Agency
ERC	Ethiopian Railway Corporation
E-W	East- West
EU	European Union
FMEA	Failure Mode Effect Analysis
FMECA	Failure Mode and Effect Criticality Analysis
FRA	Federal Railroad Administration
FTA	Federal Transit Administration or Fault Tree Analysis
GCC	Gauge Corner Cracking
GNER	Great North Eastern Railway
IEC	International Electro technical Commission
IM	Infrastructure Manager
ISO	International Organization for Standardization
ITA	Independent Technical Authority
LED	Light Emitting Diode
LRT	Light Rail Transit
LRV	Light Rail Vehicle
MK4	Mark 4
MOR	Ministry of Railway
NDA	Non Descried Alarm
N-S	North- South
ORR	Office of Rail Regulation
QRA	Quantitative Risk Assessment
PSB	Power Signaling Board
RAMS	Reliability, Availability, Maintainability and safety
RCF	Rolling Contact Fatigue

R & D	Research and Development
RGS	Rail Group Standard
RSSD	Railtrack Safety and Standards Directorate
SMS	Safety Management Systems
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
SZMC	Shenzhen Metro Group Co., Ltd
TCC	Train Control Center
TOC	Train Operating Company
UIC	International Union of Railways
UK	United Kingdom

CHAPTER ONE: INTRODUCTION

1.1. Background of the Study

- **Railway accidents**

It is widely believed that railways are safe systems due to their technological maturity. However, there are still many railway accidents every year all around the world. Although Railway have had only three fatal accidents in their 50-year history, two of them occurred over the past three years as Railway systems in operation have grown. Specifically, in 2011, a collision of two 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 [1]. In 2013, a disastrous derailment occurred in Santiago de Compostela, Spain, killing 79 passengers (Santiago de Compostela derailment) [2]. The 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. These accidents have reminded Railway planners and operators of the importance and difficulty of continuously managing safety for a large-scale system.

- **Significances of system-based approach**

This thesis research focuses on how to manage safety risks of a LRT in its development as well as operating processes. Specifically, emerging LRT projects in the Addis Ababa 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 countries' 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, 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 Railway 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 [3][4]. 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 and safety-related interactions of entities involved in the industry; e.g., the International Union of Railways (UIC) more specifically defines a Railway as a complex system that is comprised of 10 different elements [5]. Another example of inadequate awareness of system complexity can be seen in CNN's editorial in July 2013 claiming about the Spanish Railway accident.

From these countries' accidents, Addis Ababa LRT projects planners' experience System attributes of Railway 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.

1.2. Problem Statement

It is broadly known that railways are the safest mode of land transport due to their technological maturity and involvements well educated and trained workers. However, there are still many railway accidents every year all around the world. The accidents of Railway is a not an easy, like others of land transport mode, it is a huge crisis for the economic development of the country, in addition to the injury of passengers, damages of the locomotives, coaches and etc. This may arise from different socio technical factors. Most of Railway companies in the world spend most of their time in finding the route cause Railway accident rather than preventing the Railway accidents. As a result, the safety control activities are inspection-based rather than prevention-based.

Ethiopia has commenced Railway operation in the mid of 2015 .for this Railway operation, There is no institutional safety control structure, which ensures the safety of passengers during Railway operation. In Railway operation safety should be first, unless things are going to be worst.

1.3. Objectives of this Thesis

1.3.1. General Objective of the Thesis

The general objective of this research is to propose a system-based safety control structure methodology based on lessons learned from past accidents for complex, large-scale, sociotechnical systems for AA LRT systems. The method used in this work is based on the STAMP (System-Theoretic Accident Model and Processes) theory proposed by Leveson [6][7]. 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 [7][8]. The details about this theory and methodology are explained in future. As a case study, the new Addis Ababa LRT project is then analyzed by the proposed methodology.

1.3.2. Specific Objectives of this Thesis

- Analyzing past accidents and acquiring system-based lessons from past accidents
- Transplantation of learned lessons from past accidents to AA LRT
- Draw a boundary and System development
- Developing a generic safety control structure model for the AA LRT
- Provide specific suggestion about safety management in the Addis Ababa LRT for project planners, based on the analysis results.

1.4. Significances of the Thesis

The expected analysis outputs of this research are as follows.

- key safety regulations applied to the AA LRT are also identified
- Generic safety control structural will be developed for AA LRT
- Clarify safety responsibilities of all safety-related organizations involved in the AA LRT including their interactions and etc.

1.5. Scope of the Thesis

The main focus of this 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. But, the interpretation of "institutional level" in this research is described in detail. So, 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.

1.6. Structure and Contents of Thesis

The thesis is organized in six chapters. Chapter one begins with an introduction and background of the research. Chapter two contains a literature review that discusses the fundamental concepts of System Theoretic Accident Model and Process. This chapter gives theoretical background for the thesis work. It also includes traditional risk analysis tool, safety and System Theoretic Process Analysis and Proposed Methodology for this research paper.

In chapter three, Accident analysis has been conducted on the two fatal accidents of Hatfield Train Derailment and Wenzhou Train Collision, in which major lessons learned from these accidents. Chapter four is about the factors considered during transplantation of the learned lessons from past accident to AA LRT project.

In the fifth chapter, an attempt is made on system definition and model development for safety control structure of AA LRT, based on lessons learned from past accidents by developing a system boundary on the Research and Development, Design, operation and Maintenance of locomotives of AA LRT.

Finally, in the last chapter, the finding, the conclusions and recommendations has been presented

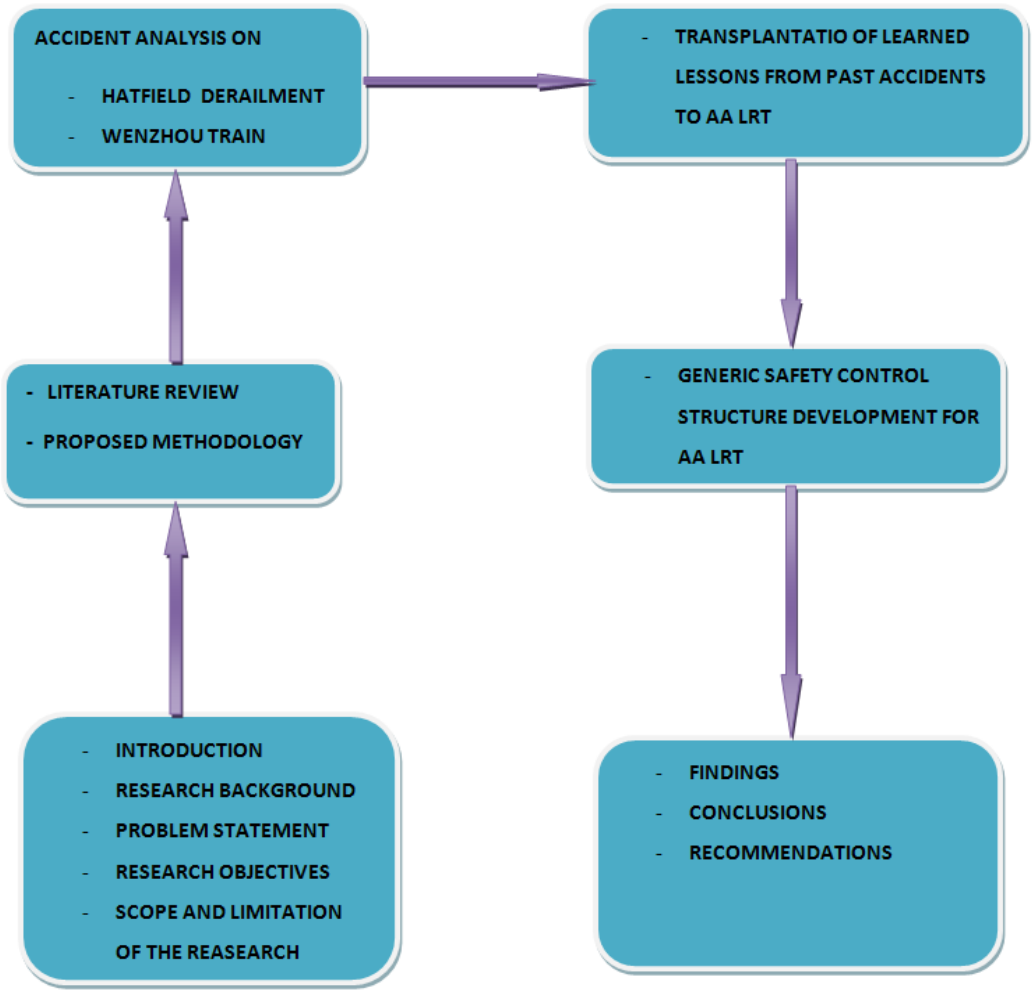

Figure 1.1 Structure of the thesis

1.7. Summary Introductions

1.7.1. Addis Ababa Light Rail Transit

An LRT system is defined as a "specially built line for operation of at 80km/h [9]. The project is located in Addis Ababa, the capital of Ethiopia, which was the location of the head office of African Union. The altitude of the plateau is 2,400m. With an urban population of over 3,400,000, it takes 24% of the total population of Ethiopia. The urban area is 530.14 km2 and the density reached 5,607.96/km2 to effectively solve the problem of urban transportation esp. that of the downtown area, the government of Ethiopia decides to build a light rail in the city of Addis Ababa. Currently this project has planned two lines, the east-west line and the south-north line. About 3 km is the sharing section for both E-W route and N-S route, which has the greatest passenger current [9].

The east-west line phase I project starts from Ayat and ends at Torhailoch. The total length is 17.4km. There are 22 stations, among which 5 are elevated stations, 1 underground station and 16 ground stations. The depot locates at the west ends of the project. The control center (commonly used by both lines) is temporarily [9]

The south-north line phase I project starts from Menelik II Square and ends at Kaliti. The total length is 16.97km. There are 22 stations, among which 9 are elevated stations (5 common stations at the common line), 2 underground stations and 11 ground stations. The depot locates at the south end of the project.

CHAPTER TWO: LITERATURE REVIEW

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. [7]
- **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 [10]
- **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. [8]
- **Hazard Level**: The combination of hazard severity and likelihood of hazard occurrence. [7]

- **Hazard Exposure**: A system state that a hazardous state exists.

- **Causal factor**: One or several mechanisms that trigger a hazard [11]

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 [8]. Specifically, this thesis refers to a system state that has an unsafe control action(s) and its causal factor(s) identified in the situation in the following Chapter, which could lead to an accident, as a safety risk of the AA LRT. Definitions of an unsafe control action and a causal factor are described in Section 2.1.4 and 2.1.5.

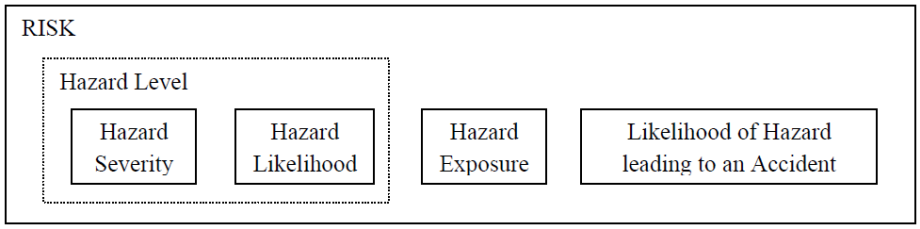

Figure 2.1 Components of risk [8]

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 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" [12]. This standard was replaced with ISO 310006 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 [4][5]. 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 AA LRT, and "hazard/risk identification" refers to identifying causes of hazards and heir causal relations in the project processes.

