Assuring Safety in High-Speed Magnetically Levitated (Maglev) Systems: The Need for a System Safety Approach

by

Shuichiro Daniel Ota

M.E., Aeronautics and Astronautics
University of Tokyo, 2000

SUBMITTED TO THE DEPARTMENT OF AERONAUTICS AND ASTRONAUTICS
IN PARTIAL FULFILLMENT OF THE REQUIRMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN AERONAUTICS AND ASTRONAUTICS
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2008

Signature of Author: ____________________
Department of Aeronautics and Astronautics
May 6, 2008

Certified by: ____________________
Nancy G. Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: ____________________
Prof. David L. Darmofal
Associate Department Head
Chair, Committee on Graduate Students

Assuring Safety in High-Speed Magnetically Levitated (Maglev) Systems: The Need for a System Safety Approach

by

Shuichiro Daniel Ota

Submitted to the Department of Aeronautics and Astronautics
on May 6, 2008 in Partial Fulfillment of the
Requirements for the Degree of Master of Science in
Aeronautics and Astronautics

ABSTRACT

Magnetic levitation is a railway technology that enables vehicles to be magnetically suspended above their tracks. Although this technology is still under development, magnetically levitated (maglev) systems have great potential to introduce significant changes in today's transportation networks.

This thesis proposes an approach to assuring safety in high-speed maglev systems. It examines characteristic features of the systems, and analyzes the Japanese commuter railway accident in 2005, using Systems Theory Accident Modeling and Processes (STAMP) and System Dynamics models. The characteristic features reveal that the likelihood and potential severity of accidents in maglev systems are higher than those in conventional railway systems because of their high speed, levitation technology, software intensiveness, and other factors. A primary lesson learned from the accident is the importance of risk/hazard analysis that can qualitatively focus on the severity of accidents and human factors. These findings are put together in the form of requirements of risk/hazard analysis and organizational structures. This thesis demonstrates that these requirements, which are not entirely consistent with current actual practices based on international railway standards, conform well to the fundamentals of System Safety, which is an organized and established method to assure safety in complex systems.

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

Acknowledgements

I would like to express my gratitude to Professor Nancy Leveson, my thesis supervisor, for her guidance and patience toward the completion of this research. I am deeply grateful to the members of the Columbia Group, an informal multidisciplinary group of faculty and students at MIT, especially Professor Joseph Sussman and Professor John Carroll, who provided useful insights for this thesis.

I also thank my friends in Room 33-407 and my family, Ayako, Ryoichiro, and Keijiro, who have given me warm encouragement throughout my studying. Finally, I gratefully show appreciation to Central Japan Railway Company, my financial sponsor, for giving me a chance to study at MIT over two years.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivations

Magnetic levitation is a railway technology that enables vehicles to be magnetically suspended above their tracks. The technology is in use in several places; however, it should be considered still under development. Further research and development are required in order to realize this next generation transportation system.

Magnetically levitated (maglev) systems have great potential to introduce significant changes in today's transportation networks. First of all, one of the significant characteristics of the maglev system is its speed. The absence of contact between the vehicles and ground allows the vehicles to run at an extremely high speed, about 500 kilometers per hour in the case of Japanese maglev systems, which is twice as fast as that of conventional high-speed trains. It is expected that more people would choose to take railways using maglev systems than airplanes. The next advantage is that maglev systems are environmentally friendly. They produce fewer carbon dioxide (CO2) emissions than airplanes (Railway Technology Research Institute [RTRI], 2006; Transrapid International, 2006). This characteristic is suited to recent concerns about global warming.

On the other hand, high-speed operation, levitation technology, software intensiveness, structural fragility, and other characteristic features will increase the likelihood and potential severity of an accident in high-speed maglev systems, compared to those in conventional railway systems. Therefore, closer attention should be paid to assuring safety in high-speed maglev systems.

1.2 Objectives and methodology

The purpose of this thesis is to propose an appropriate approach to assuring safety in high-speed maglev systems. It is important to note that the scope of this thesis is high-speed maglev systems. While there exist various types of proposed maglev systems, some of which are appropriate for high-speed railways, and others for local networks, the most notable high-speed maglev projects are: (1) the German Transrapid project and (2) the Japanese superconducting maglev project. These two projects comprise the scope of this thesis.

In light of the primary purpose, this thesis will follow three steps. First, current approaches to safety of high-speed maglev systems are examined. In addition to actual approaches in the German and Japanese high-speed maglev system projects, existing international standards for conventional railway applications, mainly IEC 62278: *Railway applications – Specifications and demonstration of reliability, availability, maintainability, and safety (RAMS)*, are reviewed. The German maglev systems are based on the standards for conventional railway applications (Steriner & Steinert, 2006).

Next, the Japanese commuter railway accident in 2005 is analyzed using Systems Theory Accident Modeling and Processes (STAMP) and System Dynamics models. Although this accident had nothing to do with maglev systems, looking at this accident is worthwhile for high-speed maglev systems. This accident was caused by a representative company of the railway industry in Japan, which is an advanced country in the field of railway. It is supposed that this kind of sophisticated company in terms of railway technology would operate a maglev train in the future. A STAMP analysis has been developed by Nancy Leveson at Massachusetts Institute of Technology (MIT) to investigate today's complex accidents. System Dynamics was originally developed by Jay Forrester at MIT in the 1950's for mangaers and public policy makers to use to design and implement high-level policies. Leveson (2002) has proposed that safety issues be analyzed using a combination of STAMP and System Dynamics. This thesis adopts its proposal.

Finally, an appropriate approach to assuring safety in high-speed maglev systems is derived from the characteristic features of high-speed maglev systems, current actual approaches, and lessons learned from the accident.

1.3 Thesis structure

Following this Introduction in Chapter 1, maglev systems are introduced in Chapter 2. First, the concept's origins and history and the current status of maglev projects, all over the world, are reviewed. Next, maglev systems are characterized for the following analysis.

In Chapter 3, current approaches to safety of high-speed maglev systems are examined. It consists of two parts: (1) Overview of existing international standards for conventional railway applications and (2) Review of current actual approaches to safety of high-speed maglev systems in Germany and Japan.

The Fukuchiyama Line derailment accident, which occurred in Japan on April 25, 2005, is analyzed in Chapter 4. After a brief review of a STAMP analysis and System Dynamics model, first the proximate events, then the STAMP analysis and System Dynamics model of this accident are presented, followed by lessons learned. Derived here is an important lesson that risk/hazard analysis is the key to assuring safety.

Subsequently, in Chapter 5, the findings through characterizing high-speed maglev systems and analyzing the Fukuchiyama Line derailment accident are put together in the form of requirements of risk/hazard analysis. It is demonstrated that these requirements are not entirely consistent with current actual practices based on international railway standards but conform well to the fundamentals of System Safety, which is an organized and established method to assure safety in complex systems.

In Chapter 6, organizational risk analysis is conducted for high-speed maglev systems. This chapter derives the organizational requirements to avoid poor risk analysis, which is considered to be the most critical hazard in high-speed maglev systems, applying a STAMP risk analysis.

Finally, Chapter 7 concludes this thesis.

Figure 1.1 shows the thesis structure.

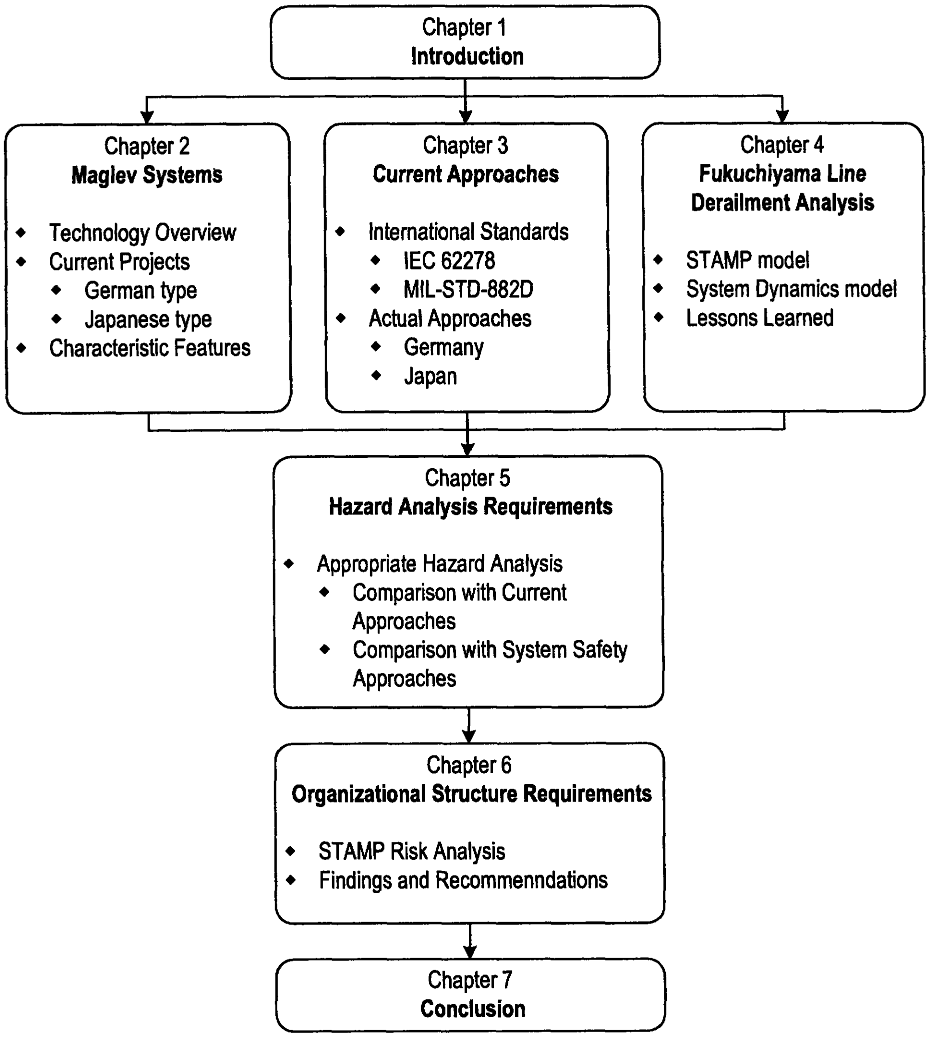


Figure 1.1: Structure of this thesis.

Chapter 2

Characteristic Features of Maglev Systems

In this chapter, magnetically levitated (maglev) systems are introduced. First, the concept's origins and history, and the current status of maglev projects all over the world are reviewed. Subsequently, maglev systems are characterized for the following analysis.

2.1 Magnetically levitated (maglev) systems

2.1.1 Overview

Magnetic levitation is a railway technology that enables vehicles to be magnetically suspended above their tracks. Since the magnetically levitated (maglev) vehicles travel free of friction, it is possible to increase operating speeds without a terrific noise. The technology is in use in several places; however, it should be considered still under development. Further research and development are required in order to realize this next generation transportation system.

There are primarily two types of levitation technology: electrodynamic suspension (EDS) and electromagnetic suspension (EMS). EDS, commonly known as "repulsive levitation," uses a repulsive force between the vehicle's magnetic field and the track's magnetic field. (In EDS, both vehicles and tracks are required to generate magnetic fields.) EMS, commonly known as "attractive levitation," uses an attractive magnetic force between a steel track and electromagnets attached to vehicles. Details will be described in the following subsection.

The concept of maglev systems is not new. It was 1914 when Emilie Bachelet, a French-born American engineer, exhibited a model of maglev systems using EDS technology in London. Hermann Kemper of Germany subsequently pioneered the concept of an electromagnetically levitated train system (EMS) in 1936.

Maglev systems have the potential to introduce great changes in today's transportation networks. First of all, one of the significant characteristics of the maglev system is its speed. The absence of contact between the vehicles and ground allows the vehicles to run at an extremely high speed, about 500 kilometers per hour in the case of Japanese maglev systems, which is twice as high as that of conventional high-speed trains. It is expected that more people would choose to take railways using maglev systems than airplanes. The next advantage is that maglev systems are environmentally friendly: They produce fewer carbon dioxide (CO2) emissions than airplanes while offering high-speed performance (RTRI, 2006; Transrapid International, 2006). This characteristic is suited to recent concerns about global warming.

2.1.2 Current maglev projects under consideration

There exist various types of levitated railway systems under consideration all over the world, in terms of suspension methods and the types of magnets applied, as shown in Table 2.1. Some of these systems are appropriate for high-speed railways, and others for local networks. Among high-speed maglev systems, the most notable projects are: (1) the German Transrapid project and (2) the Japanese superconducting maglev project. The former uses electromagnetic suspension (EMS) while the latter uses electrodynamic suspension (EDS). Both are intended for high-speed railway systems and comprise all of the scope of this thesis as mentioned in the previous chapter. A brief overview of the two is given below, and Table 2.6 shows comparisons between them.

Table 2.1: Classification of current levitated railway system projects (Source: RTRI, 2006). An asterisk (*) denotes that the system is developed especially for high-speed railway.

Categories	Countries involved
I Electrodynamic Suspension (EDS)	
(1) Superconducting magnet systems *	Japan (Superconducting maglev projects), U.S., Canada
II Electromagnetic Suspension (EMS)	
(1) Electromagnet systems *	Germany (Transrapid projects), U.K., Japan, Korea, Switzerland
(2) Combination of superconducting magnet systems and electromagnet systems *	U.S.
(3) Permanent magnet systems	Germany
III Others	
(1) Air-cushion supported	U.S., Japan
(2) Mixed-μ levitation	U.K.

German Transrapid Project

The German high-speed maglev system named Transrapid is one of the most advanced levitated railway systems being proposed anywhere in the world and is representative of electromagnetic suspension (EMS) for high-speed transportation (RTRI, 2006). The system is being developed by German companies, namely Siemens, ThyssenKrupp, and Transrapid International, which was established by Siemens and ThyssenKrupp as a joint company for systems integration, marketing, and maintenance support. According to Transrapid International (2006), Transrapid is suitable both as a fast link between a city center and its outlying airport, as a fast connection between city pairs, and as a long-distance transportation system.

Technology: In order to achieve suspension, Transrapid uses an attractive magnetic force between electronically controlled electromagnets (called support magnets) in the vehicles and ferromagnetic rails installed on the underside of the T-shape (monorail type) guideway. The gap between the vehicles and guideways is electronically controlled to be about 10 millimeters.

As for the propulsion system, the synchronous long-stator linear motor is adopted. A linear motor is essentially an electric motor that has its stator "unrolled" so that instead of producing a torque, it produces a linear force along its length. In the case of Transrapid, rotors correspond to the support magnets attached to the vehicles, while stators correspond to the ground coils. (Rotors and stators are basic components of conventional motors.) By continuously supplying alternating current to the ground coils, an electromagnetic traveling field is generated, which moves the vehicles, pulled along by their support magnets. The maximum operational speed is 500 kilometers per hour.