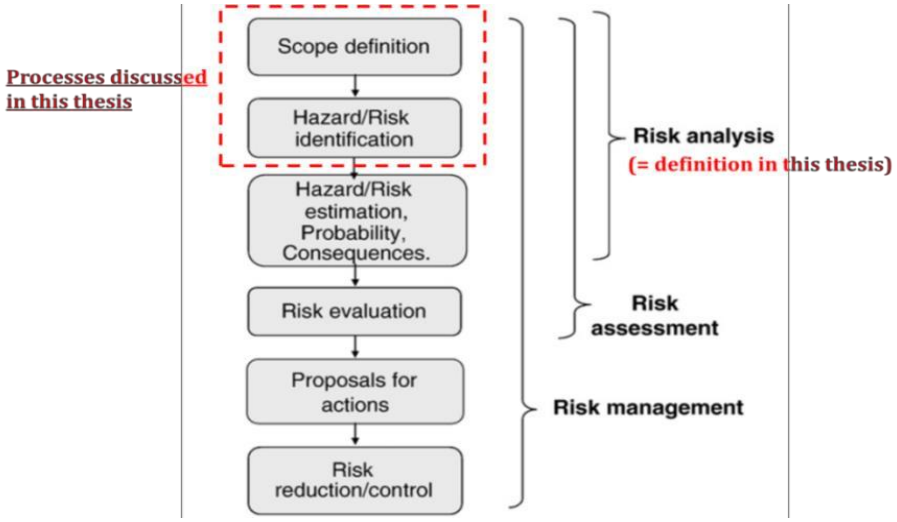

Figure 2.2 Discussed processes in this thesis as risk analysis in ISO 60300-3-9 [3]

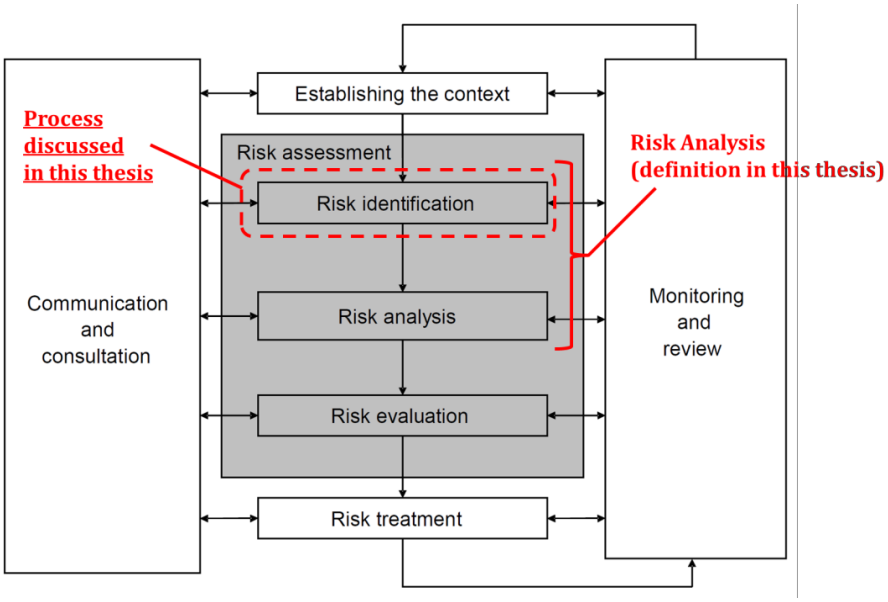

Figure 2.3 Discussed processes in this thesis as risk analysis in ISO 31000 [13][4]

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 [14]. 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 [4]. ISO/IEC 31010 compares applicability of 31 different risk assessment methods [15]. Among them, Quantitative Risk Assessment (QRA) methods such as FTA (Fault Tree Analysis) [7]–[13], FMEA (Failure Mode and Effect Analysis) [11][13][14], FMECA (Failure Mode and Effect Criticality Analysis) [16][17], and PRA (Probabilistic Risk Assessment) [18][19] have been widely used in various applications.

In order to identify safety risks of systems, it is important to understand how an accident occurs [4][5]. Each risk analysis method above is based on some accident model that describes the theory of accident causation [7]. 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 [8]. 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 [4]. 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.

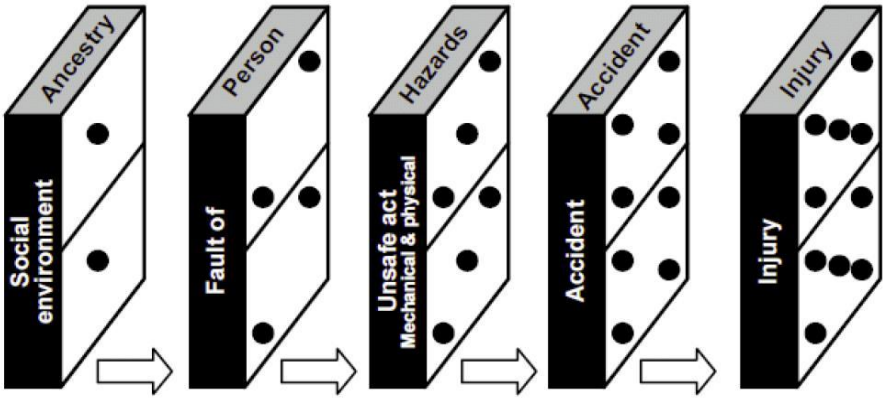

Figure 2.4 The Schematic of the *Domino Accident Model* (originally from [5])

The Swiss Cheese Model, which was proposed by James Reason in 1990 (Figure 2.5), is another event- chain accident model [20]. 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" [21].

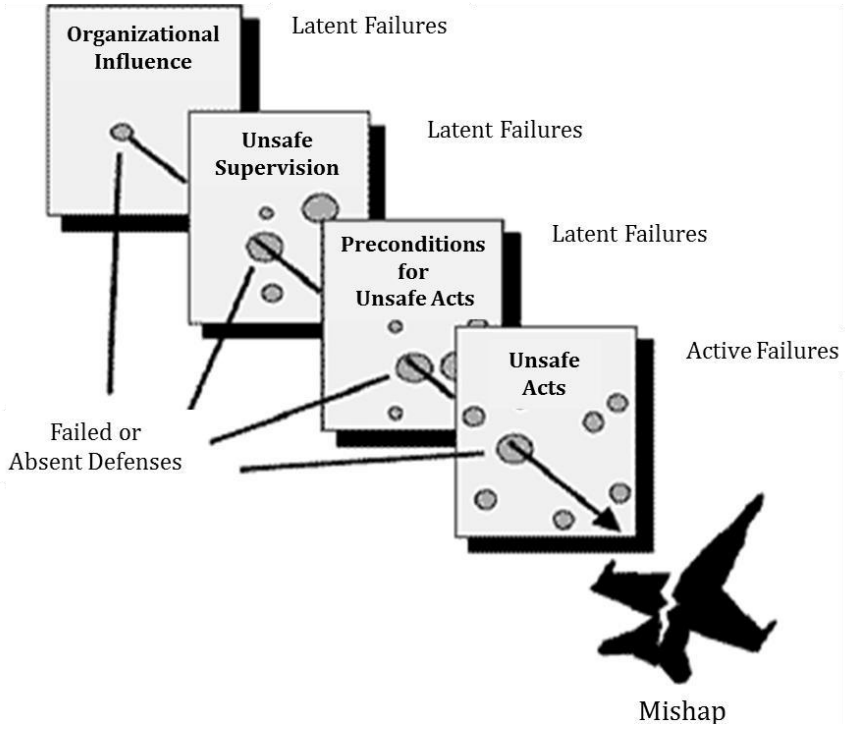

Figure 2-5 The Schematic of the Swiss Cheese Model [7]

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, socio technical systems, arguing the necessity for a broader view of accident causation and indirect or non- linear interactions among events [11][12]. LRT systems can be regarded as complex socio technical systems in that they are composed of a 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 socio technical 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.

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 [22]. 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 [22].

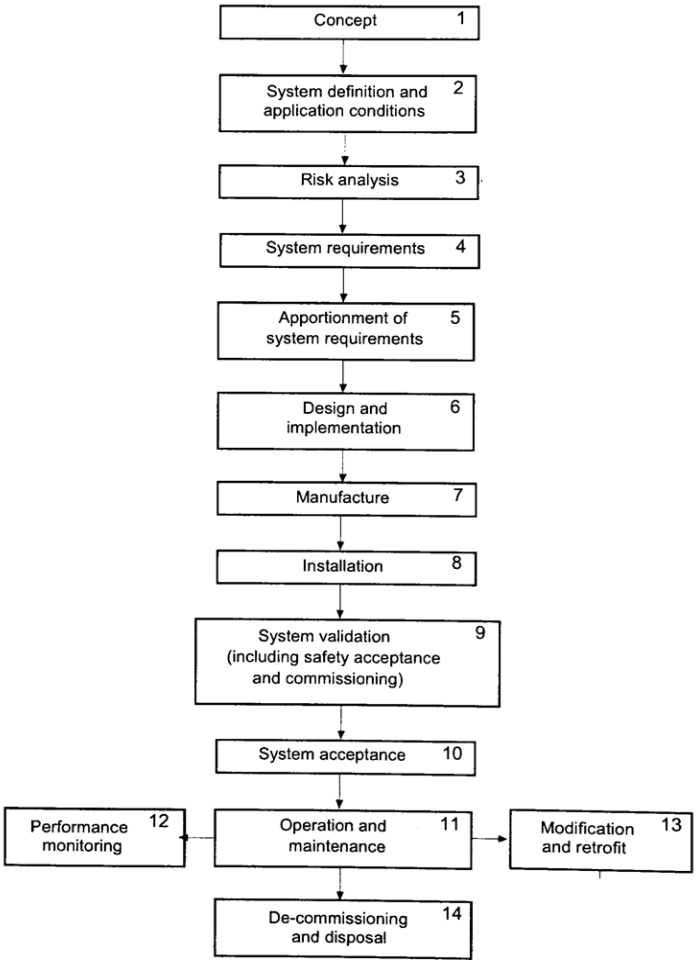

Figure 2.6 System life cycle defined in RAMS [23]

- **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) [6]. ERA has provided various methods and frameworks for the program. Common Safety Methods for Risk Assessment (CSM RA) is one of the core components in this SMS approach, aiming at harmonizing differences of risk assessment in changing or newly developing

railway systems among the integrated railway area [21]. Figure 2.7 represents the risk management processes in CSM RA; risk analysis plays an important role in these processes.

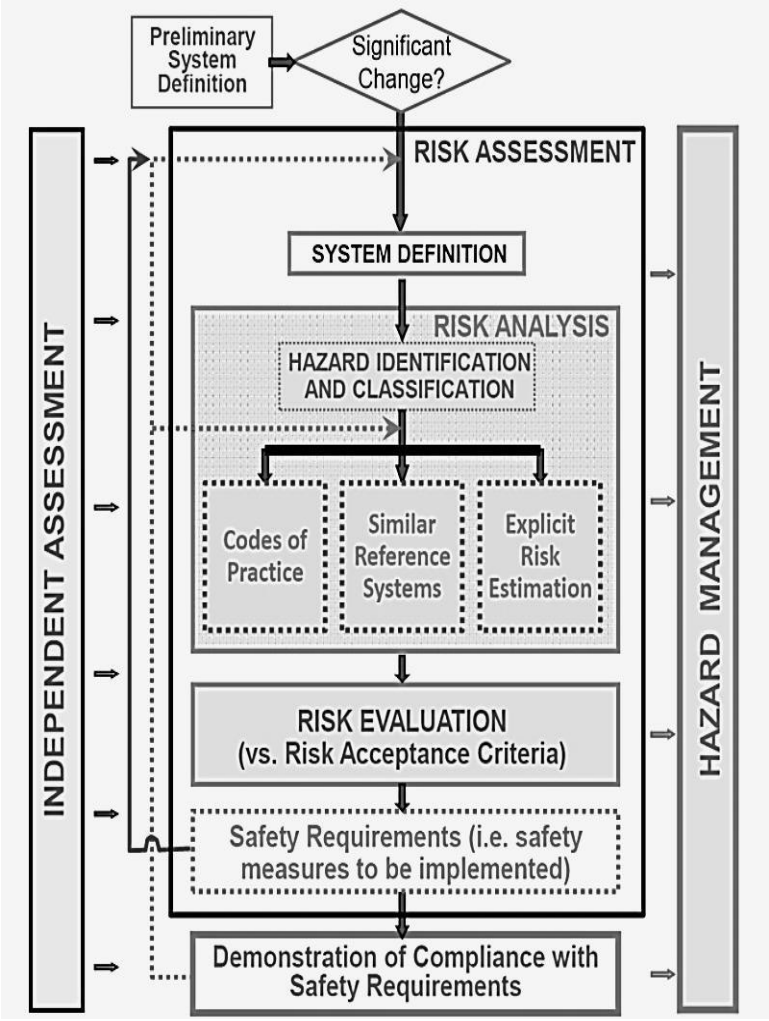

Figure 2-7 Processes in CSM RA [24]

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 [6][7], 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" [7]. In this section, key terminology and perspectives in the 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 the following Sections 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 [21]. 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 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 depends partly on the original design and partly on effective control over operations." [3] 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 [5]. 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.

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.

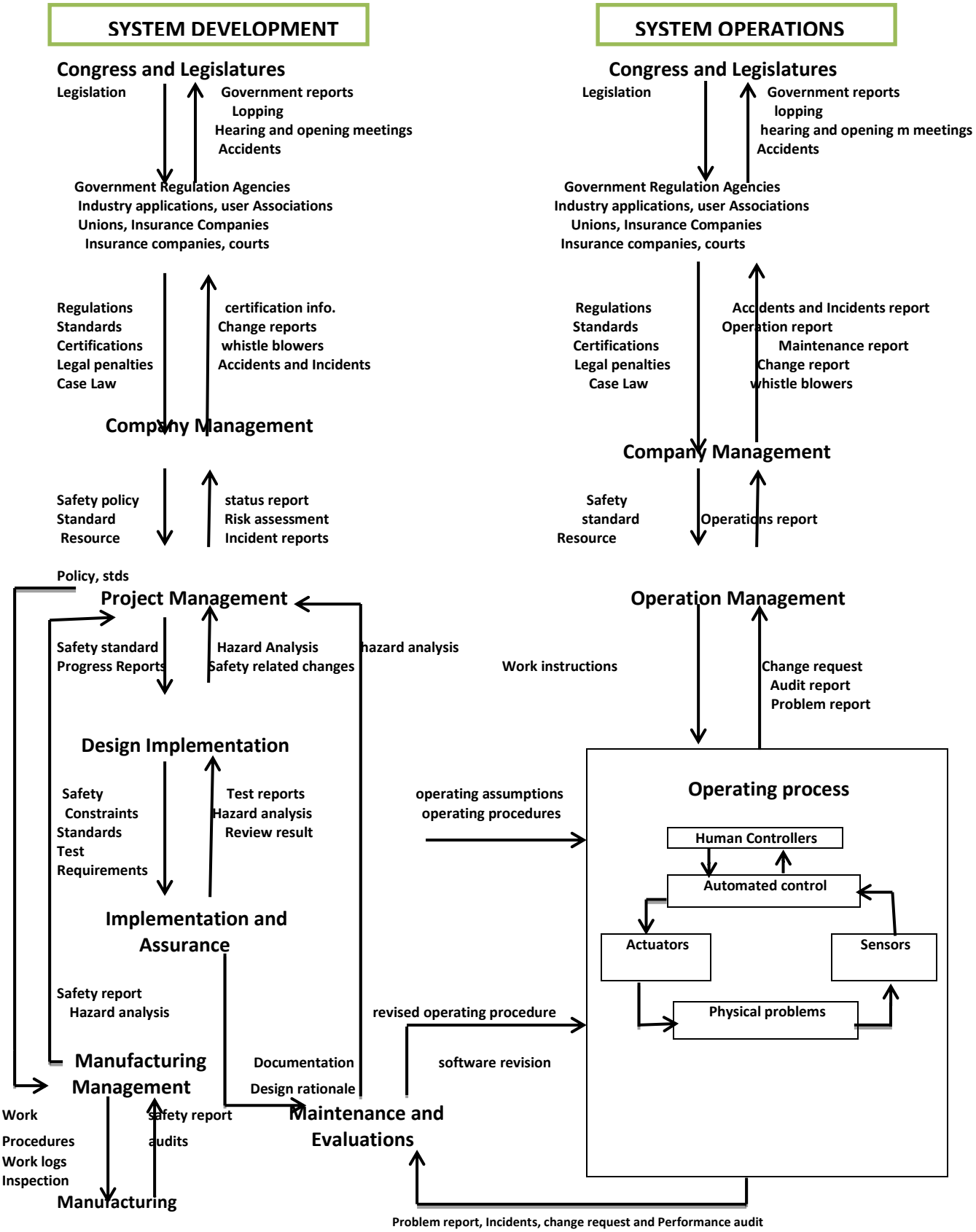

Figure 2.8 General Sociotechnical Safety Control Structures [7]

- **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.

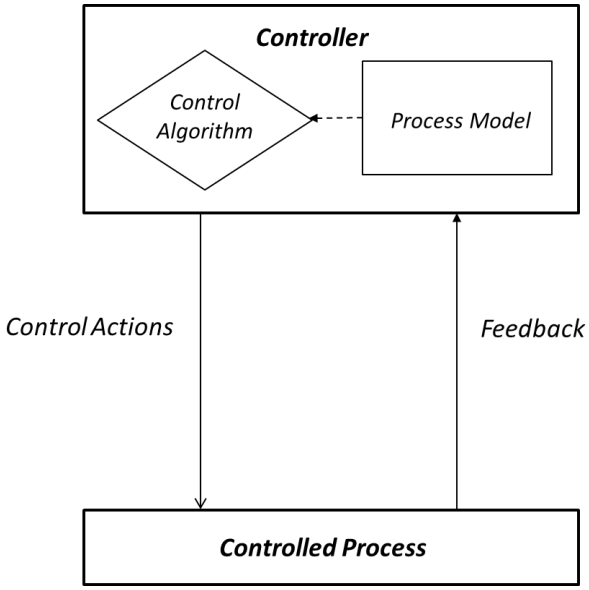

Figure 2.9 General control loop [7].

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 [21]. 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 [7], 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)**

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	Unsafe action	Incorrect	Stopped Too Soon
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 [7]. 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.

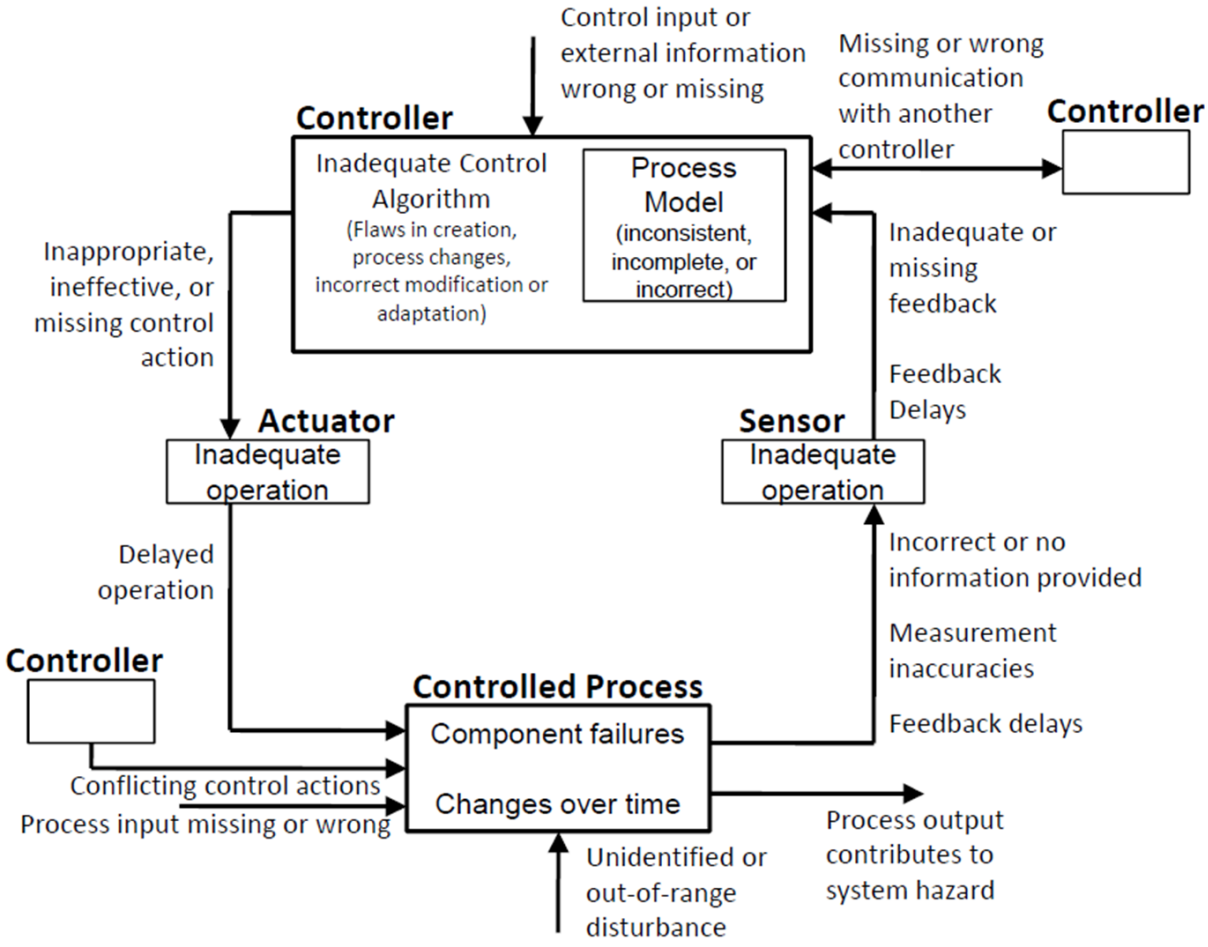

Figure 2.10 Guidewords for identifying causal factors [7][18]

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 [7].

(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 is 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.
- Inconsistencies 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.

2.1.6. Causal Analysis based on STAMP (CAST)

CAST is a STAMP-based accident analysis method, which is also proposed by Leveson [7]. 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 [7]:

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.

2.2. Proposed Methodology

This research proposes the following analysis methodology. This section explains specific processes in the following steps in the context of the case study about the AA LRT 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

2-1 defines a system and develops a generic model representing a typical railway industry with a particular focus on the institutional level.

2-2 incorporates the findings in Step 1-3 into the generic model.

2-3 consider institutional structure 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.

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 2013

2) Wenzhou Train Collision in China in 2011

In the following Chapter 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 AA LRT, 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 LRT model representing a typical LRT model is developed. The identified system requirements/constraints in Step 1-3 are integrated in this process. This generic LRT model can meet all of the system requirements and safety constraints, including the "lessons" identified in Step 1. The control model is developed with a particular focus on the institutional levels.

CHAPTER THREE: 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 [8][24]. 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) [18] and "Broken Rails," a book authored by C. Wolmar [19]. The overview of the accident is shown below [18]

- 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 C l91 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) seen on November 20, 2014.

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. 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.

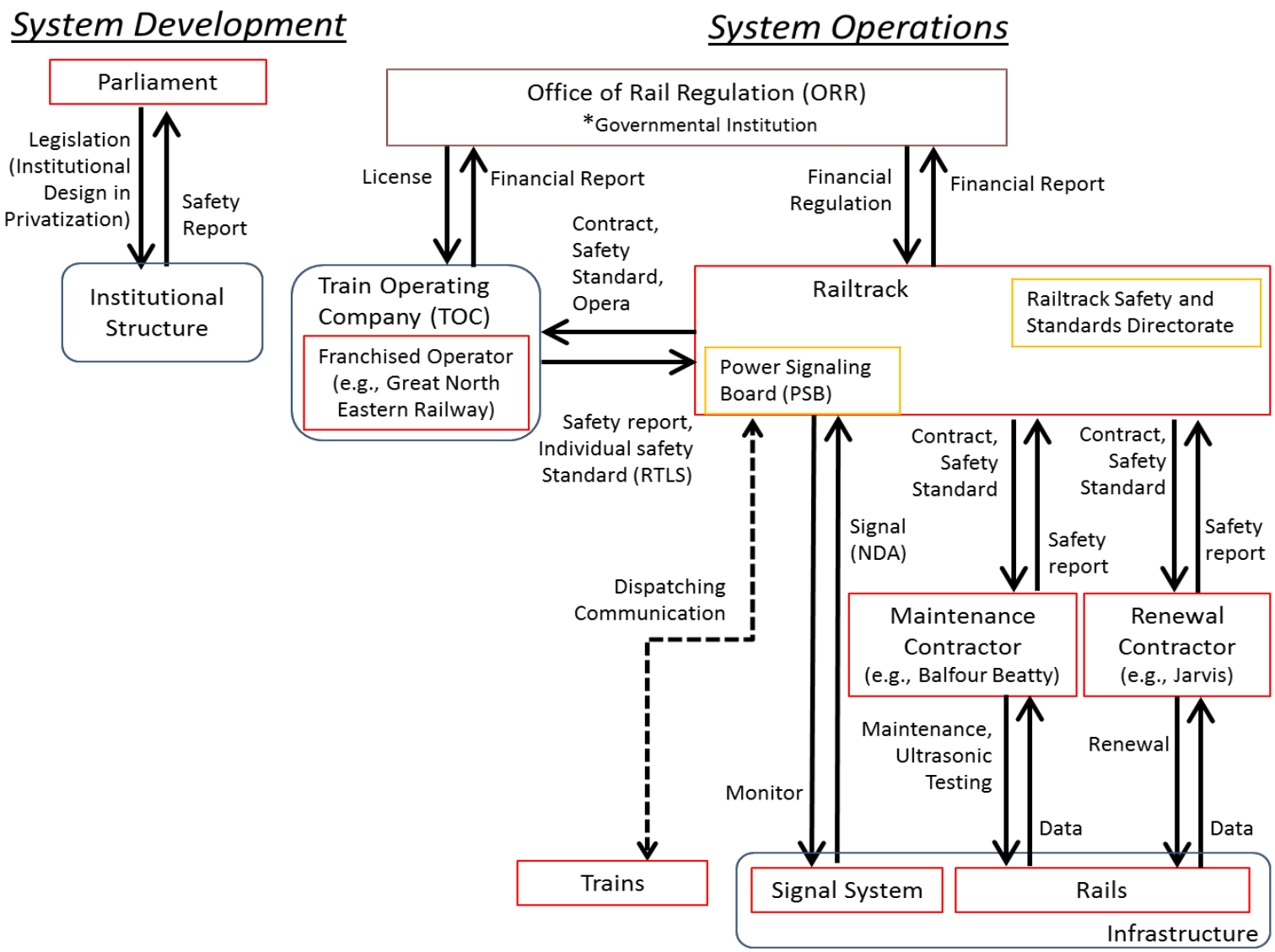

Figure 3-2 The safety control structure of the UK rail industry (1997-2000)

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 GS 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 perating 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. Rail track did not comply with standards; they did not implement temporary speed restriction, and did not replace the rails within six months.
iii. Rail track 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, Rail track 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 (Rail track), 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 Rail track 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, Rail track should have tackled this issue more proactively.