History: Electromagnetic suspension systems have a long history, and it was 1922 when the concept was first proposed (RTRI, 2006). After significant advances by Hermann Kemper, the first passenger-carrying prototype vehicle was demonstrated in Munich, Germany in 1971. The construction of the guideway of the Transrapid Test Facility (TVE) began in 1980, and intensive running tests have been conducted since then. The TVE, which was completed in 1987, has a total length of 31.5 kilometers and is the world's longest test facility for maglev systems. New prototype vehicles were continuously introduced in the test facility. The latest versions are the pre-production prototype vehicle Transrapid 08 (TR08), which was delivered in 1999, and the TR09 in 2007, which is a prototype vehicle especially for the Munich Transrapid line and is slightly different from the TR08 (Tum, Huhn, & Harbeke, 2006).

In the spring of 2004, Shanghai Maglev Transportation Development Co. Ltd. (SMTDC) began the world's first commercial Transrapid in Shanghai, China, with the technical support of the German consortium that consisted of Siemens, ThyssenKrupp, and Transrapid International. This is the first and sole commercial high-speed maglev line. The line, which connects Pudong International Airport and Long Yang Road Station, is 30 kilometers long, and the maximum operating speed is 430 kilometers per hour, which is higher than any other rail system in every day normal service (Transrapid International, 2004). The specifications are shown in Table 2.2.

On September 22, 2006, the Transrapid vehicle, the TR08, collided with a maintenance vehicle at a speed of about 170 kilometers per hour at the TVE test track. Twenty-three people were killed and ten were injured in this accident. This was the first accident that caused fatalities on any maglev systems.

Table 2.3 summarizes the history of the German Transrapid project.

Table 2.2: Specifications of the Shanghai maglev line
(Source: Transrapid International, 2004).

Length of the route	30km, double track
Link to the Service Center	3km, single track
Stations	Long Yang Road, Pudong International Airport
Number of Vehicles	3 vehicles, each with 5 sections
Running Speed	430km/h
Traveling Time	8 minutes
Service Frequency	Every 10 minutes

Table 2.3: History of the German Transrapid project.

1936	Hermann Kemper in Germany pioneered the concept of an electromagnetically levitated railway system
1971	Presentation of the first passenger-carrying prototype vehicle in Munich, Germany
1980	The construction of the guideway of the Transrapid Test Facility (TVE) began. (It was finally completed in 1987.)
1984	Introduction of two-section test vehicle, Transrapid 06, designed for a speed of 400 km/h
1988	Introduction of two-section test vehicle, Transrapid 07, designed for a speed of 500 km/h
1998	Formation of a joint company, Transrapid International, and subsequently Transrapid International-USA, whose mission is to promote Transrapid in the U.S.
1999	Introduction of pre-production prototype vehicle, Transrapid 08 (TR08)
2004	The Shanghai Transrapid line began the first commercial operation in Shanghai, China.
2006	TR08 crashed into the maintenance vehicle, killing 23 people.

Future Plans: According to Transrapid International (2007), the Munich project, which links Munich "Franz-Joseph Strauss" airport with the central station by Transrapid, is currently under active consideration. The plan is to begin operation "in just a few years" as of publishing time. The project data is shown in Table 2.4, and it is important to note that this project as well as the existing Transrapid line in Shanghai, China is a short-distance application as airport shuttle, whose route is about 38 kilometers long. At the present time, there is no notable project of a fast urban link on medium and long-distance routes.

Table 2.4: Proposed specifications of the Munich Transrapid project (Source: Transrapid International, 2007).

Number of Vehicles	5
Sections per Vehicle	3
Seats	148
Number of Stations	2
Maximum Operating Speed	350 km/h
Travel Time	10 minutes
Service Frequency	Every 10 minutes
Route Length	Approx. 38 km

Japanese Superconducting Maglve Project

The high-speed maglev system in Japan is generally called "superconducting maglev," named after its key technology, superconductivity. This is a representative system of electrodynamic suspension (EDS). The final goal of the superconducting maglev project, which is primarily developed by Central Japan Railway Company (JRC), is to establish a line between Tokyo and Osaka and to replace the Tokaido Shinkansen, a high-speed bullet train between them, which is operated by JRC, with the maglev vehicles (Central Japan Railway Company [JRC], 2007b).

Technology: There are some differences between the German Transrapid system and Japanese superconducting maglev system in terms of technology besides suspension method (EMS and EDS). One of the most notable differences is that the Japanese superconducting maglev vehicles are equipped with superconducting magnets while the Transrapid vehicles carry conventional electromagnets. Superconductivity is the characteristic of some substances at very low temperatures to let electricity flow with no resistance. When an electrical current is applied to a coil in a superconducting state, this current continues to flow permanently, resulting in the creation of a very large magnetic field. The vehicles are equipped with the superconducting magnets, which generate the necessary magnetic field. When the vehicles pass at a high speed, an electric current occurs through the coils installed in the guideways, generating a magnetic force that pushes up the vehicles. The gap between the vehicle and the guideway is about 100 millimeters. (The guideway is horseshoe type, and the superconducting magnets are attached to both sides of the vehicles.)

As for vehicle propulsion, the superconducting maglev system also utilizes the concept of the synchronous long-stator linear motor, and there is no substantial difference between the two.

History: American engineers James Powell and Gordon Danby (1966) at Brookhaven National Laboratory published the basic concept of the maglev system utilizing supeconducting magnets in 1966. Japan National Railway (JNR), which had begun the research on the maglev system in 1962, paid much attention to the Danby-Powell maglev systems and decided to adopt it at the end. Since then, JNR constructed the test track in Miyazaki, Japan in 1977 and carried out fundamental tests on the basic performance of the maglev system. Successively, in order to do advanced research, it was decided to construct a new test line, the Yamanashi Maglev Test Line in 1989. The Yamanashi Maglev Test Line is a 18.4 kilometer-long double track with tunnels, gradients, and curves, located in Yamanashi prefecture. Running tests on the Yamanashi Maglev Test Line commenced in 1997, and since then, Central Japan Railway Company (JRC) has taken the lead in the research and development of the superconducting maglev system.

The trial runs of the maglev system on the Yamanashi Maglev Test Line have been progressing smoothly since April 1997. Running tests include a new record of the maximum speed of 581 kilometers per hour in December 2003, and a continuous running test in which the vehicles traveled 2,876 kilometers in one day in November 2003. In 2005, the Maglev Technological Practicality Evaluation Committee under the Japanese Ministry of Land, Infrastructure and Transport acknowledged that all the technologies necessary for the future revenue service were established, which is considered to be the ministry's endorsement that the superconducting maglev running test has achieved the technological criteria for practical application. As of September 2006, approximately 129,800 visitors, including Japanese Crown Prince, participated in test rides, and the total distance covered in running tests has been more than 530,000 kilometers (RTRI, 2006).

Table 2.5 summarizes the history of the Japanese superconducting maglev project.

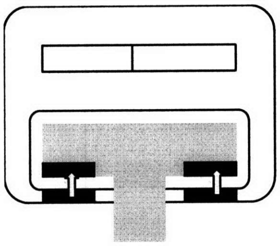
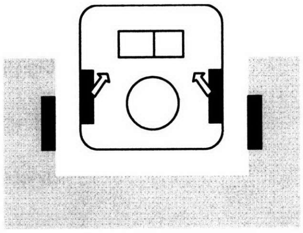
Table 2.5: History of the superconducting maglev project in Japan

1962	Japan National Railway (JNR) began research on maglev systems
1966	Powell and Danby published the concept of the superconducting maglev systems
1977	Test runs began on the Miyazaki Line
1987	JNR was divided into seven private companies including Central Japan Railway Company (JRC) and one institute, namely Railway Technology Research Institute (RTRI). JRC and RTRI took over the maglev project from JNR.
1997	Test runs began on the Yamanashi Line. The maximum design speed of 550 km/h was achieved.
2003	Manned world speed record of 581 km/h was achieved.
2005	The Maglev Technological Practicality Evaluation Committee of the Ministry of Land, Infrastructure and Transport acknowledged that its foundation technology was sufficiently established for practical application.
2006	The cumulative travel distance exceeded 500,000km.
2007	JRC decided to introduce, on its own initiative, the superconducting maglev line between Tokyo and Nagoya in 2025, bearing all the cost for the project.

Future Plans: In April 2007, Central Japan Railway Company (JRC) formally, through the financial report, acknowledged that they were considering beginning commercial operation of the superconducting maglev between the Tokyo metropolitan and Chukyo (or Nagoya) regions by 2025 (JRC, 2007a). JRC is a company that has been operating the Tokaido Shinkansen, a high-speed bullet train, which connects the Tokyo, Nagoya, and Osaka regions, for more than forty years. Since the performance of the Tokaido Shinkansen is at almost full capacity, the company is thinking of introducing, on its own initiative, the superconducting maglev line as a second, more advanced transportation artery that can replace the function of the Tokaido Shinkansen (JRC, 2007b).

Subsequently, in December 2007, the company announced that the company decided to bear all the cost for this project. The estimated cost was JPY 5.1 trillion for construction costs and rolling stock expenses for approximately the 290 kilometer line of the superconducting maglev system. (JRC, 2007c)

Table 2.6: Comparisons between German Transrapid project and Japanese superconducting maglev project

	German Transrapid project	**Japanese superconducting maglev project**
Levitation Technology	Electromagnetic suspension (EMS, attractive force)	Electrodynamic suspension (EDS, repulsive force)
Gap between Vehicles and Ground	10mm	100mm
Propulsion Technology	Synchronous Linear Motor	Synchronous Linear Motor
Magnets in Vehicles	Electromagnets	Superconducting Magnets
Guideway	T-Shape 	Horseshoe Shape 
Operating Speed	430km/h	500km/h
Existing Line	Shanghai Maglev Line	None
Next Proposed Project	Munich Project ("in a few years")	Tokyo-Nagoya Project (in 2025)

2.2 Characterizing high-speed maglev Systems

Following are safety-related significant characteristics of high-speed maglev systems. Some characteristics are described in the previous sections; however, they are re-stated from the viewpoint of safety.

High-speed operation

One of the most notable characteristics of high-speed maglev systems is the high-speed operation. For example, the operating speed of the Japanese superconducting maglev is 500 kilometers per hour, which is twice as high as that of conventional high-speed trains. Furthermore, it has a potential to increase its operating speed; on December 2, 2003, the Japanese superconducting maglev vehicles reached the maximum speed of 581 kilometers per hour, which was a Guinness world record of manned vehicles. The maximum speed of the German Transrapid, as well as the Japanese superconducting maglev, is designed to be

500 kilometer per hour, while the Shanghai maglev line is operated at a speed of 430 kilometer per hour. Figure 2.1 compares the operating speeds of some representative railway systems.

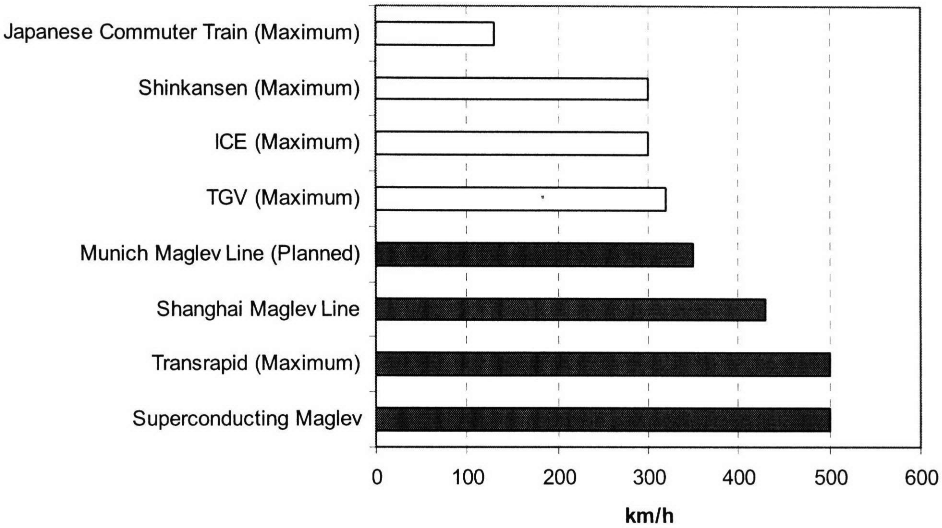


Figure 2.1: Comparison of railway operating speed: *Shinkansen*, *ICE*, and *TGV* are conventional high-speed railway systems in Japan, Germany, and French, respectively. ("Maximum" in parentheses means some of their network lines, not all of them, are operated at that speed.)

This feature, the high-speed operation, affects safety of maglev systems in two ways. First, when the operating speed is increased, delays in processing become unacceptable. Suppose that there are anomalies in guideways ahead. It is required to spontaneously deal with this situation, since the vehicles would reach the point in a short time. At the same time, increasing the operating speed leads to an increase in an inertia force; the vehicles cannot promptly stop or change the track, and there are few options during the high-speed operation with respect to movement. To sum up, the high-speed operation makes the system much more potentially dangerous.

Next, the high-speed operation increases the potential accident severity in maglev systems. Suppose that the vehicles accidentally crash into an obstacle. When the collision speed is not so high, it may result in minor damage. However, there is a possibility that the vehicles crash at a speed of 500 kilometers per hour. In that case, damage could be enormous. In the Fukuchiyama Line derailment accident in 2005 in Japan, which will be analyzed in Chapter 4, the conventional train vehicles crashed into an apartment at a speed of about 100 kilometers per hour, which is considered to be rather low compared to the high-speed operation of the maglev vehicles. Even so, the first two cars were completely damaged, no less than 106 passengers, in addition to the driver, were killed, and 562 others were injured. In short, the high-speed operation could result in the larger number of fatalities and injuries in case of an accident.

Levitation

Another characteristic to be mentioned here is, by definition, that the vehicles are levitated. As described before, the superconducting maglev vehicles are levitated about 100 millimeters above their tracks, and the gap between the Transrapid vehicles and tracks is controlled to be 10 millimeters, as shown in Table 2.6.

This condition, in which the vehicles are levitated, adds new hazards as well as new types of accident causes. When the mechanism for levitation does not work well, the vehicles inevitably crash into the tracks, which may result in substantial damage. This is recognized as a major hazard, which is unique to the maglev systems. In order to mitigate this hazard, the Transrapid vehicles and the superconducting maglev vehicles are equipped with skids (Transrapid International, 2006) and sets of wheels (RTRI, 2006), respectively, for emergency landing. However, in any event, falling is unavoidable, which leads to an accident.

Structural fragility

Making the vehicles light is extremely important for maglev vehicles (Sterinert & Keller, 2004; RTRI, 2006), since it requires much energy consumption to levitate heavy vehicles (Transrapid International, 2006). In order to reduce weight, various measures are applied. One of these measures is to apply aluminum alloys to the vehicles extensively. The high-speed maglev vehicles as well as conventional railway vehicles adopt aluminum carriage bodies, which consist of aluminum longitudinal extrusions and aluminum side and end panels. Furthermore, aluminum undercarriages are introduced in the high-speed maglev vehicles (Steinert & Keller, 2004; RTRI, 2006), while conventional railway undercarriages are made of steel. (Both the German Transrapid and the Japanese maglev vehicles adopt aluminum undercarriages.) These measures successfully reduce the weight of the vehicles:

The Transrapid vehicle achieves 0.5 ton per seat (Transrapid International, 2006), while ICE 3 results in about 1.0 ton per seat (Siemens, 2002). Skllingberg and Green (2007) state:

> While it is not clear at present what the upper limits of this advanced rail technology [the high-speed maglev systems] will be, it is obvious that both sheet and extruded aluminum and their fabrication technologies are vital to achieve these advances in transportation and infrastructure development.