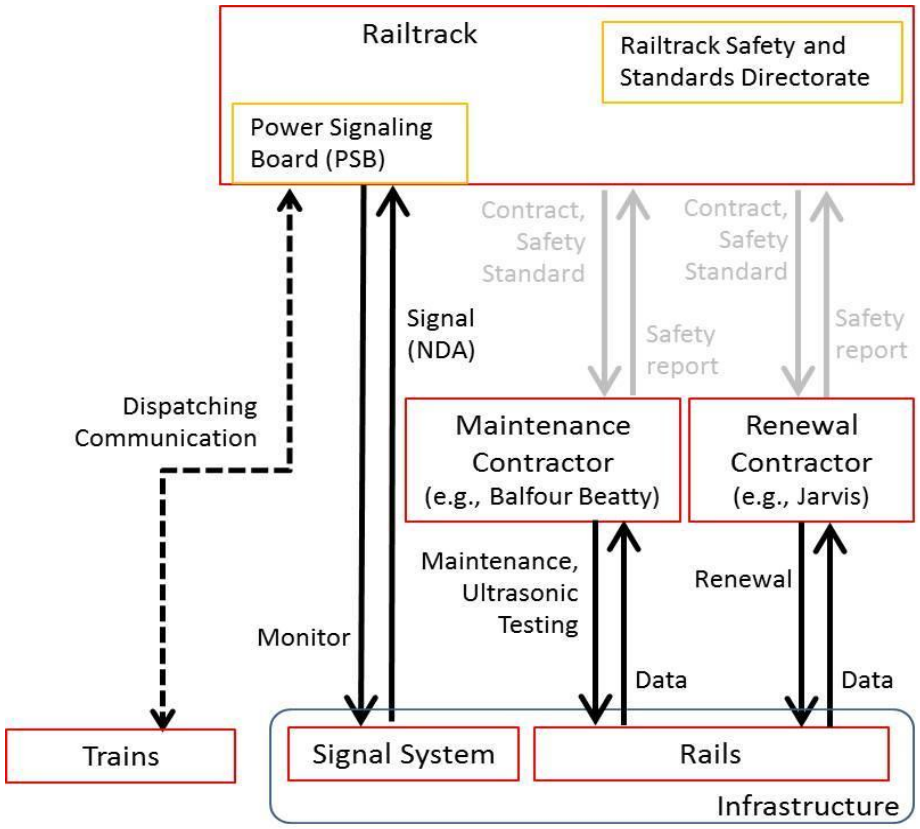

Figure 3-3 Control Structure (Maintenance and Operation) [11]

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.(Rail track) • Inadequate implementation of maintenance/renewal (maintenance contractors) • Inadequate judgment on maintenance data. (maintenance contractors, Rail track) • Inadequate compliance with regulation (Rail track) • Inadequate monitoring of control signals (Rail track)
Process Model Flaws
• Inadequate understanding of the rail maintenance method to achieve safety (maintenance contractors, Rail track) • Inadequate understanding of the symptom and risk of RCF (Balfour Beatty) • Inappropriate timing of maintenance/renewal (Rail track) • Lack of risk awareness of NDA (Rail track)

- **Company Management Level Analysis (Rail track)**

The inadequate management by Rail track is the most crucial factor in this accident. The safety control between Rail track 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 Rail track's management, and managerial decisions of Rail track were not adequately safety-oriented. For example, Rail track drastically reduced the number of maintenance workers, and mitigated safety standards. Also, Rail track made contract with a consulting company, McKinsey & Company, Inc., and Rail track 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, Rail track 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, Rail track 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, Rail track 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, Rail track 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, Rail track did not implement temporary speed restriction or replace the rails at an earlier timing.

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

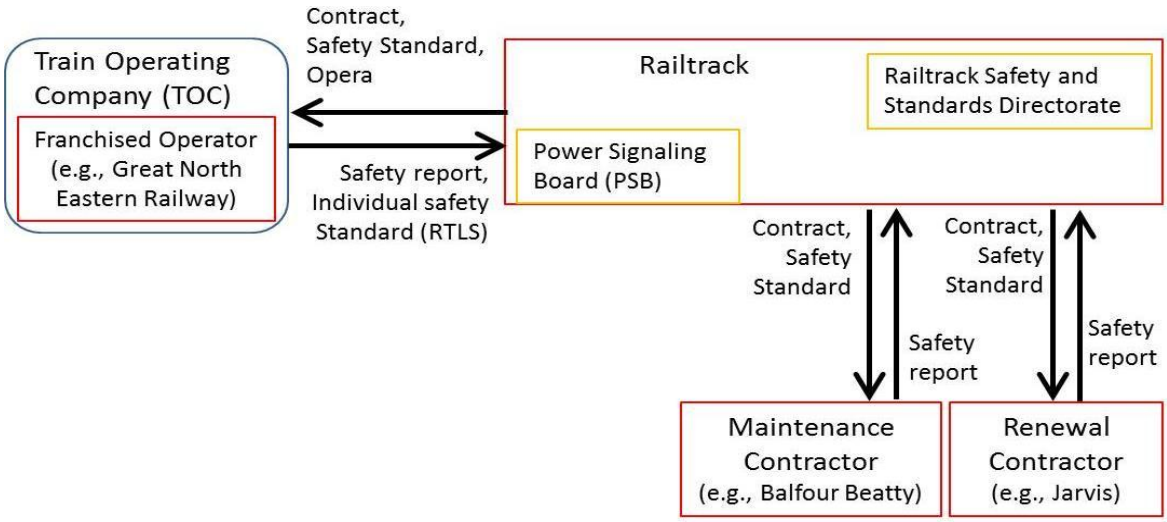

Figure 3-4 Control Structure (Corporate Management of Rail track) [11]

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 Rail track 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, Rail track was the only one infrastructure owner. • Rail track, instead of an external regulatory organization, was in charge of maintaining industry safety standards. • After the privatization, the profitability of Rail track 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
• Rail track did not understand the impact of changing standards. • Rail track did not understand the skill level of contractors.

- **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 Rail track respectively, so Rail track needed to communicate fluently with multiple operators of different companies to coordinate them under the same operation standards. Similarly, 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 Rail track headquarter did not initially realize that Balfour Beatty was not in compliance with the safety standards. Also, Rail track did not realize that some workers in Balfour Beatty were not well trained to detect rolling contact fatigue; thereby, Rail track did not know in which location the rails have serious damages. Another critical flaw in communication is that Rail track 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; Rail track 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**

In UK, 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 riskier 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 o 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 Rail track 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 Rail track; Rail track 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 are to the institutional level in the hierarchical control structure. As discussed in each step, there 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 has been developing their network at a drastic rate. [25]. However, its rapid growth had been sometimes controversial in terms of quality of construction and operational safety. The Wenzhou Train 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 Railway industry has a new industrial structure for 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 AA LRT.

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 [2][3][26][27]. 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 train D301 rear-ended another 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 [28].

- 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 top 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, 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.
- 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 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 closes to section 5829AG, and says: "Be careful D301! D3115 is ahead of you! Be careful!" The line goes dead. Train D301 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

Figures 3.5 Wenzhou train collision
[http://upload.wikimedia.org/wikipedia/en/0/0d/Wenzhou_PDL_wreck_at_night.jpg]

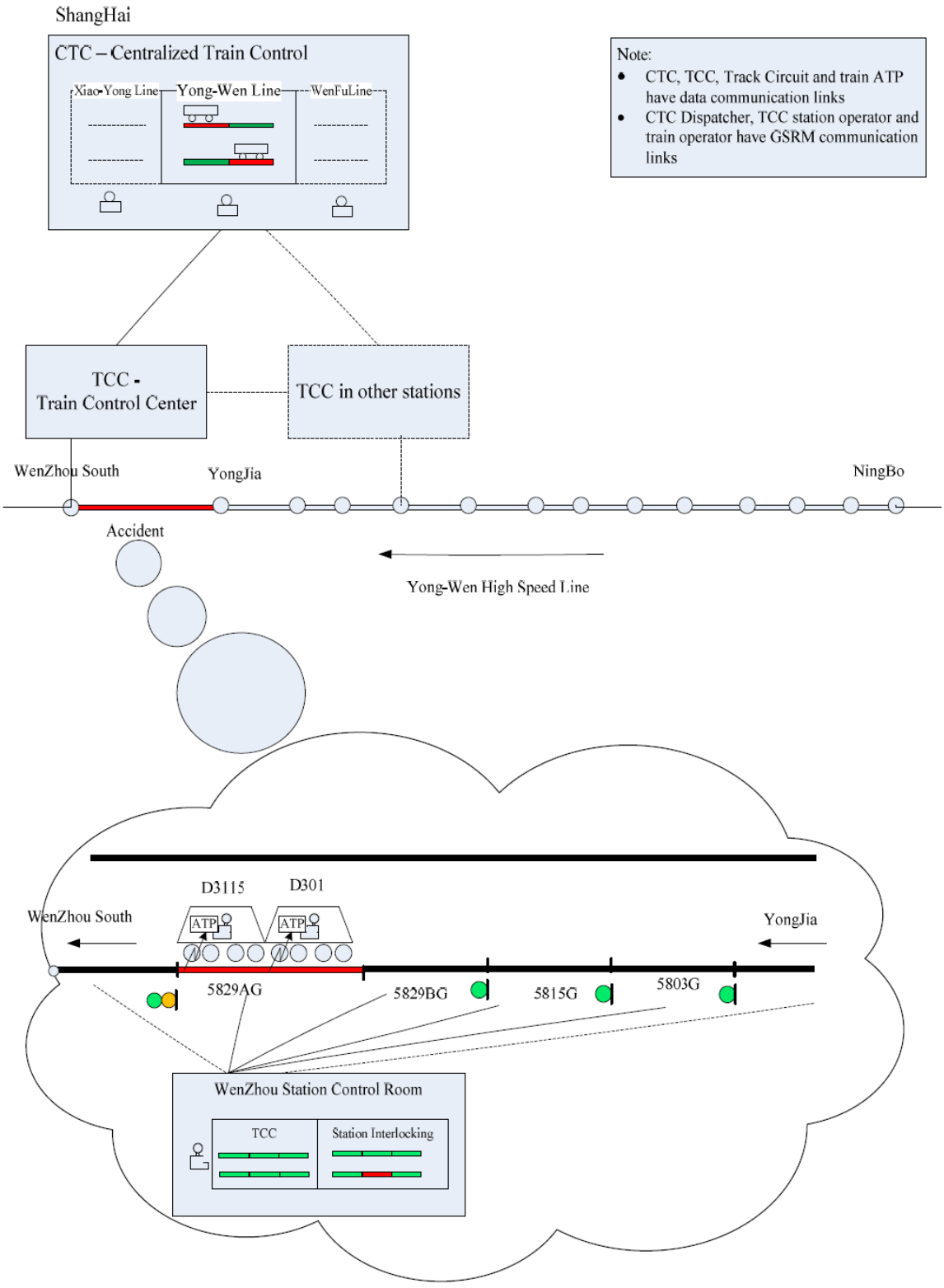

Figure 3.6 The schematic of the accident site and the control system [4]

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 [28].

- 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 [3][4]. 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 Railway industry can be regarded as vertically integrated.