Aluminum materials have superiority in many other aspects, such as high recycling efficiency and energy savings. The application of aluminum for rolling stock including the high-speed maglev vehicles will continue to grow in the future (Sakai, 2007).

It is fair, however, to say that the lightweight vehicles are structurally more fragile than conventional railway vehicles. This means that damages to the maglev vehicles would be greater in case of crashes. In the Transrapid accident in 2006 mentioned before, the first carriage of the TR08 was completely destroyed. One of the factors that magnified the damage is attributed to their lightweight vehicles. To sum up, lightweight vehicles increase the potential accident severity in maglev systems.

Mass transportation

High-speed maglev systems are designed to provide mass transportation railway service. The passenger capacities of the Shanghai maglev and of the Munich maglev are about 400 persons (Tum, Hugn, & Harbeke, 2006), which are in the same range as those of today's long-range wide-body airliners such as Boeing 777 and Airbus 340. There is no information available with respect to the capacity of the Japanese superconducting maglev at the time of this writing. However, the Japanese maglev system is designed to be a substitute for the Tokaido Shinkansen, whose capacity is more than 1,300 persons. It is apparent that the Japanese superconducting maglev, as well as the German Transrapid, becomes a mass transportation system.

Long-connected vehicles are advantageous in the sense that there is a possibility that trouble in the first car, such as derailment and collision, does not spread to subsequent cabins of the train. Even so, it should be recognized that the larger number of people being transported could increase the number of fatalities and injuries in case of an accident.

Software intensiveness

The final characteristic feature is their software intensiveness. The Japanese superconducting maglev is a fully automatic system; there is no driver in the vehicles. To begin the operation, a running plan is provided for the traffic control system (TCS), which automatically gives instructions to the power conversion station and the safeguard system. Also, the system can automatically bring the vehicles to a halt when an anomaly is detected. Therefore, during normal operations, there is almost no room where human operators can work. Besides the automatic operation, the superconducting maglev vehicles utilize various kinds of software systems, instead of hardware systems (RTRI, 2006). The German Transrapid, the TR09, is also driverless (Steriner & Steinert, 2006). Incorporating software in the systems is the recent trend of not only maglev systems but also the entire railway industry. Although there is no reliable way to measure the degree of the software intensiveness, it is apparent that the high-speed maglev systems will require more extensive use of software than conventional railway systems.

Leveson (1995) claims that software programs lead to a complex and tightly coupled designs, and Perrow (1999) agrees with her on that point. Leveson states:

> If we accept Perrow's argument that interactive complexity and coupling are a cause of serious accidents, then the introduction of computers to control dangerous systems may increase risk unless great care is taken to minimize complexity and coupling.

It is fair to say that the various kinds of software programs that are incorporated into the maglev systems make the systems more complex and more tightly coupled, which could lead to an accident. For details, see Leveson (1995).

Conclusions

Two findings are: (1) The potential likelihood of an accident in high-speed maglev systems is higher than those in conventional railway systems, because of high-speed operation, levitation technology, and software intensiveness; and (2) The potential severity of catastrophic potential in high-speed maglev systems is also higher than those in conventional railway systems, because of high-speed operation, mass transportation, and structural fragility.

Consequently, these characteristic features demonstrate the need for more attention to be paid to safety in the high-speed maglev systems.

Chapter 3

Current Approaches to Safety of High-Speed Maglev Systems

Current approaches to safety of high-speed maglev systems are examined in this chapter. It consists of two parts: (1) Overview of existing international standards for conventional railway applications and (2) Review of current actual approaches to safety of high-speed maglev systems in Germany and Japan. German maglev systems are considered to be based on the standards for conventional railway applications (Steiner & Steinert, 2006). Therefore, looking at current standards first is worthwhile although they are not necessarily intended for high-speed maglev systems.

3.1 Overview of standards for conventional railway applications

3.1.1 Framework of international standards

Three international standards have been defined for conventional railway applications (especially safety-related electronic systems) in the past few years.

- IEC 62278: Railway applications – Specifications and demonstration of reliability, availability, maintainability and safety (RAMS)
- IEC 62279: Railway applications – Communications, signalling and processing systems – Software for railway control protection systems
- IEC 62280: Railway applications – Communication, signalling and processing systems – Safety-related communication in closed/open transmission systems

While there is a generic standard for the safety of electronic safety-related systems, IEC 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems*, the three standards above are regarded as application sector standards and as the sector specific interpretation of IEC 61508.

It is important to note that these standards were originally developed from European standards, namely the European Committee for Electrotechnical Standardisation (CENELEC), and every international standard above has its origin in the CENELEC standards. For example, IEC 62278 is derived from EN 50126, which has the same title, *Railway Applications - The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS)*. (*EN* stands for the European Norms.) IEC 62279 and IEC 62280 are based on EN 50128: *Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems* and EN 50159: *Railway Applications – Communication, signalling and processing systems – Safety-related communication in open/closed transmission systems*, respectively. In European standards, there is another important standard EN 50129: *Railway applications – Safety-related electronicsystems for signalling*, which has not published as the international standard yet.

Among these standards, IEC 62278, or EN 50126, is the top-level document that covers the overall process for the total railway systems, and its idea is based on RAMS (Reliability, Availability, Maintainability, and Safety) methods. The remaining standards are primarily developed for a complete railway signalling system. The structure of the railway standards is summarized in Figure 3.1. Since the scope of this thesis is the total railway system, IEC 62278 is worthy of review and will be described further in the next subsection.

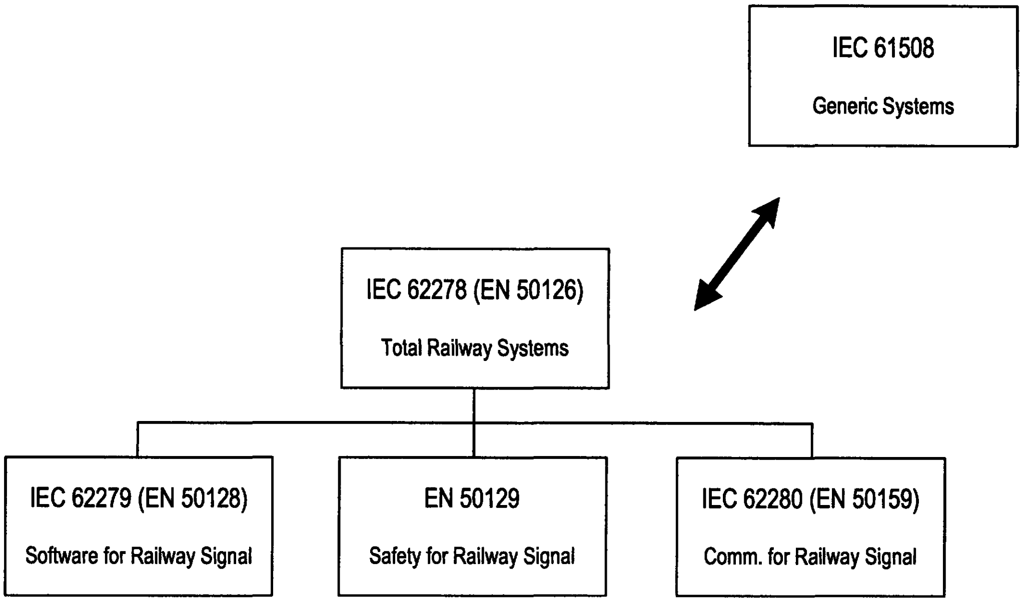


Figure 3.1: Structure of railway standards.

3.1.2 IEC 62278

In its introduction, IEC 62278 describes its purpose as follows: (The definition of Railway Authority is a body with the overall accountability to a Regulator for operating a railway system.)

> This International Standard provides Railway Authorities and railway support industry with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS. Processes for the specification and demonstration of RAMS requirements are the cornerstones of this standard. This standard aims to promote a common understanding and approach to the management of RAMS.

Here, the important aspect is that IEC 62278 does not define targets, quantities, requirements or solutions for specific railway applications; its focus is on how to approach RAMS management, rather than what are RAMS requirements.

Some fundamental aspects to be reviewed here from the viewpoint of safety are as follows.

(a) The standard defines RAMS in terms of reliability, availability, maintainability and safety and their interaction.

It proposes that Railway Authorities manage the RAMS elements of reliability, availability, maintainability, and safety. In addition, the standard claims, as shown in Figure 3.2, that quality of service is achieved by RAMS elements and other attributes such as frequency of service and fare structure.

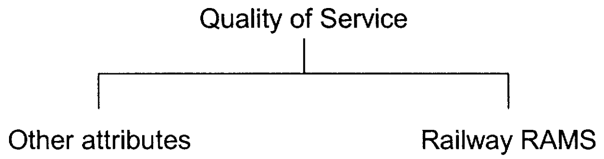


Figure 3.2: Quality of service and railway RAMS (Source: IEC 62278).

The definitions of RAMS elements in the standard are:

- **reliability**: probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2);
- **availability**: availability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided;
- **maintainability**: probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources;
- **safety**: freedom from unacceptable risk of harm.

The inter-linking of railway RAMS elements is shown in Figure 3.3. As shown here, it considers safety and availability to be the most critical parts to achieve a dependable system.

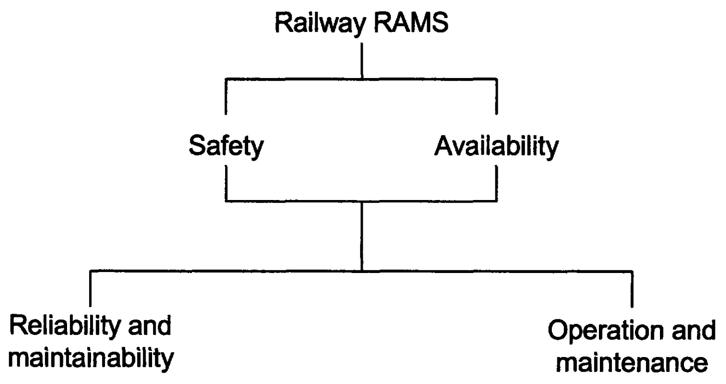


Figure 3.3: Inter-relation of railway RAMS elements (Source: IEC 62278).

(b) The standard introduces the concept of risk, and demands that risk analysis shall be performed at various phases of the system life cycle.

The definition of risk presented in the standard is probable rate of occurrence of a hazard causing harm and the degree of severity of the harm, and the concept of risk is the combination of two elements:

- the probability of occurrence of an event or combination of events leading to a hazard, or the frequency of such occurrences;
- the consequence of the hazard.

Based on these ideas, IEC 62278 provides typical categories of probability or frequency of occurrence of a hazardous event, as shown in Table 3.1, and typical hazard severity levels, as shown in Table 3.2, in qualitative terms. Defining qualitative categories of risk and the actions to be applied against each category as in Table 3.3, it proposes the formation of a "frequency- consequence" matrix for evaluation of the results of risk analysis. An example of risk evaluation and risk reduction/controls for risk acceptance is demonstrated in Table 3.4.

Table 3.1: Frequency of occurrence of hazardous events (Source: IEC 62278).

Category	**Description**
Frequent	Likely to occur frequently. The hazard will be continually experienced.
Probable	Will occur several times. The hazard can be expected to occur often.
Occasional	Likely to occur several times. The hazard can be expected to occur several times.
Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

Table 3.2: Hazard severity level (Source: IEC 62278).

Severity level	**Consequence to persons or environment**	**Consequence to service**
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment	
Critical	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system
Marginal	Minor injury and/or significant threat to the environment	Sever system(s) damage
Insignificant	Possible minor injury	Minor system damage

Table 3.3: Qualitative risk categories (Source: IEC 62278).

Risk category	**Actions to be applied against each category**
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate
Tolerable	Acceptable with adequate control and with the agreement of the Railway Authority
Negligible	Acceptable with/without the agreement of the Railway Authority

Table 3.4: Typical example of risk evaluation and acceptance (Source: IEC 62278).

Frequency of occurrence of a hazardous event	**Risk Levels**			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	Marginal	Critical	Catastrophic
	Severity levels of hazard consequence			

IEC 62278 places a great deal of emphasis on risk analysis. Risk analysis is assigned to the third phase in the system life cycle as shown in Figure 3.4. (The system life cycle is a sequence of phases, each containing tasks, covering the total life of a system from initial concept through to decommissioning and disposal. It consists of fourteen phases.) However, the standard states that risk analysis may have to have repeated at several stages of the system life cycle.