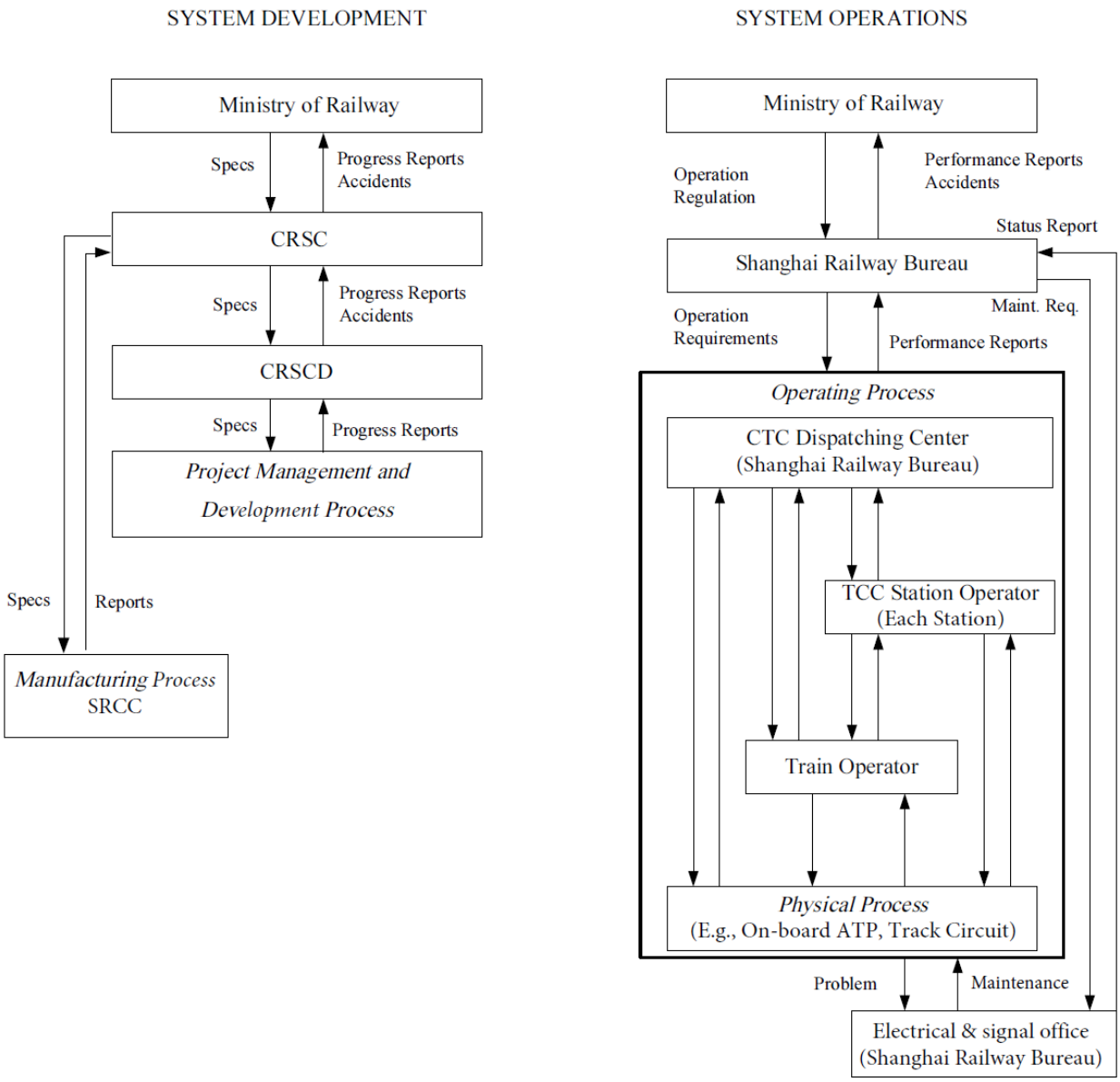

Figure 3-7 Safety control structure of the control system in the Chinese Railway [3]

Table 3-4 Components of the control system and their responsibilities

	Main Agencies in Chinese Railway Industry	Responsibility in the System
System Development		
	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 [3][4][28].

- **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 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 was warned that delays would cut their bonuses [29]. 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 [29], 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 Railway 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.

▪ **Certification**

The certification given to CRSC by MOR was not based on thorough inspection or testing, and Suo and Dong suggests 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 [29], 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 AA LRT, 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 Railway model in Chapter 5.

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 a 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 AA LRT in Section 4.1 as system-based lessons from past accidents.

CHAPTER 4: FACTORS CONSIDERED DURING TRANSPLANTATION OF THE LEARNED LESSONS FROM PAST ACCIDENT TO AA LRT

4.1. Current situation of AA LRT Project

The project of the AA LRT is still on the stage of construction, and the operation is the next step. However, as many stakeholders have already been discussing, there is no safety control structure for the institutional structure of this project. So, there is nothing explanation of the existence of safety control structure of AA LRT project. 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 and finally develop the generic safety control structure, which will save AA LRT from hazards that lead to accidents in its lifecycle.

Currently, the AA LRT project is under constructions and it is at the edge of finalizing by Chinese company, China Railway Engineering Corporation (CREC).

The China CNR Corporation Limited (Stock No. SH601299) is a company approved by China Securities Regulatory Commission for;

- research,
- development,
- design,
- manufacturing,
- refurbishment,
- Overhaul
- Maintenance

And service of Rolling Stock of Addis Ababa Rail Transit project.

Shenzhen Metro Group Co., Ltd (SZMC) is also another Chinese company which is responsible for operation, development and comprehensive utilization of Addis Ababa Rail Transit project.

4.2. Factors Considered during Transplantation of the Learned Lessons from Past Accident to AA LRT.

This learned lessons from past accident transplant process considers the following factors at Addis Ababa city;

- **Traffic engineering**

In order that the LRT system can operate without being delayed by traffic congestion, segregation of its 'right of way' from the highway system is essential. This is achieved by installing the tracks and stations within the median areas of urban dual-carriageway highways where adequate reserve width exists. If the road width is inadequate, the LRT tracks can be located in tunnel below the roadway, or on viaduct above it.

- **Urban Development**

Future proposals for the city include the redevelopment of industrial zones; reconstruction of residential blocks; the creation of large public, cultural and business centers; development of the urban infrastructure and the formation of new recreation zones. The introduction of LRT will greatly assist with the developments particularly where the new system can be integrated with them. A breakdown of the present transit demand and modal split in Addis Ababa is provided in the Report, with detailed plans of the existing urban road network.

- **Stations**

LRT stations will be located at-grade, below ground and on structures. Despite the variety of the locations, standard details and a common theme should be introduced to link all the station structures to the LRT system. Some overseas examples of different stations are provided in the text and details of the ancillary buildings and equipment are described. The exciting possibilities for station sites when developed as commercial enterprises, with resulting financial advantages for the LRT system, particularly at "Transit Hubs", is described further under this heading. The heavily used at-grade stations and all stations on viaducts will be reached by overhead footbridges. Underground stations will have subway accesses. The at-grade stations will also have pedestrian crossing access for use by the handicapped, the infirm and others.

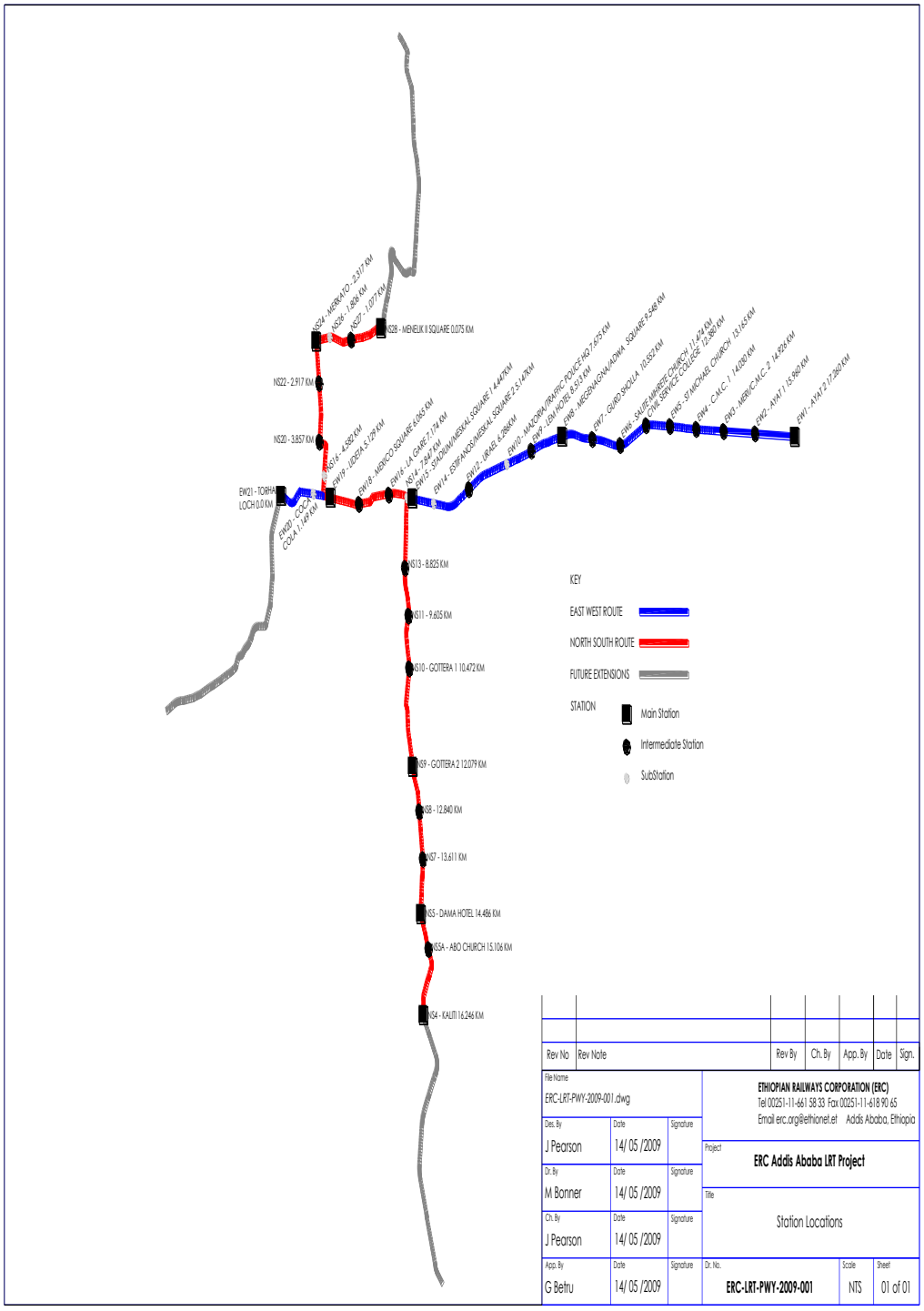

Figure 4.1: stations of AA LRT [33]

- **Depots**

The Depots are located near the extremities of the East-West line, and at the southern end of the North- South Line. The Depots will provide facilities for the servicing, repair, maintenance and stabling for the Vs. The main workshop will be equipped with specialized machinery to maintain vehicle components such as wheels, bogies, brakes and electronic controls. The Depot areas should allow additional space for an increase in the stabling sidings as the number of LRVs increases. 12. Depots (Maintenance and Stabling Facilities).

The Depots (Maintenance and Stabling Facilities) which are located near Torhailoch (around station E_W) and Kaliti area (around station N_S) will comprise:

- Stabling Tracks
- Operations and Maintenance Building
- Gatehouse
- Fire Protection Pumping Station
- Traction Power Substation
- Operation Control Centre
- System Administration

- **Climate**

Addis Ababa has a mild Afro-Alpine/warm temperate climate. The range of temperature in the year is between 10°c to 25°c. It receives an average annual rainfall of 1200mm of which 80% falls in the months of June to September. Though the gradients help in quick run off of surface water, still surface drainage has remained as a major problem in large areas of the city.

- **Transport**

The main transport facilities in Addis Ababa are Bole International Airport, the road network, the Anbassa Bus Service, the mini-bus taxi services, and the number of rapidly increasing private motor vehicles. Anbassa Bus Service and Mini-bus Taxi Service are the backbone of Addis Ababa's transport system. They provide limited mobility for the population but suffer from many constraints. Access to finance; an ageing bus fleet; inadequate infrastructure; an adverse external operating environment particularly due to severe traffic congestion; extensive competition, etc.

Have restrained the growth and efficiency of the various systems. They require rejuvenation and their route structure and service pattern rationalized. Future public transport capacity must be supplemented by medium and large capacity vehicles preferably incorporating some modern technology.

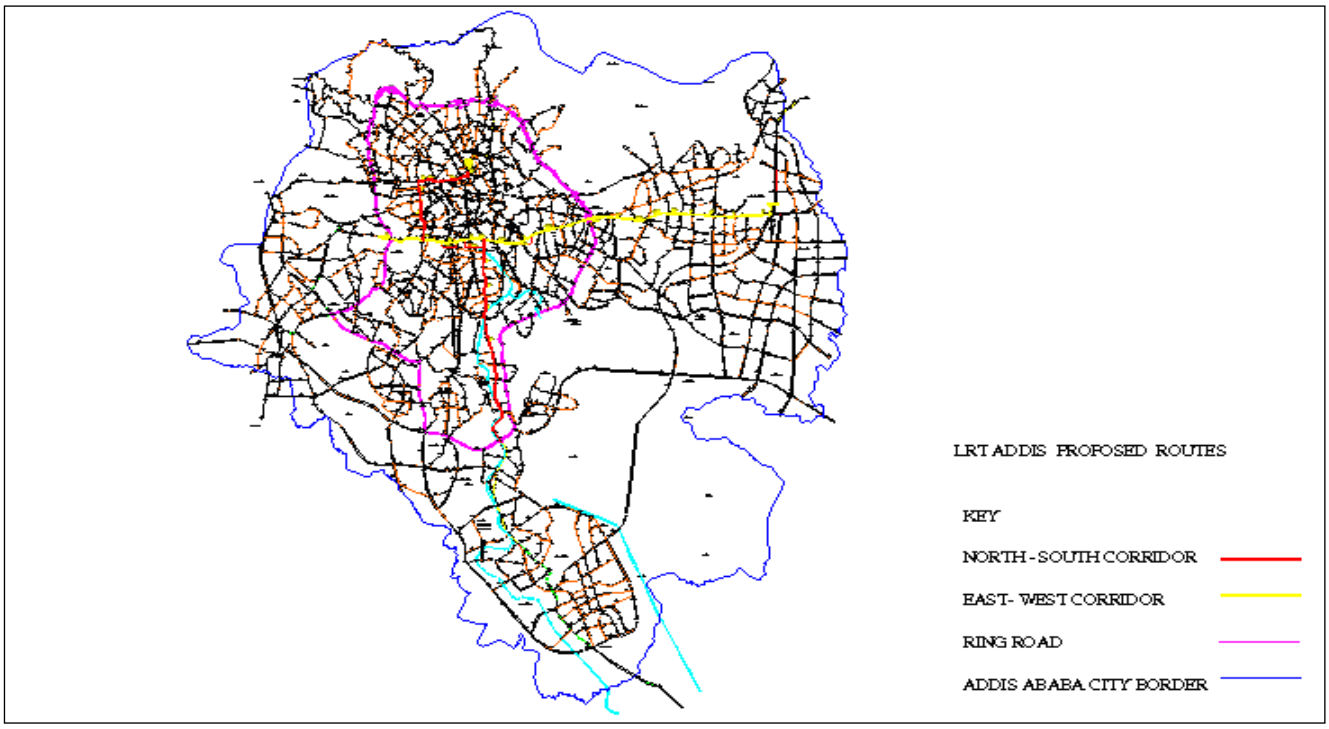

Figure 4.2: Addis Ababa City Road network Integrated with the proposed LRT routes. [33]

- **System technology**

The technology of the Addis Ababa system shall be consistent with that used in cities in Europe, Asia or North America while at the same time being compatible with the specific conditions of Addis Ababa.