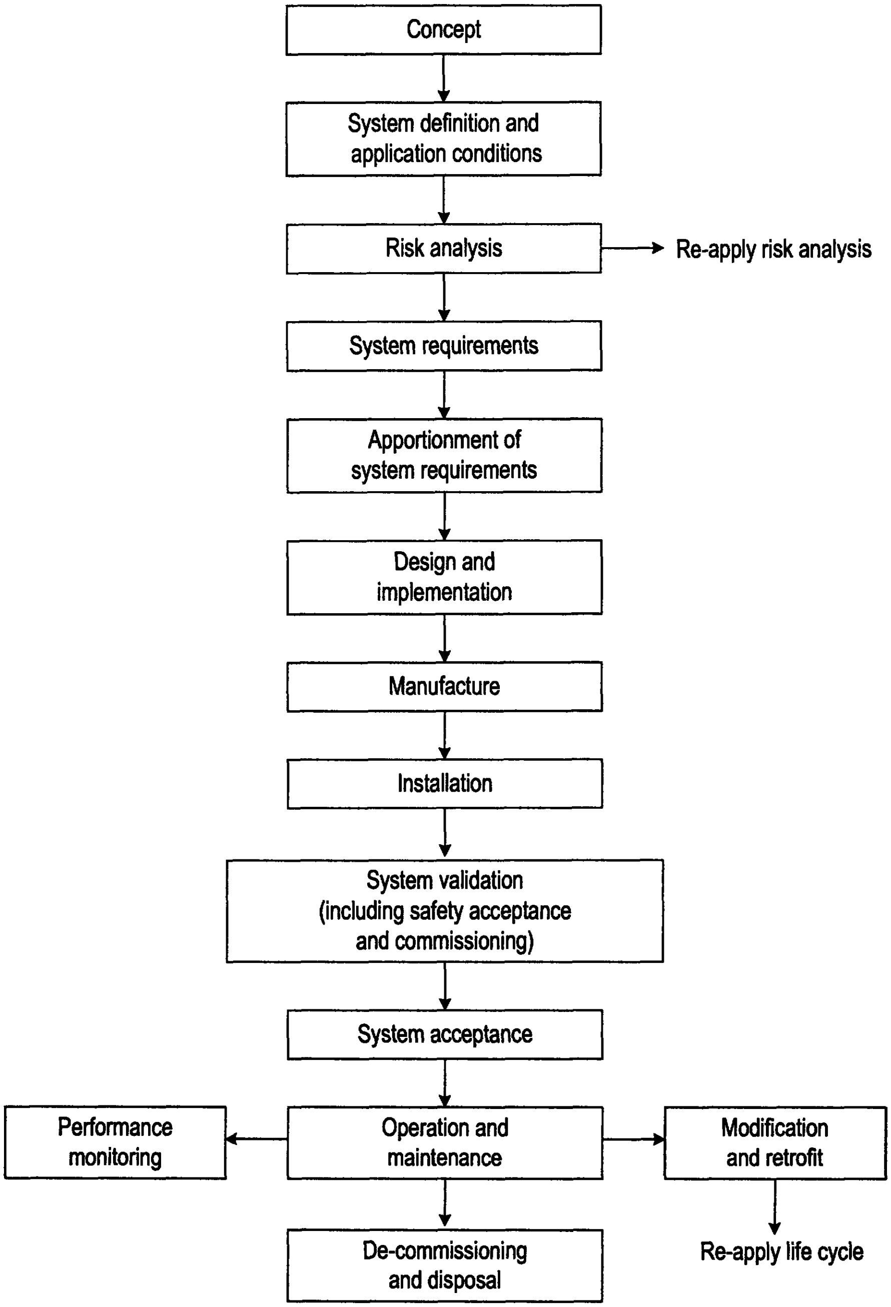
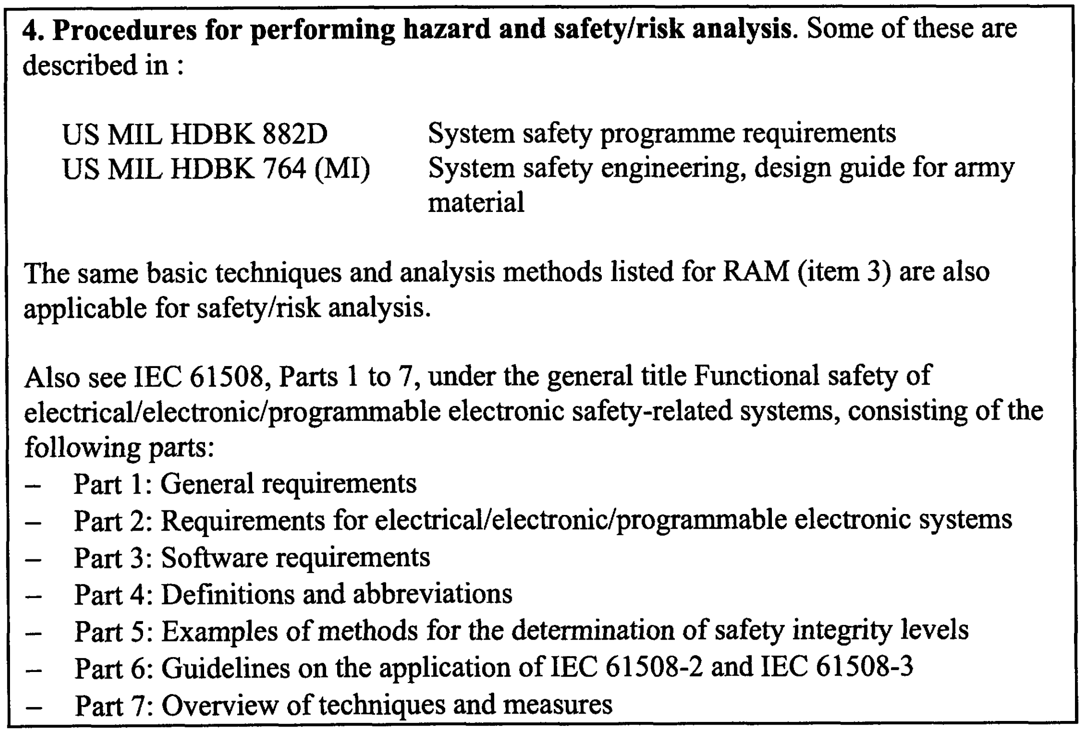

Concept
System definition and application conditions
Risk analysis
Re-apply risk analysis
System requirements
Apportionment of system requirements
Design and implementation
Manufacture
Installation
System validation (including safety acceptance and commissioning)
System acceptance
Performance monitoring
Operation and maintenance
Modification and retrofit
De-commissioning and disposal
Re-apply life cycle

Figure 3.4: System life cycle (Source: IEC 62278).

It is important to note that the standard does not specify any method or tool in particular for RAMS management and analysis; however, some methods and tools are listed in the appendixes, all of which are "informative," which means compliance with them does not have to be demonstrated. It writes, "The choice of relevant tool will depend on the system under consideration and the criticality, complexity, novelty, etc. of the system." As for the procedures for performing hazard and safety/risk analysis, the excerpt from the standard is shown in Figure 3.5.



4. Procedures for performing hazard and safety/risk analysis. Some of these are described in :

US MIL HDBK 882D	System safety programme requirements
US MIL HDBK 764 (MI)	System safety engineering, design guide for army material

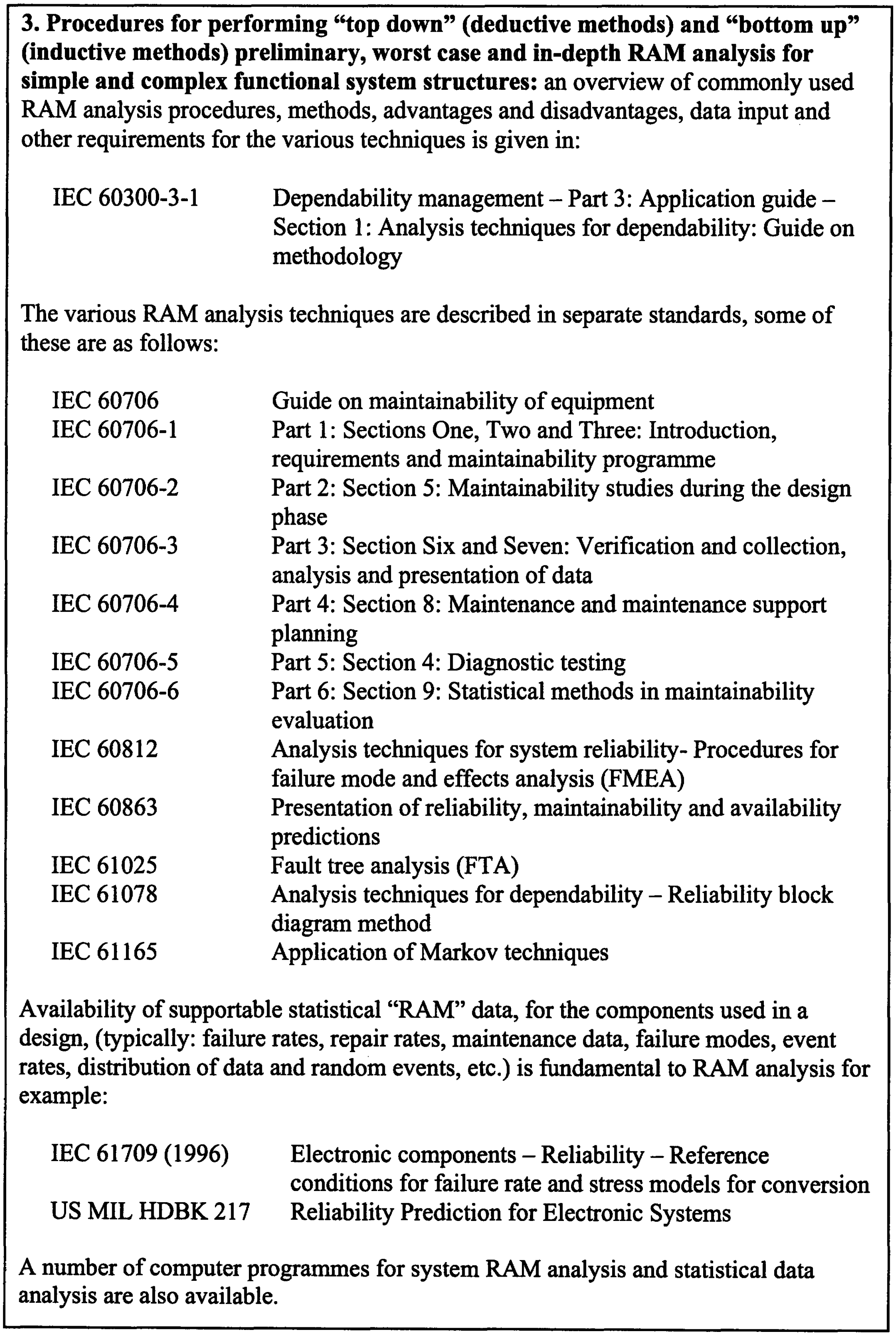
The same basic techniques and analysis methods listed for RAM (item 3) are also applicable for safety/risk analysis.

Also see IEC 61508, Parts 1 to 7, under the general title Functional safety of electrical/electronic/programmable electronic safety-related systems, consisting of the following parts:

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

Figure 3.5: Procedures for performing hazard and safety/risk analysis (Source: IEC 62278).

Here, "the same basic techniques and analysis methods listed for RAM" in Figure 3.5 are described as Figure 3.6.



3. Procedures for performing "top down" (deductive methods) and "bottom up" (inductive methods) preliminary, worst case and in-depth RAM analysis for simple and complex functional system structures: an overview of commonly used RAM analysis procedures, methods, advantages and disadvantages, data input and other requirements for the various techniques is given in:

IEC 60300-3-1	Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology

The various RAM analysis techniques are described in separate standards, some of these are as follows:

IEC 60706	Guide on maintainability of equipment
IEC 60706-1	Part 1: Sections One, Two and Three: Introduction, requirements and maintainability programme
IEC 60706-2	Part 2: Section 5: Maintainability studies during the design phase
IEC 60706-3	Part 3: Section Six and Seven: Verification and collection, analysis and presentation of data
IEC 60706-4	Part 4: Section 8: Maintenance and maintenance support planning
IEC 60706-5	Part 5: Section 4: Diagnostic testing
IEC 60706-6	Part 6: Section 9: Statistical methods in maintainability evaluation
IEC 60812	Analysis techniques for system reliability- Procedures for failure mode and effects analysis (FMEA)
IEC 60863	Presentation of reliability, maintainability and availability predictions
IEC 61025	Fault tree analysis (FTA)
IEC 61078	Analysis techniques for dependability – Reliability block diagram method
IEC 61165	Application of Markov techniques

Availability of supportable statistical "RAM" data, for the components used in a design, (typically: failure rates, repair rates, maintenance data, failure modes, event rates, distribution of data and random events, etc.) is fundamental to RAM analysis for example:

IEC 61709 (1996)	Electronic components – Reliability – Reference conditions for failure rate and stress models for conversion
US MIL HDBK 217	Reliability Prediction for Electronic Systems

A number of computer programmes for system RAM analysis and statistical data analysis are also available.

Figure 3.6: Procedure for performing RAM analysis excerpted (Source: IEC 62278).

(c) The standard describes the concept of safety integrity, and requires specifying safety integrity requirements for each safety function.

In the standard, the concepts of safety integrity and safety integrity level are defined as:

- **safety integrity**: likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time;
- **safety integrity level (SIL)**: one of the number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level with the highest figure has the highest level of safety integrity.

Safety integrity requirements for the systems and components of the application shall be specified in terms of the safety integrity level at the beginning of the system life cycle, and their achievements shall be confirmed later through the effective application of a combination of many techniques. Safety integrity correlates to the probability of failure to achieve required safety functionality. IEC 62278 does not define the correlation between safety integrity and failure probabilities for railway system and states that it is the responsibility of the Railway Authority. It should be noted that IEC 61508, which is one of normative references of IEC 62278, provides a generic correlation for electronic safety-related systems as shown in Table 3.5.

Table 3.5: Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation (Source: IEC 61508).

Safety Integrity Level	Description	High demand or continuous mode of operation (probability of a dangerous failure per hour)
1	low	$\geq 10^{-6}$ to $< 10^{-5}$
2	medium	$\geq 10^{-7}$ to $< 10^{-6}$
3	high	$\geq 10^{-8}$ to $< 10^{-7}$
4	very high	$\geq 10^{-9}$ to $< 10^{-8}$

Another example of safety integrity is that IEC 62278 defines the relationship between safety integrity level and the minimum level of independence of those carrying out the functional safety assessment, as shown in Table 3.6. Since IEC61508 does not specify anything about this, this table should be applied to the safety assessment of railway system.

Table 3.6: Minimum levels of independence of those carrying out functional safety assessment (Source: IEC61508).

Minimum level of Independence	Safety Integrity Level			
	1	2	3	4
Independent person	HR	HR1	NR	NR
Independent department	-	HR2	HR1	NR
Independent organization	-	-	HR2	HR

HR: Highly recommended. In the table, either HR1 or HR2 is applicable, depending on a number of factors specific to the application. If HR1 is applicable then HR2 should be read as no requirement; if HR2 is applicable then HR1 should be read as no requirement applicable

NR: Not recommended

3.1.3 MIL-STD-882D

MIL-STD-882D: *Standard Practice for System Safety* is briefly reviewed in this subsection. Although this standard is primarily for U.S. Department of Defense (DoD) systems such as ballistic missiles, remote-piloted vehicles, and nuclear weapons, it is worthy of review here because IEC 62278 encourages Railway Authorities to refer to this standard for methods and tools to perform risk analysis as mentioned in the previous section and because this standard is very strong in the area of hazard analysis (Herrmann, 1999).

MIL-STD-882A: *System Safety Program Requirements* was issued in 1977, and the next version, MIL-STD-882B, in 1984 was the first to incorporate software safety. The current version, MIL-STD-882D, whose title became *Standard Practice for System Safety*, was published in 2000, following MIL-STD-882C in 1993, which deleted a clear distinction between hardware and software and integrated software into the entire process.

The purpose of this standard is to define an approach for the management of environment, safety, and health mishap risks caused by DoD systems. A notable feature of the standard is its great emphasis on system safety, which is defined as the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle. It states as follows:

> Integral to these efforts is the use of a system safety approach to manage the risk of mishaps associated with DoD operations. A key objective of the DoD system safety approach is to include mishap risk management consistent with mission requirements, in technology development by design for DoD systems, subsystems, equipment, facilities, and their interfaces and operation.

In terms of risk analysis, there is no significant difference between IEC 62278 and MIL-STD-882D. Both standards require analyzing risk and managing it. MIL-STD-882D, like IEC 62278, does not provide specific methods and tools, but recommends classifying mishap risk by mishap severity and mishap probability, using a mishap risk assessment matrix. Suggested mishap probability levels, suggested mishap severity levels, and example mishap risk assessment values in MIL-STD-882D are similar to those in IEL 62278, namely Tables 3.1, 3.2, and 3.4 respectively. (The small difference is that categories suggested in MIL-STD-882D are more specific than those in IEL 62278. For example, MIL-STD-882D assigns dollar values to property losses.)

It is important to note that a software hazard criticality matrix is developed in MIL-STD-882C, the predecessor of MIL-STD-882D. It states:

> The initial assessment of risk for software, and consequently software controlled or software intensive systems, cannot rely solely on the hazard severity and probability. Determination of the probability of failure of a single software function is difficult at best and cannot be based on historical data.

Subsequently, it introduces the concept of a mishap risk assessment matrix by potential hazard severity and software control categories, which demonstrate the degree of control that software exercises over the hardware. Software control categories are shown in Table 3.7, and a sample of a software risk assessment matrix based on software control categories is shown in Table 3.8. Although the concept of software control categories is eliminated in MIL-STD-882D, there is still a description of that in Software System Safety Handbook by Joint Software Safety Committee U.S. DoD (1997), which, Herrmann (1999) says, supplements MIL-STD-882D. (It is important to note that this approach is still controversial, and, for example, Leveson (2002) addresses counter opinions. She argues that the software that provides information to the human controller but does not directly issue control commands, is also safety-critical, since its behavior will affect the human controllers' decisions and actions.)

Table 3.7: Software control categories (Source: MIL-STD-882C).

Category	Definition
I	Software exercises autonomous control over potentially hazardous hardware systems, subsystems, or components, without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard occurrence. Software interlocks that prevent a hazardous event should be an integral part of the design process and verified.
Iia Iib	Software exercises control over potentially hazardous hardware systems, subsystems, or components, with time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate. Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow, or fail to prevent, the hazard occurrence.
IIIa IIIb	Software item issues commands over potentially hazardous hardware systems, subsystems, or components, requiring human action to complete the control function. There are several redundant independent safety measures for each hazardous event. Software generates information of a safety-critical nature used to make safety-critical decisions. There are several redundant independent safety measures for each hazardous event.
IV	Software does not control safety-critical hardware systems, subsystems, or components and does not provide safety-critical information.

Table 3.8: Example software hazard criticality matrix (Source: MIL-STD-882C).

Control Category	Hazard Category			
	Catastrophic	Critical	Marginal	Negligible
I	1	1	3	5
II	1	2	4	5
III	2	3	5	5
IV	3	4	5	5

Hazard Risk Index	Suggested Criteria
1	High risk – significant analysis and testing resources
2	Medium risk – requirements and design analysis and in-depth testing required
3-4	Moderate risk – high level analysis and testing acceptable with Managing Activity approval
5	Low risk – acceptable

Neither MIL-STD-882D nor IEC 62278 specify any tools or methods for identifying hazards and recommends referring for commonly used approaches to two sources below, which are just general guidance on various techniques.

- *Defense Acquisition Deskbook.* Wright Patterson Air Force Base, Ohio: Deskbook Joint Program Office. (Currently, *AT&L Knowledge Sharing System* by Defense Acquisition University, available at http://akss.dau.mil)
- *System Safety Analysis Handbook.* Unionville, VA: System Safety Society.

To sum up, none of the standards recommends specific approaches to identify system hazards and it is engineers' responsibility to determine which technique is appropriate.

3.1.4 Comparison between IEC 62278 and MIL-STD-882

There are some similarities between IEC 62278 and MIL-STD-882. Both standards put great emphasis on analyzing risk throughout all phases of the system life cycle and recommend using similar tables, as shown in Tables 3.1, 3.2, and 3.4, for risk assessment. However, there exists a considerable difference between them. In short, IEC 62278 adopts a reliability engineering approach, while MIL-STD-882D adopts a System Safety approach to assuring safety.

A reliability engineering approach is failure oriented: Engineers assume that safety can be achieved by increasing reliability of components, and focus on failure rate reduction, using various techniques such as redundancy. To put it another way, reliability engineers assume that safety and reliability are almost identical. It is the reliability engineering approach that IEC 62278, the railway standard, advocates. With regard to Figure 3.3, which shows inter-relation of railway RAMS elements, the standard describes:

> Attainment of in-service safety and availability targets can only be achieved by meeting all reliability and maintainability requirements and controlling the ongoing, long-term, maintenance and operational activities and the system environment.

This description implicitly demonstrates that the underlying concept of the standard is the reliability engineering approach.

Another example is the concept of safety integrity. Below are the definitions of safety integrity and reliability in the standard:

- **reliability**: probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2)
- **safety integrity**: likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

The difference between the two is that the term reliability refers to an item, while the term safety integrity refers to a system. (A system is defined in the standard as an assembly of sub-systems and components, connected together in an organized way, to achieve specified functionality.) Since safety integrity correlates to the probability of failure to achieve required safety functionality, the approach using safety integrity is definitely the reliability engineering approach.

On the other hand, MIL-STD-882D adopts a different approach that is called a System Safety approach. In the System Safety approach, safety has nothing to do with reliability, and never assumes that safety and reliability are almost identical; safety can be achieved through a systematic approach of hazard analysis, risk assessment, and risk management. The details of the System Safety approach will be described in Chapter 5.

To sum up, although IEC 62278 and MIL-STD-882D are similar on several points as mentioned early, the underlying concepts are completely different between the two. While MIL-STD-882 advocates the System Safety approach, IEC 62278, the railway standard, adopts the reliability engineering approach.

3.2 Current approaches to safety of maglev systems

3.2.1 German approach

Some papers describe approaches to safety assessment and safety approval in Germany, which are reviewed here. It is important to note that the description below does not necessarily cover all of the approaches, and some approaches may not be mentioned here.

Systems under consideration are Transrapid TR08, Shanghai maglev line, and Transrapid TR09.

Transrapid TR08

The TR08 is a 3-car pre-production vehicle, whose running test started in 1999 at the Transrapid test facility (TVE) in Emsland, Germany. Since the international standards or European standards explained in the previous section are relatively new (EN 50126 and IEC 62278 were issued in 1999 and 2002, respectively.), the assessment process of the TR08 was not based on the international standards, but on some German standards such as German ordinance on the construction and operation of maglev systems (Verordnung über den Bau und Betrieb der Magnetschwebebajnen, MbBO), according to Steiner and Sterinert (2006). They also state:

> For the safety relevant vehicle functions levitation, guidance, and braking, quantitative requirements were defined in the requirement specification. The tolerable rate for dangerous failures for these safe-life functions was given as $R \leq 10^{-6}$ /year. The fulfillment of these quantitative safety targets was demonstrated by fault tree analysis.

The Fault Tree Analysis (FTA) is a hazard analysis technique used to assess a system by identifying an undesirable event first and examining the range of potential events that could lead to the event. Figure 3.7 provides an example of a fault tree graphic from System Safety Society (1993).

In addition to this, Steinert (2004) states, a Failure Mode Effect Analysis (FMEA) was conducted in order to examine all primary structural elements such as an undercarriage and cabin of the TR08. The FMEA is also a hazard analysis technique that uses inductive logic to evaluate system hazards: It supposes a failure of sub-element first and determines the results or effects of it, classifying each potential failure according to its severity. Table 3.9 is an example of the FMEA worksheet from System Safety Society (1993).

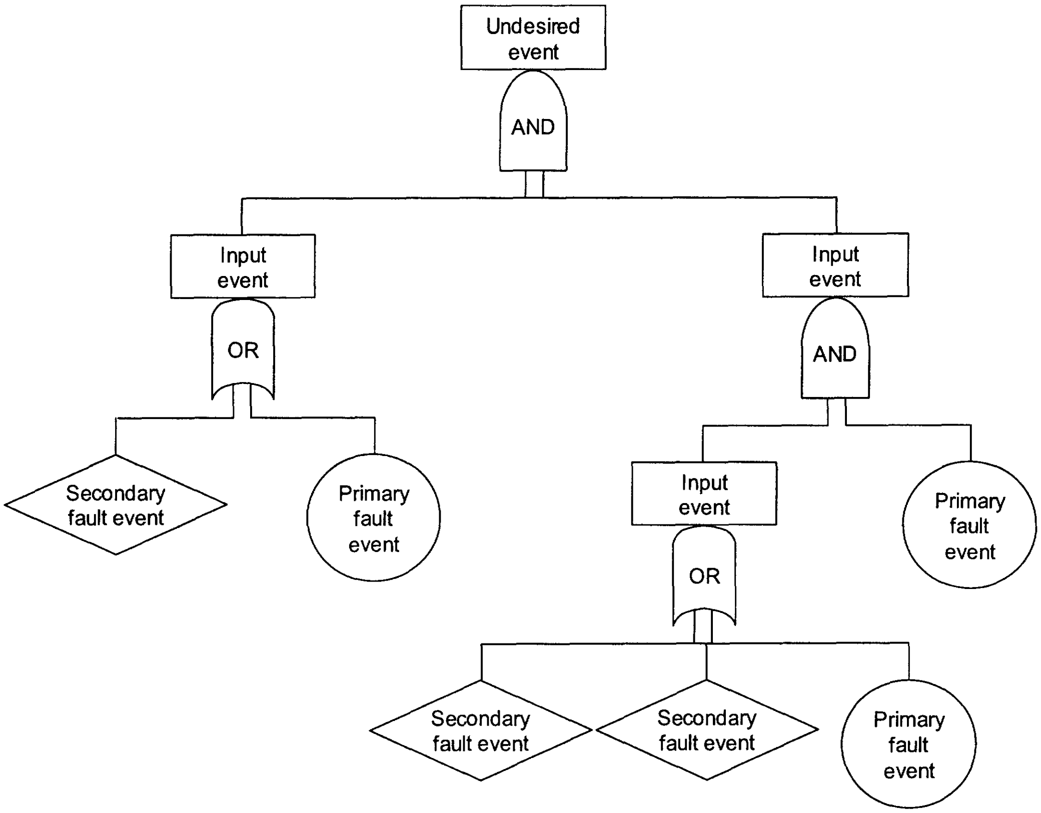


Figure 3.7: Example of a fault tree graphic (Source: System Safety Society, 1993).

Table 3.9: Sample of the FMEA worksheet (Source: System Safety Society, 1993).

Item	Failure Modes	Causes of Failure	Possible Effects	Probability of Occurrence	Criticality	Possible Action to Reduce Failure rate or effects
Explosive	Cracking Voids	Unusual stresses during cure Extreme temperatures Aging	Low yield Failure to ignite Uneven burn rate	0.0025	Critical	Carefully controlled production Storage and operation only within specified temperature limits
Casing	Rupture	Poor Quality Control	Accidental detonation	0.0007	Critical	Rigid QC of manufacturing process Contract requirements Inspection of materials

Shanghai maglev line

Shanghai maglev, which began its operation in 2004, is the first commercial line of maglev systems. In addition to the railway system, which is primarily based on the German maglev systems Transrapid, the European concepts of safety assessment and approval were introduced (Tao, 2004). The central part and basis of the safety verification of the Shanghai maglev line is the Safety Concept, according to Wolfgang (2004). The idea of the Safety Concept comes from German Maglev Law, MbBO, and its core is the risk analysis and safety measures (Tao, 2004). The MbBO requires a third-party assessor to compile documents named the Safety Concept, which include the safety procedure, overall system hazard analysis, and proof of safety measures. Tao (2004) states that EN 50126 was a reference material about the system hazard analysis.

Sawilla and Otto (2004) describe, in their paper, the safety certification process of the Operation Control System (OCS) implemented on the Shanghai maglev line. The OCS is a key system that administers planning, monitoring, and safeguarding of train operation such as automatic train operation and automatic train protection. They state as follows:

> For the Shanghai Maglev project the German guideline Mü8004 (Technical Principles for the Approval of Railway Signalling Equipment) issued by the Federal Railway Authority (Eisenbanhn-Bundesamt, EBA) was agreed as the contractual basis for the assessment and approval of OCS since final versions of the European railway standards weren't available at this time. The Guideline Mü8004 distinguishes safety relevant ("vital") and not safety-relevant ("non-vital") requirements. Further graduations of safety levels do not exist.... However, in general, the development of OCS and the verification and validation activities have been executed similar to the approach stated in EN 50126 and EN 50159. For "key safety functions" quantitative hazard rates have been calculated and verified in addition and included in the respective safety evidence documents.

Transrapid TR09

The TR09, a newly developed vehicle in 2007, is a prototype of the maglev vehicle for the Munich airport project. It is primary based on the TR08, but there is a notable range of modifications between the TR08 and TR09 in terms of technology. Additionally, the safety assessment process has changed: The CENELEC railway standards, namely EN 50126, EN50128, and EN50129 have to be applied for the TR09 safety assessment. Though the main target of EN50129 is railway signaling, its applicability to other safety related electronic systems is widely recognized. Therefore, EN50129 is adopted not only for signal systems but also for the safety relevant vehicle electronics (Steriner & Steinert, 2006).

No information is available about risk analysis techniques that were adopted.

To sum up, the safety assessment for every maglev system in Germany is based on the international standards or some other German standards that are similar to the international standards, and quantitative analysis with FTA and FMEA techniques is preferred to analyze safety. It is also important to add that there is no description of designing for safety, rather than safety assessment, which implies that their focus is on safety assessment, rather than designing for safety.

3.2.2 Japanese approach

Although no paper about Japanese approach to safety of maglev systems is available, there are some papers about approach to safety of Japanese conventional train systems, which are worthy of review here.

As for standards, Hirakawa (2006) states that Japanese railway engineers don't have design standards that they can rely on. This is not his personal idea and backed up by Braband, Hirao, and Luedeke (2003), who write that Japanese safety guidelines, which are partly based on IEC 61508 concepts, are treated as guidelines, instead of mandatory regulations. These demonstrate that there is a significant difference between Japan and Europe in terms of the attitude to and application of standards.

Braband, Hirao, and Luedeke (2003) also describe quantitative analysis in Japan as follows:

> In Japan there is a feeling that quantitative analysis should be only applied for the purpose of identifying the most critical part and confirming the consecutive safety approach results.... By allocating numerical values to each hazard, it indeed becomes possible to identify the more dangerous points and to take necessary measures against them. In this point, however, absolute values are not necessarily important, and relative values are quite adequate.

Another source is Mizoguchi and Sato's (2006) reference book about RAMS methods. According to them, Japan raised an objection to including RAMS methods in the international standard IEC 62278 because Japanese approaches were not necessarily consistent with RAMS approach. However, as RAMS methods were incorporated in the international standard in 2002, Japan, as a member of World Trade Organization (WTO), is required to comply with RAMS methods. (According to the WTO agreement, a member of WTO should make an order requirement consistent with international standards including IEC 62278. The goal of this agreement is to facilitate international trade and investment by eliminating technical trade barriers.) Under these conditions, the purpose of this book is to provide a short summary of RAMS approaches described in IEC 62278 for railway engineers in Japan.

Some important descriptions from the viewpoint of safety are as follows.

(a) Japan is one of a few countries that do not evaluate RAMS of rail systems systematically.

The way the Japanese railway companies adopt new technologies is as follows: First, factory tests are conducted for new products. After their performance and reliability are confirmed, the next step is long-term tests, which are carried out using a few commercial trains. When there is no malfunction through the long-term tests, the products are finally incorporated into mass-produced trains. During these steps, quantitative targets for reliability are not necessarily provided. The goal is to make them as reliable as conventional products in the past.

Mizoguchi and Sato (2006) insist that some of the RAMS methods are already incorporated into Japanese approaches, unintentionally. For example, operating companies and manufacturing companies jointly conduct the study of failures over the whole life cycle on a tacit understanding, and their results are effectively utilized to improve the performance of the products. They conclude that Japanese approaches are never totally against RAMS methods; however, the Japanese way is not organized at all.

(b) Business writings such as contractual documents and specification documents in Japan are exceedingly simple and vague, compared to those in European countries.

In addition to risk analysis, configuration management, which is defined below, is an essential part of RAMS approaches.

- **configuration management**: discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control change to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements

However, Japanese business writings are defective on an international basis because they are too simple and vague. Mizoguchi and Sato (2006) suggest that flawed Japanese paperwork could be a big hurdle when Japanese companies try to introduce RAMS methods and recommend that they should pay much attention to configuration management in the early stages.