The LRT system shall comply with the following:

- Provide a fully accessible system with at least a 70% low floor modern LRT vehicles which will provide access to all passengers including those with disabilities or old persons. Accessibility provision will incorporate the requirements for emergency services.
- Modern 30m long electrically powered rail vehicles, which can be formed into trains of up to three vehicles allowing for expansion of service as demand is expected to grow.

The latest technology in signaling and control systems to provide on time performance and service to the people of Addis Ababa.

- **Operations**

By its first years of full operation (with 41 LRV of each 286 capacity for an operation of 16 hours per day at an average speed of 21.6km/h) it is expected to attract up to 4.05 million passenger kilometers per day. By year 2025 (with 82 LRV of each 286 capacity for an operation of 16 hours per day at an average speed of 21.6km/h) an estimated 8.10 million passenger kilometers per day.

It will offer an initial 6 minute service frequency during the peak period and 10 minutes off peak.

It will serve the suburban neighborhoods of Ayat, Kaliti and Torhailoch. Until further extensions to the farthest suburban areas of Legetafo, Akaki and Sebeta respectively which will be implemented under Phase 2 of the project?

- **Utilizing Context**

Altitude: =2500m

Temperature: +100—+280 degree Celsius

Relative Humidity: 95%

The atmosphere around the rolling stock equipment has mild acidity and contains some light dusts. And the rainfall sometimes in Addis Ababa is quite great. Therefore the equipment should be able to bear heavy wind, high temperature, high humidity, high vibration, heavy noise, rain, and frost, the contamination from detergent, mildew, dust, rodent infestation and fires

- **Communication and Signal System**

Following the safe, economical and practical principles, and the characteristics of LRT in Addis Ababa, this design chooses a reasonable communication and signal system. The communication system consists of digital transmission net, telephone, wireless communication and the relevant affiliated facilities. Main line Station interlocking system would be adopted for the proper interlocking and the Route control between the switch track section, signal and the switches on

the main Line; the computer interlocking system would safely work for the interlocking and route control of the depot; the crossing signal control system would realize the priority of tramcars and matching of the urban transportation signal system. The central working station in the control center (shared by both the east-west line and south-north line) would monitor and simply dispatch the signal facilities in order to improve transportation efficiency, lower the operation cost, improve the working condition, and service level for better social and economic benefits.

The maximum and minimum intervals between stations are 1.972km and 0.435km respectively. The average station interval is 0.773km.For E-W line, Ayat Depot is set near to the terminal of east end; for N-S line, and Kaliti Depot is set near to the terminal of south end. A control center for both the E-W line and N-S line is set at depot on the N-S line.

- **Design scope communications**

Communication system design includes preliminary design of communication systems within the scope of the line in length of 16.998km, 22 stations, one depot and 11 substations (including mixed traction and step-down substations, following substations and step-down substations) for Addis Ababa E-W (Phase I) Light Rail Transit Project, and the line in length of 16.689km, 22 stations, one depot, one control center (including a common rail section of 2.662km long and 5 common rail stations) and 9 substations (including mixed traction and step-down substations, following substations and step-down substations) for Addis Ababa N-S (Phase I) Light Rail Transit Project.

- **Telephone System**
  - **System functions**

Telephone system consists of telephone business and non-telephone business, and it provides business contact between management department, operating department and maintenance department and can interconnect with local public telephone network (the interconnection is excluded in the scope of the Project). To sum it up, the functions are as follows:

- It provides the users with telephone call between internal users of the light rail.
- It provides the users with local telephone calls and national and international long-

distance calls after the interconnection with local public telephone network.

- It provides the users with voice mail service.
- It provide the users with all kinds of new telephone services, such as abbreviated dialing, hot line service, outgoing call barring, do-not-disturb service, searching of malicious call, wake-up service, call forwarding no reply service, absent subscriber service, registered call, call back, call transfer, call waiting, three-way calling, etc.
- It provides the users with service of voice channel fax and voice channel data through analog subscriber line.
- It provides all-around billing functions: Charge the calls of users with external call authorization after interconnection.
- It is embedded with maintenance management functions: Billing management function, maintenance management function for office data, user data, software and equipment, telephone traffic statistics function, and failure diagnose function.

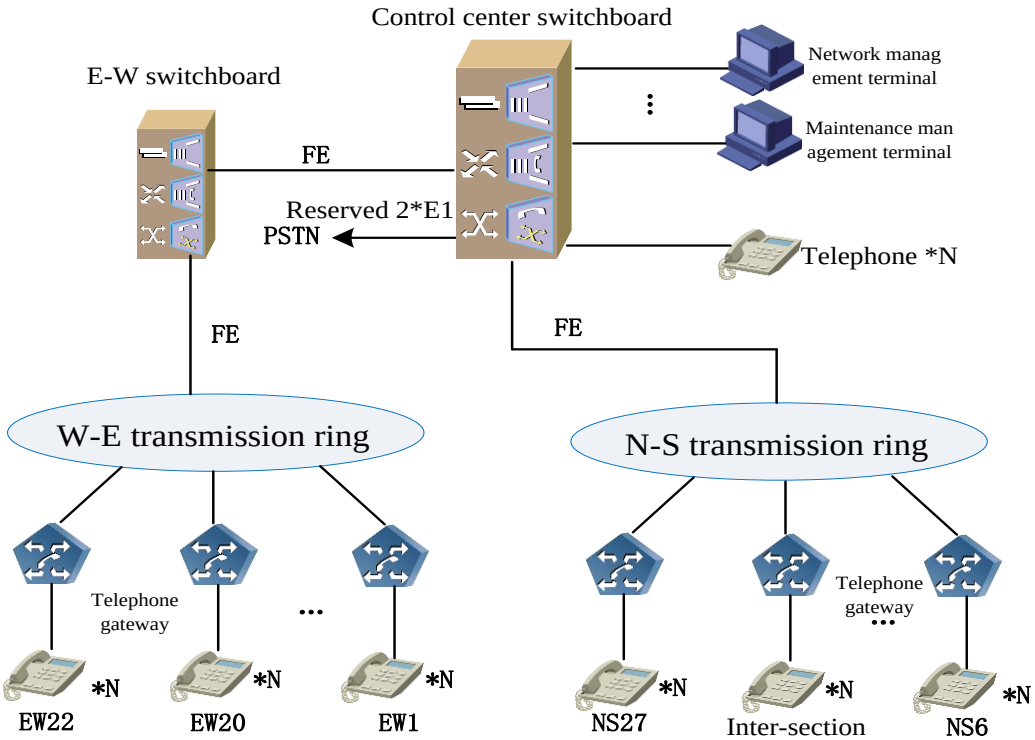

Figure 4.3 Schematic Diagram of Telephone System [31]

- **Radio Communication System**

a) System functions

Radio communication system is an important supporting measure to ensure traffic safety, to increase transportation efficiency and management level and to improve service quality. This system provides radio communication services for all the related users in the control center and the depot, including dispatcher, driver and staff, operating personnel, site personnel, etc. The radio communication system has the following functions:

1) Dispatchers and radio subscribers and radio subscribers between radio subscribers can communicate directly, and there are selective calling, group calling, and general calling and broadcast in response to business contact of different subscribers.

2) Record and search the call conversations of dispatchers.

3) Emergency call (insert) function.

4) System network management (saving and monitoring) function.

5) Data transmission function and can transport data for signal system.

b) Signaling System of Main Line

The signaling system of main line is the key subsystem in the whole signaling system. According to the design principle of the Project, the signaling system of main line is divided into the following two zones by functions:

1) Non-blocking protection zone. The signaling system provides no space headway protection for the train in this zone. Instead, the driver drives the train through control of the running speed and the safety headway with the front train only by viewing the indication in the switch area signal.

2) Blocking protection zone. The signaling system provides space headway protection for the train in fixed blocking mode in this zone. The driver drives the train manually through control of the running speed by viewing the speed limit signs of the line and the indication of the signal.

c) Signaling System in Non-blocking Protection Zone

- **Principle**

Typical interlocking signal rules are adopted in the switch area within the non-blocking protection zone of Main Line, to prevent the following possible risks when the driver controls the train by viewing.

(1) Head-on collision

(2) Side collision

(3) Trailing of a switch

The risks can be prevented by the following functions of the signaling system:

(1) Train occupancy/vacancy detection in the track section of switch area

(2) Switch monitoring

(3) Route establishment in switch area

(4) Signal control

(5) Route locking

(6) Route release

- **Functions**

(1) Train occupancy/vacancy detection in the track section

Axle counter equipment is used to detect the train occupancy/vacancy condition in the switch area of the main line.

(2) **Route establishment**

Route is jointly established by car borne signal equipment, route request equipment, and control system equipment in the switch area. The route in normal service may be established in the following methods:

A **Normal operation condition**

When the train approaches the switch area, the car borne signal equipment can automatically send the train ID to the trackside control system equipment through the route request equipment provided in the middle of the track in front of the signal. The trackside control system can automatically set the route according to the train ID and the operation schedule on the current day.

B) **Single fault condition of route request equipment**

When the train approaches the switch area, the train ID fails to be transmitted to the control system in the switch area due to a single fault on the route request equipment. The driver shall stop the train in front of the signal and request the route by pressing the car borne button. This route request order will be transmitted to the control system in the switch area through route request equipment provided next to the signal. The control system in the switch area will set the route according to the manual order.

C) **Complete fault condition of route request equipment**

When both the route request equipment at the front of the signal fails, the driver shall contact with the center dispatcher through the radio communication system which provided by the communication discipline, to request manual setting of the route by the dispatcher.

- **Switch monitoring:**

The control system in the switch area can monitor the switches within its span of control. The control and indication circuit of the switch machine shall meet the following technical requirements:

- The interlocked switch can be automatically selected depending on the route setting. The switch on the route can be selected in sequence to allow that the action current can keep away from the starting peak.
- Once the switch is locked, the switch cannot be moved.
- once started, the switch shall turn to a specified position. In case the switch fails to turn to the specified position within the set time due to any reasons, alarm will be initiated.

- After completion of the switches, the power for initiating the switch machine can be automatically cut off. In case of fault on the motor circuit of the switch machine, the starting circuit of switch can be automatically cut off.

- **Signal control**

Upon route locking, when the clear signal indication condition is met, the system can control the signal at clear and monitor the indication state of the signal. After closing of the signal, the signal shall not be re-cleared unless the route is set again.

- **Route locking**

After the route is selected, the switch and conflict route can be locked when the track section related to the route is vacant, the switch position is correct, and the conflict route is not established.

- **Route release**

The locked route can release automatically by segments each track section as the train or train set runs normally after the protection signal is closed.

- **System composition**

The control system equipment in the switch area of the main line is composed of trackside control box, axle counter, signal, switch machine, etc., as shown in Fig. 4.4

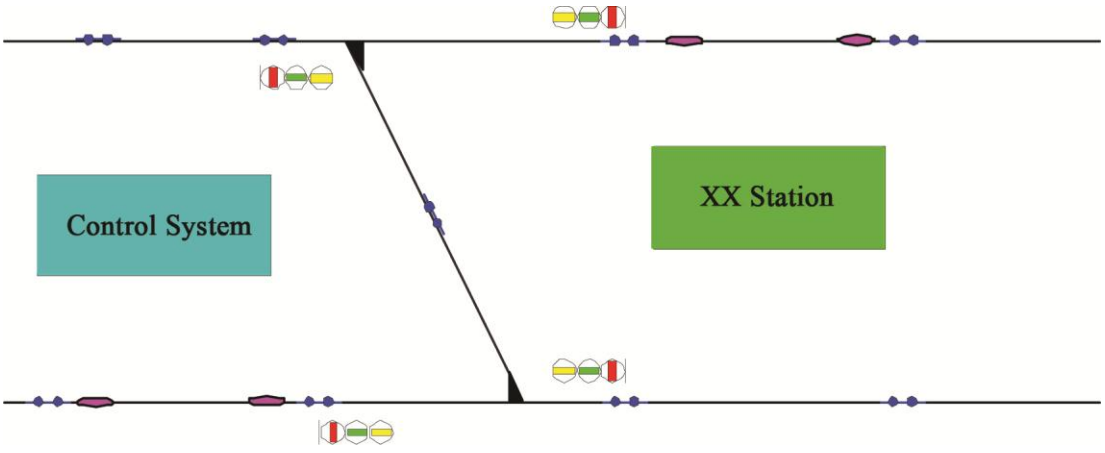

Figure 4.4 Layout of Trackside Equipment in Switch Area of Non-blocking Protection Zone of Main Line [32]

1) : Axle counter, used for train occupancy/vacancy detection in the track section.

The axle counter equipment is composed of track head, outdoor electronic unit, and axle counter host computer. The axle counter equipment shall comply with the Principle of Fail-Safe in Railway Signaling and is designed to:

(1) Handle the signal from Axle counter magnetic head;

(2) compare the number of axles entering and leaving the section;

(3) Monitor the track section for occupancy/vacancy indication.

2)  : LED signal as the running token in the switch area, which has the meaning as follows:

-  indicates no passing; when seeing the red lamp, the driver must ensure that the train stops in front of the signal.

-  Indicates clear route in the front; all the switch directions are straight in the route and the train must run within the limit speed according to the line.

-  Indicates clear route in the front; at least one of switch directions are lateral. The driver shall reduce the running speed of the train and allow the train run at a lateral speed of passing the switch.

The route indicated on the signal is the route in the switch area

When the system failure or power failure causes abnormal working of the signal, and all the lamps are off, it indicates no passing.

3) : Route request loop, which is used to transmit the train ID and the route order made by the driver.

4) The trackside control system is used to complete interlocking logic operation and control of switch area.

- **Signaling System in Blocking Protection Zone**

For the line section built underground and overhead, the space headway between the trains shall be controlled by blocking.

1) **Principle**

The line is divided into numbers of block section. More than two trains shall not run in the same block section to prevent any accident.

2) **Functions**

Interlocking rules are adopted in the blocking zone to realize the protection of safety space headway of the train within the whole blocking zone.

- **System composition**

Schematic diagram of system composition is as follows:

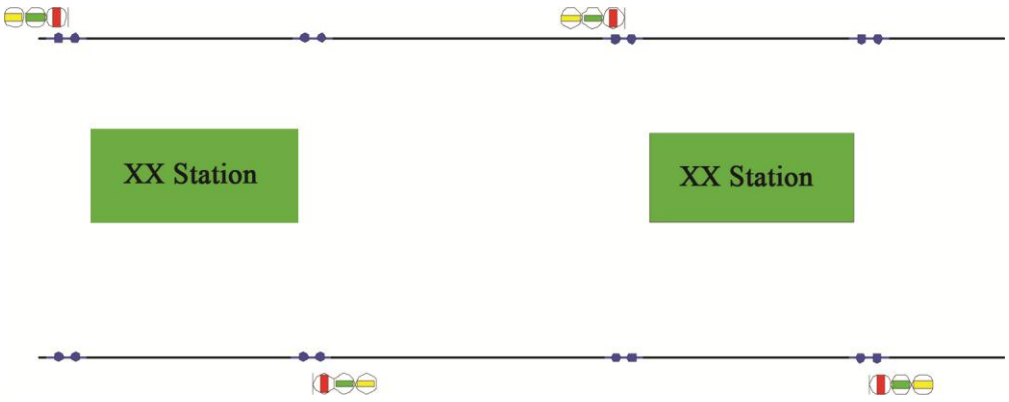

Fig. 4.5 Layout of Trackside Equipment in Blocking Protection Zone [32]

- **Other Items to be specified**

Due to limited engineering condition, the indication distance of the signal fails to meet the braking distance requirement of the train manually driven by the driver. Therefore, increase of

repeating signal will be considered for compliance with the braking distance requirement of the train.

The division of the visual driving zone and the blocking zone as well as the layout of trackside equipment of signaling system of main line is shown in attached drawing I "Plane Layout of Signal for N-S Line" and attached drawing II Plane Layout of Signal for E-W Line.

- **Crossings Signaling System**
  - **System Functions**

The line of the Project has level crossings with the urban public transport roads at 5 places. To ensure the operation service level of the urban mass transit, the public transportation operation shall be organized in such manner that LRT is given the priority to pass through the level crossings. With respect to the operation requirements and safety at level crossings, the crossing signaling control system should provide the following functions:

1) Allow the train at the level crossing to be given the priority to pass through the level crossing;

2) Detect trains approaching and leaving the level crossings.

3) Control the signal at crossings;

4) Monitor the crossing signal state and transmit relevant information to the operation assistant dispatching system.

- **System Design Plan**
  - **General**

The passing priority of LRT at level crossings is mostly realized through the interface between the LRT signaling system and the traffic light control system of the roads. The LRT signaling system transmits the information of the train approaching the level crossing to the traffic light control system of the roads. After receiving such information, the traffic light control system of the roads will control the traffic signal light so as to allow the train can have the priority to pass through the level crossing. Refer to the following figure for details:

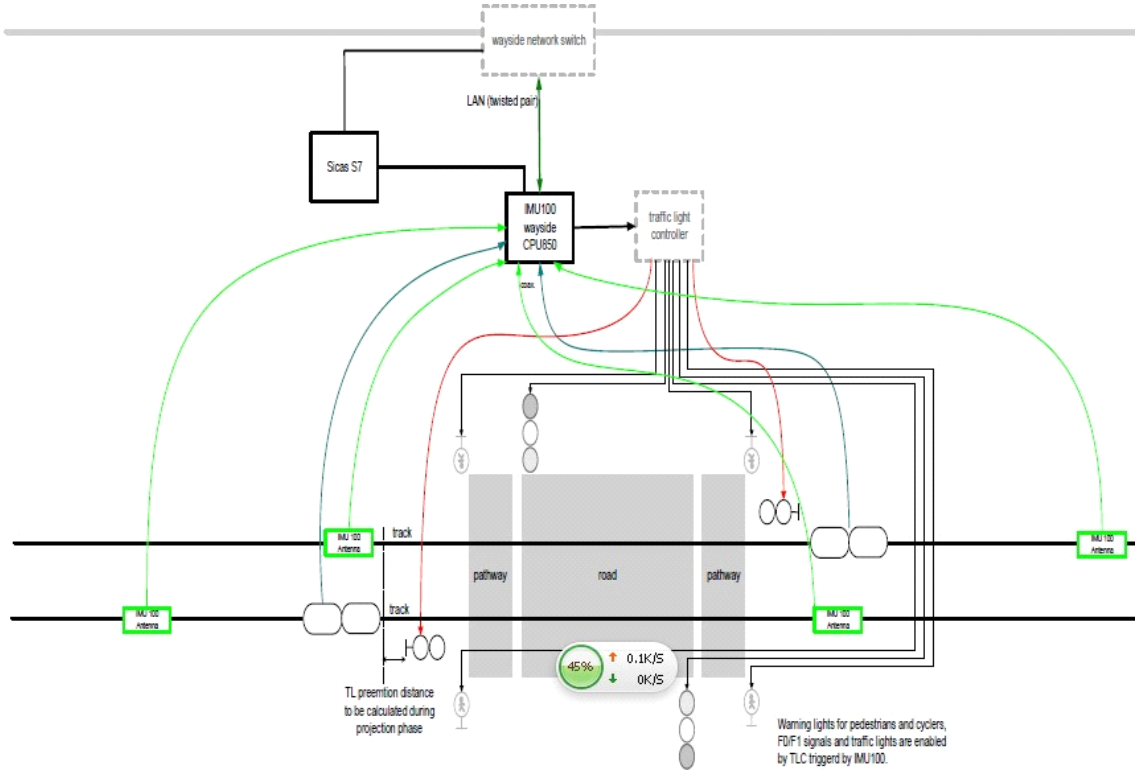

Fig. 4.6 Schematic Diagram of Solution (SIEMENS) for Level Crossing of LRT Project [32]

In Addis Ababa, no traffic light control system is available at the level crossing between the line of the Project and the public roads. However, the aforesaid solution has some reference significance for the design of the signaling system at the level crossing for the Project in urban environment.

Therefore, the design of the signaling system at the level crossing for the Project shall adhere to the following principle:

(1) Since manual driving mode by viewing is adopted for the Project, the running speed of the train shall be controlled manually by the driver.

(2) The signaling system at level crossing shall be designed to avoid any serious impact on the urban road car flow caused by fault of the signaling equipment at the crossing.

(3) The signaling system at level crossing shall be designed in full combination with the urban roads environment where the line runs through.

- **Design principle**

The composition of signaling system at crossing is shown in the following figure:

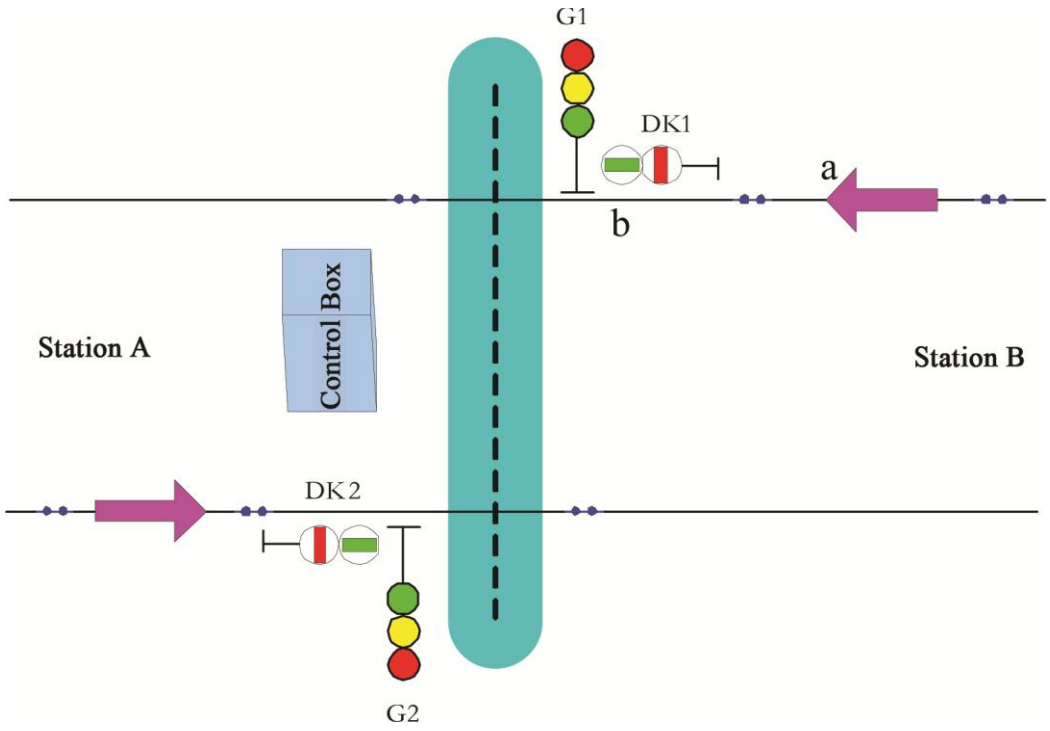

Figure 4.7 Equipment Diagrams of the Crossings Signaling Control System [32]

Take the train running from Station B to Station A for example. The control principle is generally described as follows:

(1) When the train does not occupy the track section a, the road signal G1 and G2 in the signaling system at the crossing indicates a stable green light, which allows the motors and pedestrians to pass through the level crossing. Meanwhile, the signal DK1 indicates a red light, which prohibits the train from passing through the level crossing.

(2) When the train is detected to occupy the track section a, the road signal indicates a yellow light and initiates an acoustic alarm to remind the motors and pedestrians already in the crossing area to pass through the level crossing at a faster speed and to stop the motors and pedestrians that intend to enter the crossing area.

(3) When the train occupies the track section b, the road signal G1 and G2 indicates a stable red light, which prohibits the motors and pedestrians to enter the crossing area. Meanwhile, the signal DK1 indicates a green light, which allows the train to pass through the level crossing.

(4) After the train passes through the track section b, the road signal resumes the stable green light, which allows the motors and pedestrians to pass through the level crossing. Meanwhile, the signal DK1 indicates a red light, which prohibits the train from passing through the level crossing.