(c) Quantitative analysis with FTA or FMEA is recommended to analyze safety of railway systems.

As described before, quantitative analysis is not prevalent in Japan. Based on this situation, the book recommends that Japanese companies become familiar with quantitative techniques such as FTA and FMEA to analyze the safety of railway systems. (It is important to note that IEC 62278 does not require analyzing safety quantitatively.)

To sum up, Japanese approaches are not necessarily based on any standards including IEC 62278 or any methods such as RAMS methods. Recently, they have been forced to incorporate RAMS methods. As part of their effort, they are focusing on quantitative techniques for safety analysis, which have not been so preferred in Japan.

Chapter 4

Lessons Learned from the Fukuchiyama Line Derailment

On April 25, 2005, in Amagasaki, Hyogo Prefecture, near Osaka, Japan, the Rapid Service train on the West Japan Railway Company (JR-West) Fukuchiyama Line derailed at a high speed, crashing into an apartment building. 'Of the roughly 700 passengers onboard, 106 passengers, in addition to the driver, were killed and 562 others were injured in this accident. This was Japan's most serious accident in forty years. There was no malfunction in the train and in the ground equipment. The train was driven above the speed limit on a tight curve, and it failed to follow the track.

In this chapter, a Systems Theory Accident Modeling and Processes (STAMP) analysis and System Dynamics model on this accident are developed. It is important to note that this accident had nothing to do with maglev systems. This was an accident in the conventional railway system. However, there are good reasons to analyze this accident here. Most of all, it was Japan where this accident occurred. Japan is considered to be an advanced country in the field of railway technology (Kubota, 2000). For example, the Shinkansen, a high-speed bullet train in Japan, is one of the most successful high-speed railway lines in terms of safety all over the world (Yamanouchi, 2005). This train of the accident was operated by JR-West, one of the companies that was formed upon the privatization and split-up of Japanese National Railways (JNR) in 1987. JR-West provides passenger railway transportation services on a network of lines that extends through 18 prefectures and has a total route length of approximately 5,000 kilometers. This network covers around one-fifth of Japan's land area. In the 18 years since the dissolution of JNR, JR-West has overcome many challenges, including the Great Hanshin-Awaji Earthquake, and has forged ahead with the goal of forming and reinforcing a strong management foundation, according to West Japan Railway Company (2006). In 2004, JR-West successfully became a fully-privatized company after the completion of stock sell-off. In conclusion, a representative company of railway industry in Japan, which is an advanced country in the field of railway, caused this accident. It is assumed that this kind of sophisticated company in terms of railway technology would operate a maglev system in the future. From this point of view, there must be lessons learned from this accident. Additionally, as mentioned in the previous chapters, Japan is one of the countries developing maglev systems.

The Aircraft and Railway Accidents Investigation Commission (ARAIC) reports were the source for this analysis. The ARAIC is a Japanese commission, which was established to scientifically investigate the causes of aircraft and railway accidents from a fair and impartial stance, and help prevent accidents. The ARAIC is a national body with a high degree of independence, and broadly comparable to the National Transport Safety Board (NTSB) in the USA in terms of its brief (Sato, 2002). The reports in Japanese can be easily accessed at the ARAIC web site, http://www.mlit.go.jp/araic. Also Yamaguchi (2007), a professor at Doshisha University in Japan, personally investigated this accident and published a book, which was referred to in addition to the ARAIC reports.

After brief reviews of a STAMP analysis and System Dynamics model, first the proximate events, then the STAMP analysis and System Dynamics model of this accident are presented, followed by lessons learned.

4.1 Reviews of a STAMP analysis and System Dynamics model

4.1.1 Investigating and analyzing accidents

Investigating and analyzing accidents that occurred in the past is important for preventing further accidents, but sometimes it is hard to model accidents because of their complexity. According to Braband (2002), the requirements of frameworks to analyze accidents are as follows.

- A method should be easy for average engineers to apply. Preferably it requires a minimum amount of training and no proprietary tool.
- A method should provide a graphical representation.
- A method should allow "modular approaches", which means that several engineers can work on an analysis at the same time, sharing their tasks.

Various frameworks have been proposed to effectively analyze incidents or accidents (Braband, 2002). For example, the U.S. Navy, Army, and Air Force have adopted the Human Factors Analysis and Classification System (HFACS), which is now relatively well known within many sectors of aviation (Wiegmann & Shappell, 2003). This framework is mainly for human error in aviation and based on the well-known Swiss cheese model of accident causation developed by Reason (1990). Unfortunately, however, the causes of accidents in railway engineering are not investigated systematically (Braband, 2004).

A Systems Theory Accident Modeling and Processes (STAMP) analysis and System Dynamics will be used to analyze the Fukuchiyama Line derailment accident. A STAMP analysis has been developed by Nancy Leveson at Massachusetts Institute of Technology (MIT). System Dynamics was originally developed by Jay Forrester at MIT in the 1950's for managers and public policymakers to use to design and implement high-level policies for complex systems (Sterman, 2000). Leveson (2002) has proposed that safety issues be analyzed using a combination of STAMP and System Dynamics.

4.1.2 Systems Theory Accident Modeling and Processes analysis

In this subsection, the Systems Theory Accident Modeling and Processes (STAMP) analysis is reviewed. (Leveson (2002) is the source for this review if not otherwise specified.)

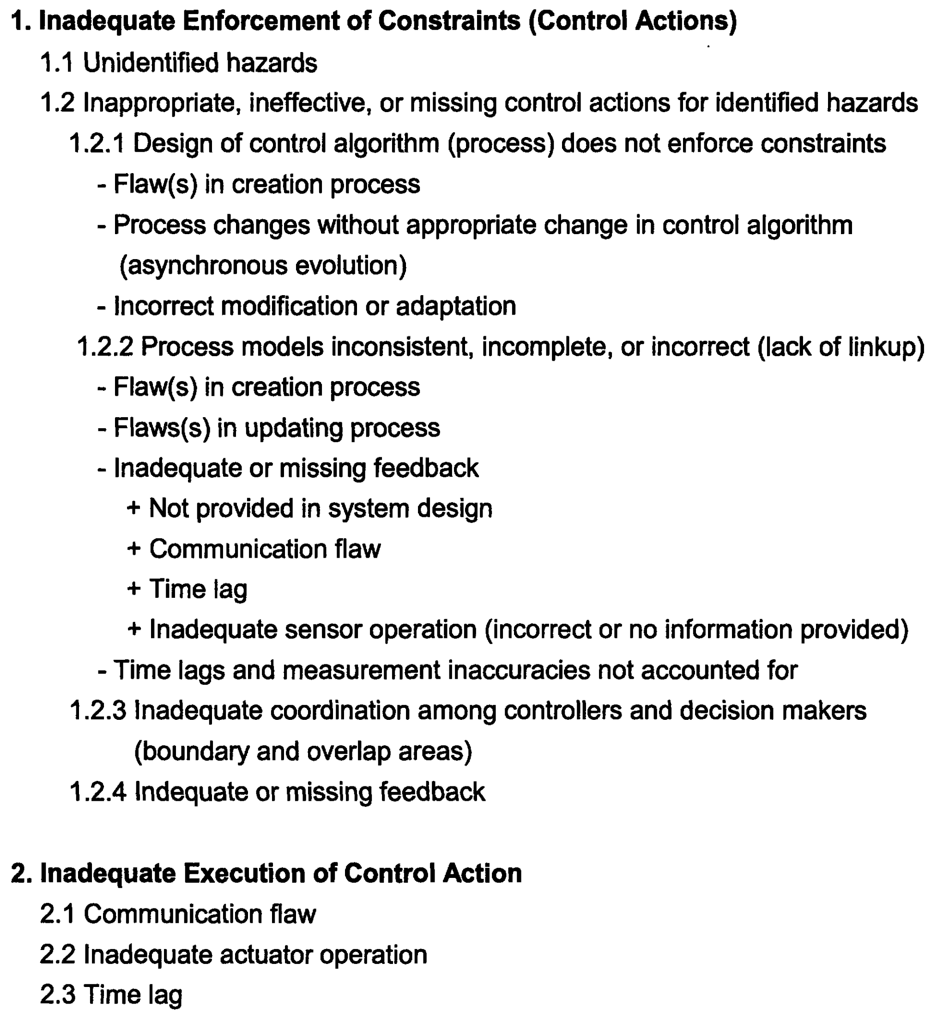
Two pairs of ideas are the foundation of STAMP: (1) emergence and hierarchy and (2) communication and control.

Emergence and Hierarchy: Safety is an emergent property, which means that safety is not a property of individual component. Rather, safety is a system property and must be addressed in terms of all the systems together and their interactions. It is important to note that the relationship among components is defined hierarchically; complex systems are defined in terms of a hierarchy of levels of organization. Safety, which is an emergent property of systems, only exists at the system level.

Communication and Control: In a hierarchy of levels of components, a system component at a higher level controls another component at a lower level, while the latter communicates with the former, which is called feedback. This relationship of communication and control between components of different levels is another key part of basic systems theory.

In STAMP, accidents are viewed as a result of inadequate control. There are various kinds of inadequate control actions in the design, development, and operation of the system. In some cases, inconsistent design results in inadequate control. Sometimes, poor quality control in manufacturing is a trigger. Also, a system component failure and human operator error could cause inadequate control actions. In this view, accidents necessarily involve inadequate control.

Based on these ideas, Leveson (2002) classifies control flaws leading to hazards, as shown in Figure 4.1. She pays close attention to ideas of asynchronous evolution, where one system component evolves without coordination of other system components, and boundary and overlap areas, where a distinction between components is vague in terms of which component is in charge of control. (Leplat (1987) originally introduced these two ideas as categories of dysfunctionings that often lead to an accident, based on studies conducted in the iron and steel industry.)



1. Inadequate Enforcement of Constraints (Control Actions)

1.1 Unidentified hazards
1.2 Inappropriate, ineffective, or missing control actions for identified hazards
  1.2.1 Design of control algorithm (process) does not enforce constraints
    - Flaw(s) in creation process
    - Process changes without appropriate change in control algorithm (asynchronous evolution)
    - Incorrect modification or adaptation
  1.2.2 Process models inconsistent, incomplete, or incorrect (lack of linkup)
    - Flaw(s) in creation process
    - Flaws(s) in updating process
    - Inadequate or missing feedback
      + Not provided in system design
      + Communication flaw
      + Time lag
      + Inadequate sensor operation (incorrect or no information provided)
    - Time lags and measurement inaccuracies not accounted for
  1.2.3 Inadequate coordination among controllers and decision makers (boundary and overlap areas)
  1.2.4 Indequate or missing feedback

2. Inadequate Execution of Control Action

2.1 Communication flaw
2.2 Inadequate actuator operation
2.3 Time lag

Figure 4.1: Classification of control flaws leading to hazards (Source: Leveson, 2002).

In practice, the first step to conduct a STAMP analysis is to identify system hazards and to construct a hierarchical control structure. It is important to note that the control structure can include socio-technical components, software, and human operators, which are considered to be among the most important factors that play a major role in current complex system accidents. Figure 4.2 is a general form of a model of socio-technical control structure. Once the control structure is established, the next step is to determine for each component what controls were inadequate and why. The general description of each component in the control structure is as follows. (The below is slightly different from the original one proposed by Leveson (2002), but the author believes that this is consistent with her latest ideas.)

- Safety Requirements and Constraints
- Context in Which Decisions Made
- Inadequate Control Actions
- Mental Model Flaws
- Feedback Flaws
- Inadequate Coordination among Multiple Controllers

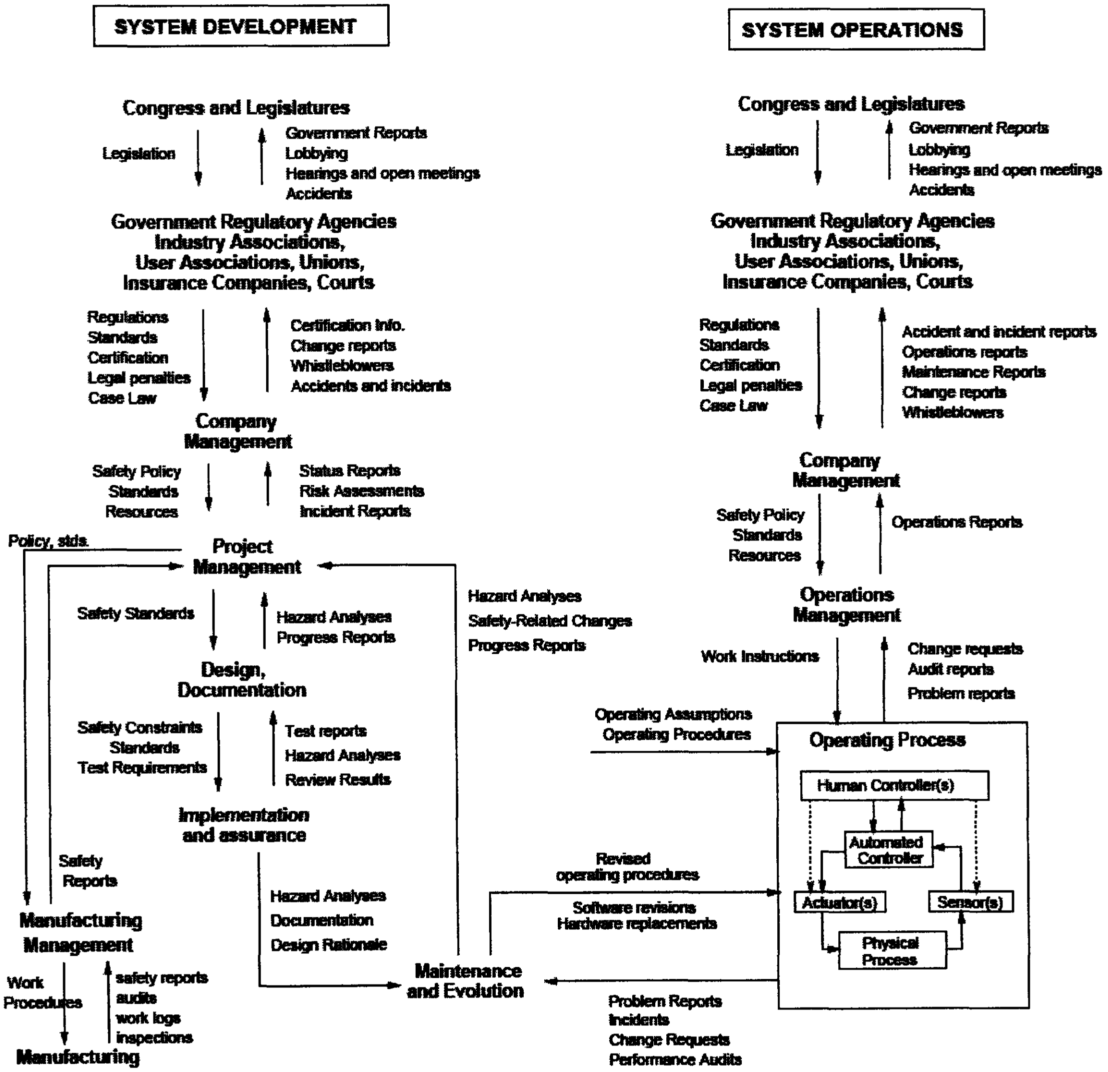


Figure 4.2: General form of a socio-technical control structure (Source: Leveson, 2002).