CHAPTER FIVE: SYSTEM DEFINITION AND MODEL DEVELOPMENT

This Chapter represents Step 2 of the proposed methodology in Section 2.2. A generic Railway model is developed, for the AA LRT models. The generic model is introduced, aiming at making it easier to develop safety control structure of the AA LRT in Section 5.2; the generic LRT model is developed based on the STAMP theory. Responsibilities and control actions of each system component are defined.

- **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.

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

4.1. Draw a System Boundary

- **Project processes**

LRT projects are comprised of various processes. In order to develop control models, it is necessary to specify processes on which this thesis focuses. Figure 5-1 represents a process flow of a typical LRT project development and operation.

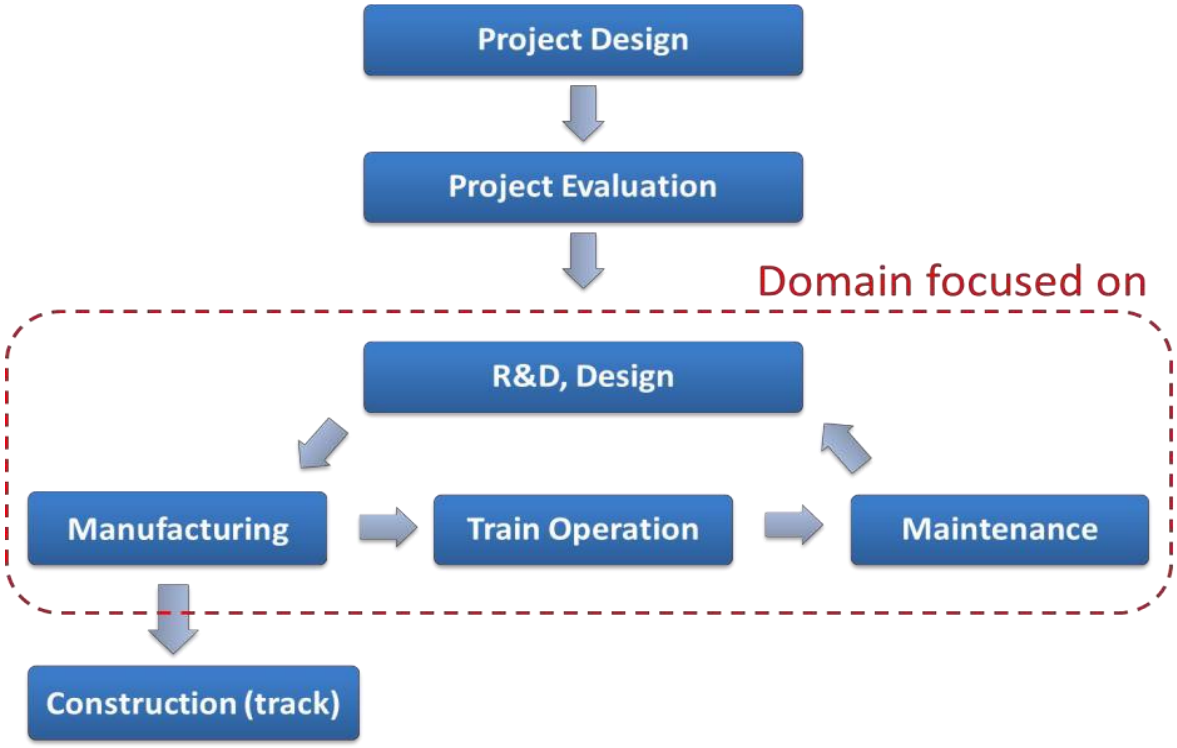

Figure 5-1 Project Development and Operation Flow Diagram

In emerging markets for LRTs, 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. In the next Project Evaluation phase, this structure is evaluated and compared, through implementing evaluation processes such as Environmental Impact Assessment, Cost-Benefit Analysis, Demand Analysis, or Service Development Planning [17]. 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 level.

- **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.

4.1.1. 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.

- **Define System Requirements and Safety Constraints**

The preliminary hazard defined in Section 5.1.3 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 Levisohn [67].

A) **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.e.

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)

B) **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 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.

C) **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 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 &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.

4.1. Generic AA LRT Safety Control Structure Model

In this section, a generic LRT model is developed based on the system boundary defined in Section 5.1.2 and the system requirements and safety constraints defined in Section 5.1.4. Also, responsibilities, control actions, feedback, and a process model are defined for each component. As explained in Section 2.2, this generic LRT model can be regarded as the simplest structure that can meet all requirements from Section 5.1. This generic LRT model is introduced to help develop models of the complex unique institutional alternatives of the AA LRT and highlight the structural differences, which can provide safety risks in the AA LRT. Figure 5-2 represents a safety control structure of the generic LRT model. Table 5-1 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 LRT 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 LRT model as a vertically integrated industry.

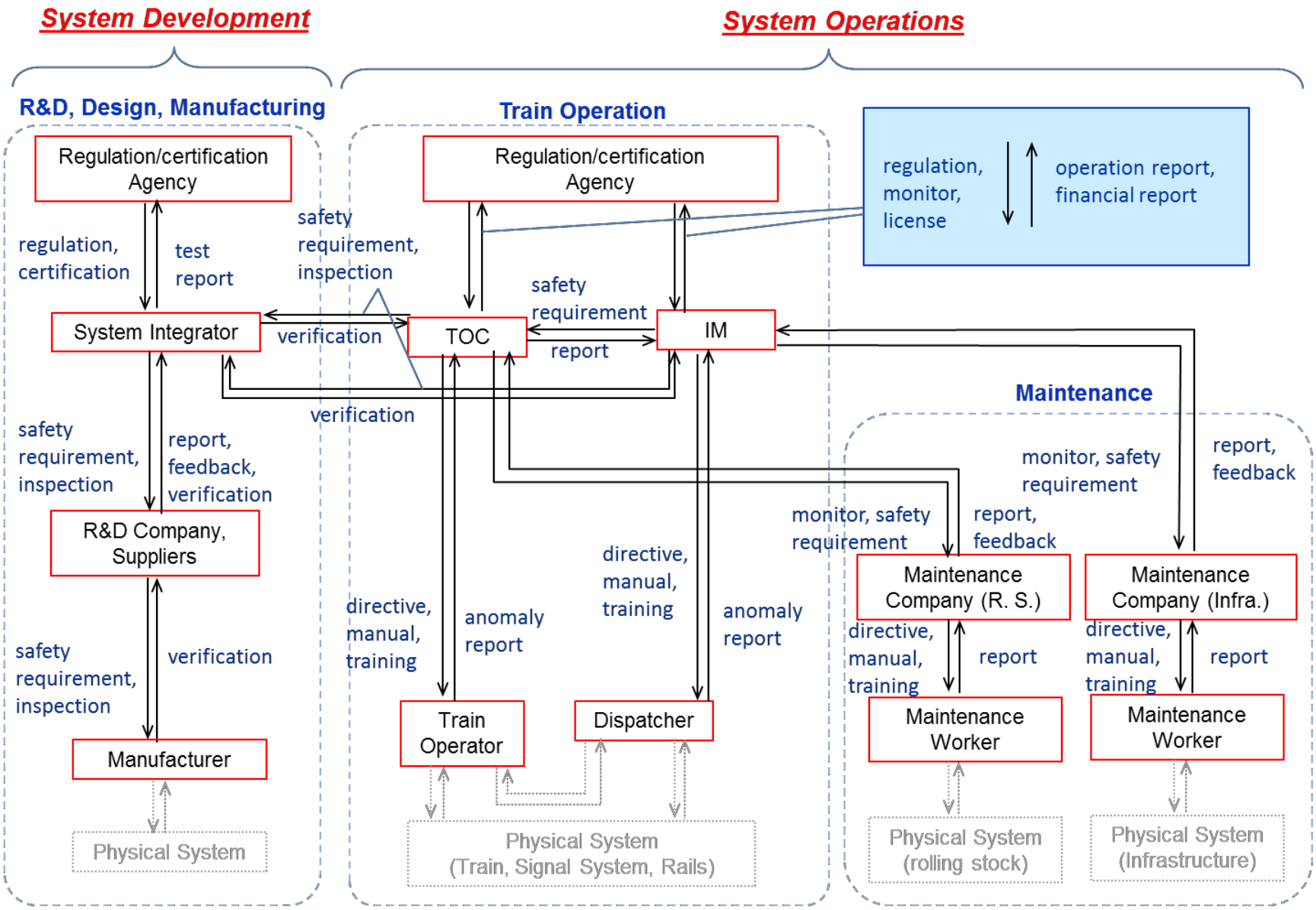

Figure 5-2 Safety control structure of the generic LRT model

Table 5-1 Responsibilities, control actions, feedback and process models (generic LRT 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	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	
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	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	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	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	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*			

CHAPTER SIX:FINDINGS, CONCLUSION, AND RECOMMENDATIONS

Findings, conclusion, and recommendations are described in this chapter. The recommendations are organized for project planers and implementers of the AA LRT based on the safety control structure that this research developed.

6.1. Findings

The findings in this research are as follows.

- The following is the findings from CAST of Wenzhou Train Crash and Hatfield Derailment.

- In developing a new LRT 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, corporate cultures, nationality character, regulations, etc. Safety risks related to these interfaces must be adequately identified.

6.2. Conclusions

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 AA LRT, a holistic approach focusing on not only physical systems but also institutional levels is essential for Safety control structure.

- The safety control 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 safety control methodology that can meet these requirements. The case study of the LRT project in the AA has shown the usage of this methodology. This research strongly recommends that the project planers of the AA LRT adopt the proposed methodology as a "safety-guided institutional design" tool. Specific recommendations for the AA LRT are described in Section 6.3

- Safety-related regulations should be developed from a neutral standpoint about the institutional structure.

- This research developed and analyzed specific institutional safety control structure of the AA LRT, 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, the author proposes 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.

6.3. Recommendations

- **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 AA LRT, 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.

- **Support 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 AA LRT should use the proposed methodology. This research has developed a control structure on the AA LRT 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.

- **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 AA LRT are organized as follows:

- **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.

- **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 AA LRT is doing.. This research recommends that ERC establishes a regulation to require any suppliers for AA LRT systems to implement a system safety approach that is harmonized to ensure their consistencies throughout the total system. Furthermore, ERC needs to overarch this system safety approach 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 incorporate flexibility to adapt all system safety activities to any future system change

– Need to have consistent criteria about risk evaluation and risk acceptance.

6.4. Future Work

This thesis is the first research case to apply the STAMP-based approach to safety control structure 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, especially risk identification and evaluation of AA LRT is open for other researchers and 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 AA LRT which is still in the development process, should be further analyzed from STAMP-based perspectives.

REFERENCES

[1] State Administration of Work Safety, "Official Accident Report of Wenzhou Derailment (Chin2011.[Online].Available: http://www.chinasafety.gov.cn/newpage/Contents/Channel_5498/2011/1228/160577/content_1605 77.htm? COLLCC=485100271&

[2] BBC, "Spain train driver 'on phone' at time of deadly crash," 2013. [Online]. Available: http://www.bbc.com/news/world-europe-23507348

[3] A. Dong, "Application of CAST and STPA to Railroad Safety in China," 2012

[4] D. Suo, "A System Theoretic Analysis of the '7. 23 Yong-Tai-Wen Railway Accident," 2012

[5] UIC, "High speed rail -faxt track to sustainable mobility-," 2012

[6] N. G. Leveson, "A new accident model for engineering safer systems," Saf. Sci., vol. 42, no. 4, p.

237–270, Apr. 2004

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

[8] N. G. Leveson, Safe Ware : System Safety and Computers. Addison-Wesley Professional, 1995

[9] China Railway Group limited: AA LRT Project E-W & N-S, Project study Report, 2009

[10] OECD, "Structural Reform in the Rail Industry," no. February, 2005.

[11] DOD, "Department of Defense Standard Practice -System Safety- (MIL-STD-882E)," 201

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

[13] 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- USTRE6B860B20101209

[14] FRA (NEC FUTURE), "Scoping Package," no. June, 2012

[15] ISO/IEC, "ISO/IEC 31010 Risk Management – Risk Assessment Techniques," vol. 2009.

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

[17] 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

[18] 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.

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

[20] 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

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

[22] F. Kurosaki, "An Analysis of Vertical Separation of Railways," 2008.

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

[24] UIC, "General Definition of High speed." [Online]. Available: http://www.uic.org/spip.php?article971

[25] UIC, "Railway Lines in the world," 2013.

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

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

[28] H. Qiao, "Wenzhou crash report blames design flaws and poor management," Int. Railway. J., vol. January 30, pp. 8–10, 2013

[29] P. Booth, D. Shouts D. Comment, A. Davidson, J. Cassidy, A. Borowitz, R. Brody, and T. N.Yorker, "How a Railway Disaster Exposed China's Corruption," New Yorker, vol. 10/29, pp. 1–15, 2012.

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

[31] AA LRT Project, 'Communication System " Vol. One, page 11

[32] AA LRT Project, 'Signaling system "Vol. 1, page 9 – 11

[33] AA LRT Feasibility study vol. 1-General & Transport Issues, pages 16 & 21