4.1.3 System Dynamics

In this subsection, System Dynamics modeling is reviewed. (Sterman (2000) is the source for this review if not otherwise specified.)

System Dynamics is a tool and method for modeling the structure and dynamics of complex systems for the analysis of policy and strategy. Jay Forrester originally focused on business and public applications. His idea is that the complexity of the systems in which we live is growing at increasing rates, so that we need to expand the boundaries of our mental models by a tool such as System Dynamics for effective decision making and learning without unanticipated side effects. Another important advantage is that System Dynamics enables us to conduct computer simulations, by which we can design more effective policies and organizations.

According to System Dynamics theory, the keys to modeling the dynamics of current complex systems are (1) the feedback processes and (2) the structures of the stock and flow.

Feedback Process: There are just two types of feedback loops, positive (or self-reinforcing) and negative (or self-correcting) loops. Sterman (2000) argues that "all systems, no matter how complex, consist of networks of positive and negative feedbacks, and all dynamics arise from the interaction of these loops with one another."

Positive loops tend to reinforce and amplify variables in the loop. Figure 4.3 represents the structure of the positive loops in System Dynamics modeling. The arrow with a + sign at the arrowhead from Variable 1 to Variable 2 indicates that an increase in Variable 1 leads to an increase in Variable 2 and that a decrease in Variable 1 leads to a decrease in Variable 2. To put it another way, the arrow with + represents that the effect is positively related to the cause. The arrow from Variable 2 to Variable 1 represents the same relation because there is also a + sign at the arrowhead. With this loop, Variable 1 and Variable 2 would both increase or decrease exponentially; therefore it is called a self-reinforcing loop.

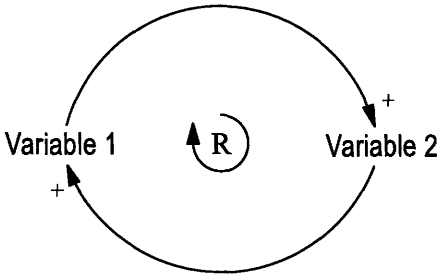


Figure 4.3: Positive feedback loop structure.

On the other hand, a negative loop acts to counteract change, and the model of its structure in System Dynamics modeling is shown in Figure 4.4. The arrow with a – sign at the arrowhead from Variable 2 to Variable 1 indicates that an increase in Variable 2 results in a decrease in Variable 1 and that a decrease in Variable 2 results in an increase in Variable 1. As a result, in the case of this structure, Variable 1 and Variable 2 would balance at some points over time; therefore it is called a self-correcting loop.

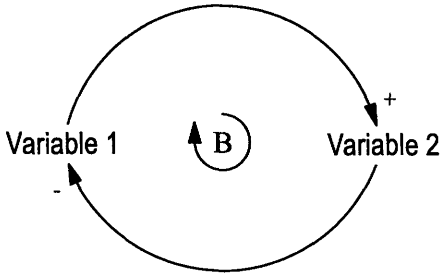


Figure 4.4: Negative feedback loop structure.

The feedback structure of systems is shown by causal loop diagrams, which consist of variables connected by arrows denoting the causal influences among the variables, as shown in Figures 4.3 and 4.4. Figure 4.5 is an example of causal loop diagrams from Sterman (2000). The loop on the left-hand side of the model shows a reinforcing loop, which means that the more births, the more people and that the more people, the more births. Birth rate is also positively affected by fractional birth rate. On the other hand, the loop on the right-hand side indicates a balancing loop, which means that the more population, the more deaths and that the more deaths lower the population. Death rate is negatively influenced by average lifetime. ("R" and "B" in the loops indicate the positive (reinforcing) loops and negative (balancing) loops respectively.)

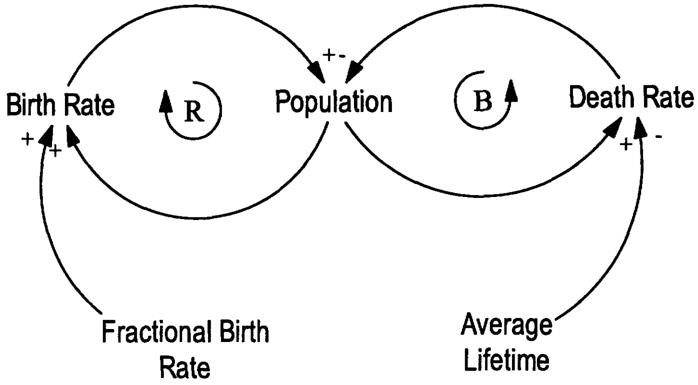


Figure 4.5: Example of causal loop diagrams (Source: Sterman, 2000).

Stocks and Flows: Another central concept of System Dynamics is stocks and flows. In System Dynamics modeling, variables that are considered to be accumulation are called stocks, which are represented by rectangles. Along with rectangles, a pipe pointing into/from the stock represents inflows/outflows, which rates are controlled by valves. Also, clouds represent the sources and sinks for the flows, which are assumed to have infinite capacity. The structure of all stocks and flows is composed of these elements. Figure 4.6 represents an example of stocks and flows from Sterman (2000). The valve on the left-hand side labeled production controls the inflow to the stock of inventory. Increasing production rate would increase inventory. The valve on the right-hand side labeled shipments controls the outflow from inventory. When the rate of shipments is high, the amount of inventory would decrease subsequently.

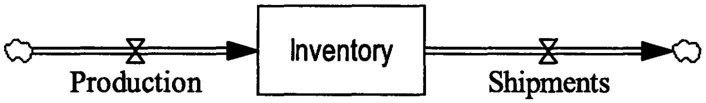


Figure 4.6: Example of stocks and flows (Source: Sterman, 2000).

Using the causal loop diagrams and the stocks and flows, every complex system can be modeled so that decision makers can analyze it and determine a strategy, sometimes conducting numerical simulations.

Systems are never static, but dynamic; systems continuously change to achieve their goals and to react to changes in themselves and their environments. Also, accidents are viewed as the result of inadequate control structures that evolve over time. From this point of view, Leveson (2002) proposes to apply System Dynamics to safety issues and argues that System Dynamics models can show how the aptitude and behavior of the components are greatly affected by each other and how and why such behavior may change in the future. There are many case studies available, such as a public water supply contamination accident in Ontario, Canada (Leveson, 2002), the Space Shuttle Columbia accident in 2003 (Leveson & Cutcher-Gershenfeld, 2004), and a security problem in the U.S. air transportation system (Laracy, 2007). Figure 4.7 shows a simplified model of the dynamics behind the space shuttle Columbia loss.

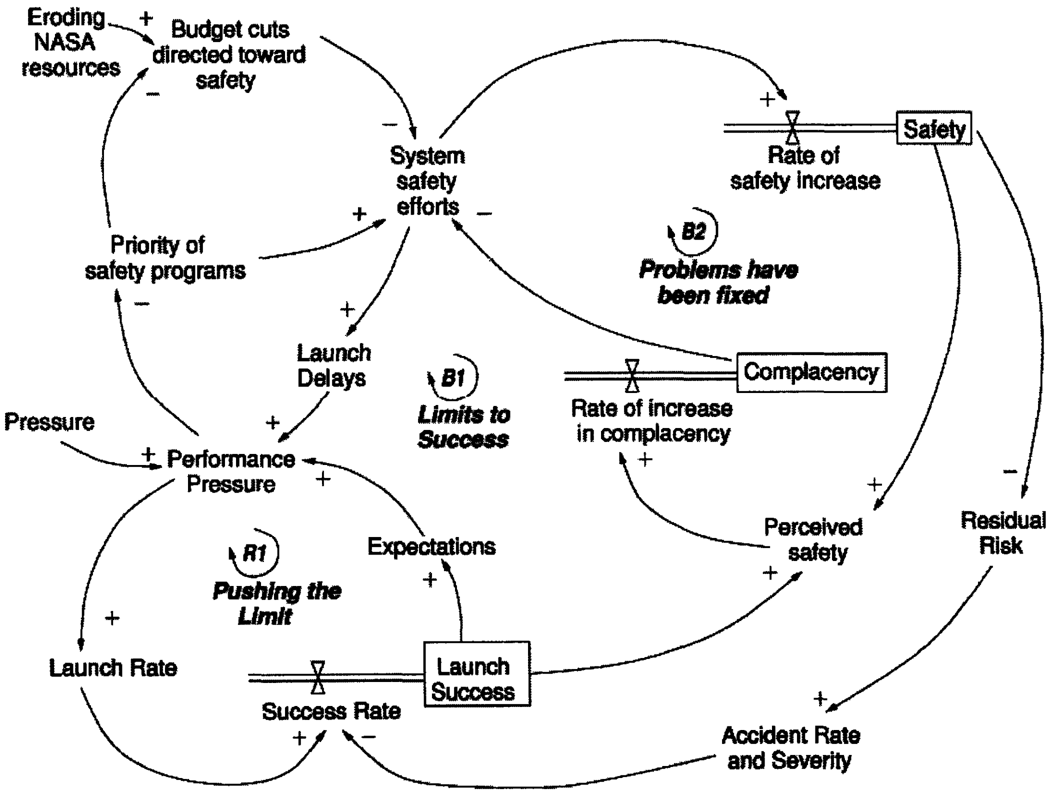


Figure 4.7: Simplified model of the dynamics behind the space shuttle Columbia loss (Source: Leveson & Cutcher-Gershenfeld, 2004).

4.2 The Fukuchiyama Line Derailment Accident

4.2.1 Proximate events on the Fukuchiyama Line

It was a driver's second day of a two-day-long track on April 25, 2005. His driving started at 06:48 at Hanaden Station in Osaka, Japan and would have ended at 09:58 at Kyobashi Station if there had been no accident. The driving record on the day of the accident is shown in Figure 4.8.

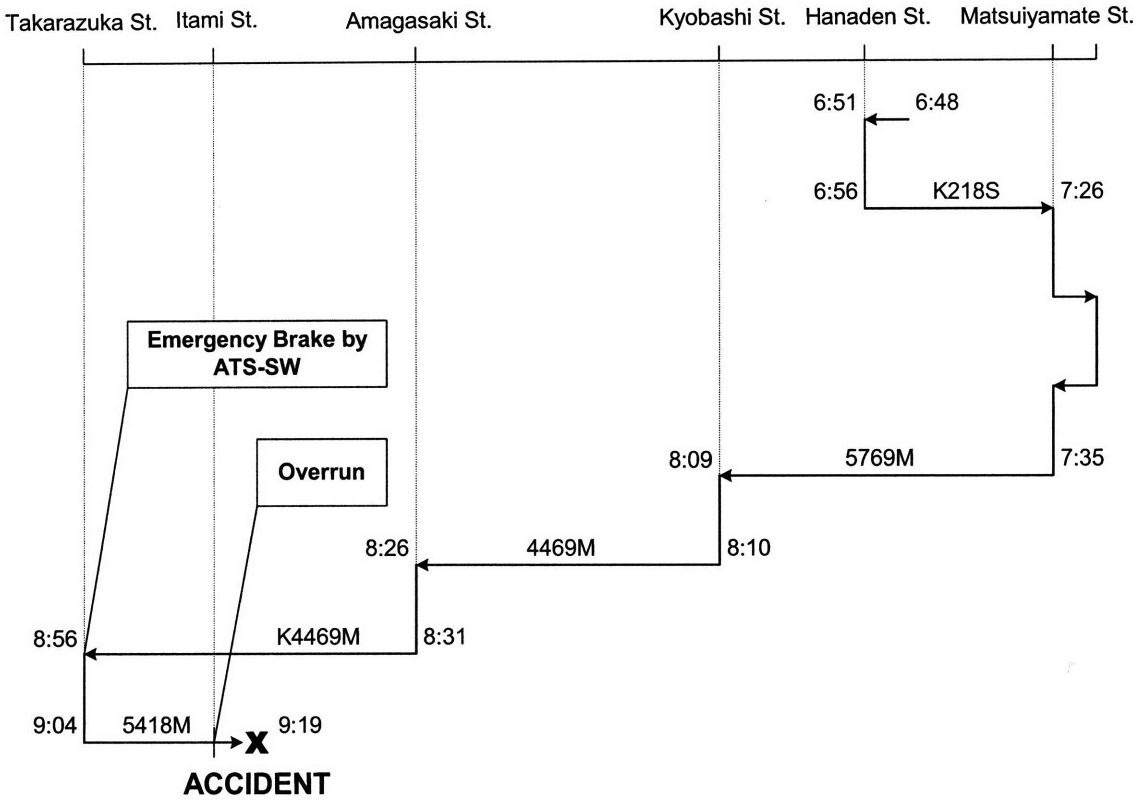


Figure 4.8: Driver's driving record on the day of the accident.

There were no major problems about the first trains, trains number K218S, 5769M, and 4469M, although the trains were slightly behind schedule by about one minute. ("K" before train numbers denotes deadhead trains.) On 4469M, the maximum regular brake was automatically activated by Automatic Train Stop (ATS) system near Kashima Station. ATS is a train system that will automatically stop a train if a certain situation happens, such as an unresponsive train operator, an earthquake, a disconnected rail, and a train running over a stop signal. In this case, the ATS brake was activated due to a slight over-speed. However, this was not an unusual situation, and it was assumed that this ATS brake had nothing to do with the accident that happened afterward. (After the accident, the investigation revealed that the configuration of ATS near Kashima Station was wrong so that the brake was mistakenly activated. Details will be discussed later.)

The first mistake conducted by the driver occurred on K4469M at Takarazuka Station. Approaching the station, the train passed through a diverging device at about 65 kilometers per hour where the speed limit was set at 40 kilometers per hour. As a result, the emergency brake was automatically activated by ATS again. The brake forced trains to stop far before Takarazuka Station, which caused additional delays. The train arrived at Takarazuka Station about 44 seconds late. According to the traffic signal before the station, the speed limit on the truck can be set to 65, 55, or 40 kilometers per hour, although the traffic signal for this train K4469M showed the 40-kilometers-per-hour limiting speed. The reason for this 25 kilometers per hour over-speed is not clear at all; however, it is suggested that the driver might have mistakenly understood the traffic signal. Also, the investigation revealed that some drivers felt seriously drowsy during K4469M. There was a possibility that the driver's consciousness level was affected by his sleepiness.

The next mistake, namely the overrun at Itami Station, happened on 5418M following K4469M. Approaching Itami Station, the voice equipment was activated at the point 643 meters before the station. This is an alarm system that raises a voice saying, "Stop at a station," when a running speed is over the designated one. The primary purpose is to prevent faults of sweeping through stations without making scheduled stops. But in this case the driver kept on coasting when the first female voice alarm sounded. It was when the second male voice alarm sounded, 6 seconds after the first alarm, that the driver began to apply both the maximum regular brake and the backup brake. It is important to note that the driver did not apply the emergency brake. One of the probable reasons is that he mistakenly thought the combined usage of the maximum regular brake and the backup brake could produce a greater speed reduction than the emergency brake could, which was not the case. Some drivers believed this according to the questionnaire result after the accident. Another probable reason is that he was aware that he had to report the usage of the emergency brake to supervisors while the backup brake was exempt from reporting. The train could have stopped at the right position if the emergency brake had been activated. Also, the investigation report concluded that the probable reason of the late braking was that he was distracted from driving because of the previous mistake on K4469M. The late and small braking resulted in 72-meter overrun at Itami Station.

The accident occurred after the train left Itami Station one minute and twenty seconds behind schedule at 9:16'10. As soon as the conductor finished the announcement to passengers about the next station, the driver called the conductor via an in-car telephone and asked the conductor to underreport the overrun distance to the ground control center. It was when the conductor said the overrun distance was quite big that a passenger approached the conductor's office and knocked on the door. The passenger asked the conductor to apologize for the overrun; therefore, the conductor brought the in-car telephone call to an end. Because the conversation was suddenly terminated due to the passenger, it is supposed that the driver had an impression that his request to underreport the overrun distance was rejected by the conductor. He had no ideas about what was going on in the conductor's office.

The train accelerated the speed until it reached 124 kilometers per hour, which was slightly over the speed limit of 120 kilometers per hour. (It is estimated that the in-car speed meter indicated 121 or 122 kilometers per hour due to an accident error, which is discussed later.) Subsequently the train shifted into coasting operation, and it was about one minute and twelve seconds late when the train passed Tsukaguchi Station at 9:18'22.

The train kept on coasting and passed the point where the brake should have been applied, without any braking. It was 116 kilometers per hour when the train went around a curve with a radius of 300 meters where the speed limit was set to 70 kilometers. Some regular brakes were applied for about 4 seconds after that, but the train couldn't follow the track at the curve because of the overspeed, resulting in the overturn of the first cabin at 9:18'54.

The overturned first cabin broke through a parking area on the first floor of a nearby apartment and crashed into the far wall of the parking area. The second cabin heavily impacted against a column of the apartment. Among seven cabins, the first five cabins were derailed.

106 passengers and a driver were killed in this accident, and 562 passengers were injured. Most of the fatalities were in the first two cabins.

4.2.2 System hazards, system safety constraints, and control structure

In this subsection, the system hazards, the system safety constraints, and the hierarchical control structure are identified.

The system hazard related to the Fukuchiyama Line derailment accident is derailment of vehicles. This hazard leads to the following system safety constraint:

The safety control structure must prevent derailment of vehicles.

1. Vehicles must not be driven over the speed limit.
2. Ground equipment must reduce the speed of vehicles if they run over the speed limit.

The safety control structure is given in Figure 4.9. In this figure, rectangles with straight lines are organizations within JR-West while rectangles with dashed lines are outside JR-West. It is important to note that JR-West is a company that manages the whole railway system, from infrastructure to train operations; Japanese railway companies possess infrastructure and rolling stocks as well as operate daily trains. On this point, it is quite different from European railway system in which train operating companies, infrastructure holding companies, and rolling stock leasing companies exist separately.

The government authority for railway in Japan is the Ministry of Land, Infrastructure and Transport (MLIT). According to the MLIT website, the MLIT has a legislative responsibility to implement transportation policies, and one of the five goals of the MLIT administration is to ensure traffic safety without ever assuming absolute safety.

One of the few tasks that JR-West isn't directly involved in is manufacturing; JR-West never manufactures anything although the company maintains the system once it is purchased. On the other hand, it is JR-West or JR-West's Rolling Stock Department in particular that draws up design specifications and confirms that the specifications are fulfilled. The line between Rolling Stock Department and Manufacturing Company in Figure 4.9 represents this relationship.

As well as the MLIT and manufacturing companies, each department or organization within JR-West plays a role in enforcing the safety constraints. Their safety requirements and constraints are respectively discussed in the later sections.

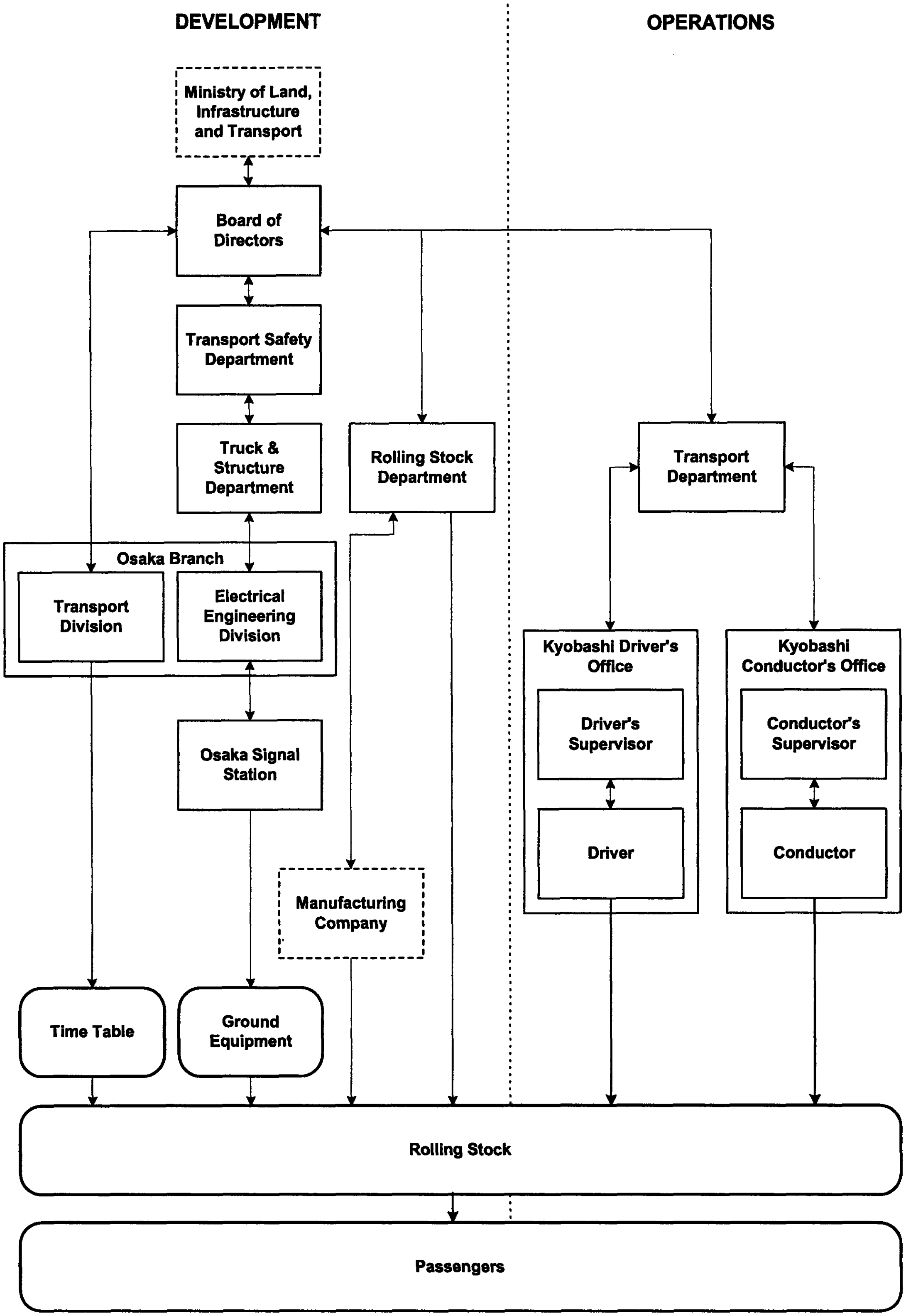


Figure 4.9: Basic railway safety control structure. Rectangles with sharp corners are controllers while rectangles with rounded corners represent material or immaterial products. In addition, rectangles with continuous lines are organizations within JR-West while rectangles with dashed lines are outside JR-West.

Following the STAMP procedure, the inadequate control in terms of enforcing the safety constraints by each component in the control structure is described in Sections 4.2.3 through 4.2.9.

4.2.3 Physical process view of the accident

The accident investigation revealed that there was no malfunction in rolling stocks and ground equipments such as tracks and signals. Every component was working correctly, as expected. The physical components in the accident can be simplified as in Figure 4.10, and the safety constraint being enforced at this level is that rolling stocks must be free from derailment.

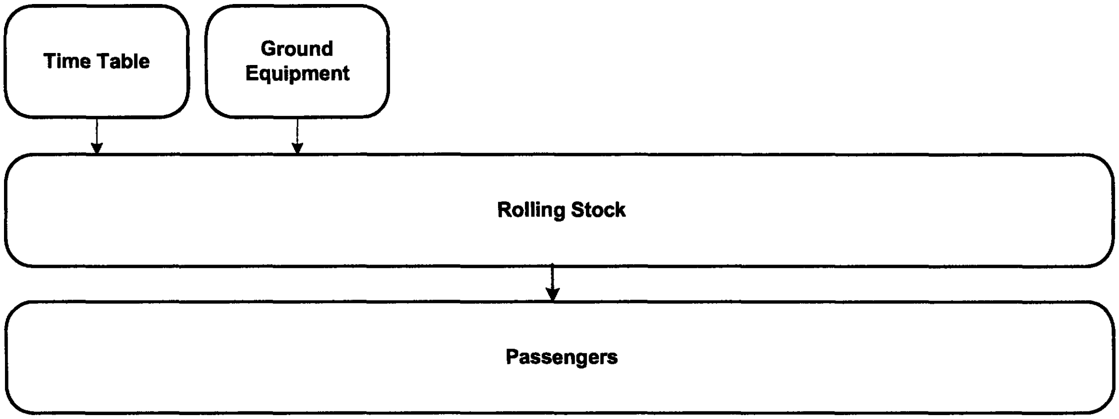
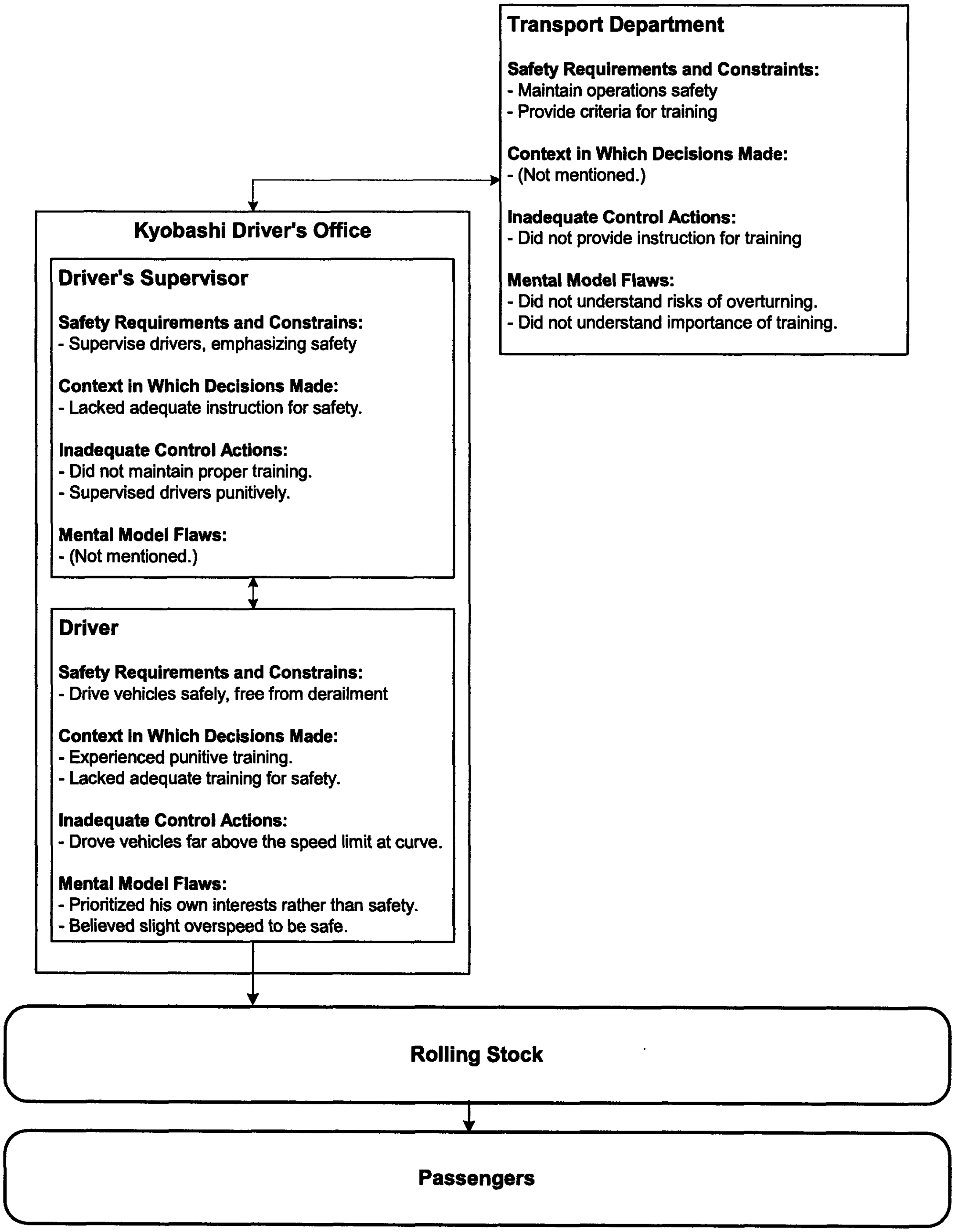


Figure 4.10: Physical components of the railway safety control structure.

One important finding by the accident investigation was that the in-car speed meter indicated a speed that was about 2 to 3 kilometers per hour less than the actual speed when a train ran at a speed of about 120 kilometers per hour. This error was necessarily caused by signal processing of a velocity sensor and is described later in this chapter section; therefore, this cannot be considered as a malfunction in the in-car speed meter.

4.2.4 Operations

In this section, the contribution of the operations to the accident is considered. Figure 4.11 shows the results of a STAMP analysis of the flaws by the operations, namely by the driver, driver's supervisors, and Transport Department.



Transport Department

Safety Requirements and Constraints:
- Maintain operations safety
- Provide criteria for training

Context in Which Decisions Made:
- (Not mentioned.)

Inadequate Control Actions:
- Did not provide instruction for training

Mental Model Flaws:
- Did not understand risks of overturning.
- Did not understand importance of training.

Kyobashi Driver's Office

Driver's Supervisor

Safety Requirements and Constrains:
- Supervise drivers, emphasizing safety

Context in Which Decisions Made:
- Lacked adequate instruction for safety.

Inadequate Control Actions:
- Did not maintain proper training.
- Supervised drivers punitively.

Mental Model Flaws:
- (Not mentioned.)

Driver

Safety Requirements and Constrains:
- Drive vehicles safely, free from derailment

Context in Which Decisions Made:
- Experienced punitive training.
- Lacked adequate training for safety.

Inadequate Control Actions:
- Drove vehicles far above the speed limit at curve.

Mental Model Flaws:
- Prioritized his own interests rather than safety.
- Believed slight overspeed to be safe.

Figure 4.11: Physical and operational components of the railway safety control structure.

The physical cause of the derailment or overturning was simply and solely the overspeed of the train, which was running at a speed of 116 kilometers per hour around the curve where the speed limit was 70 kilometers per hour. The train was so fast that the first cabin overturned outward. The safety requirements and safety constraints on the driver were to drive a train safely, free from the derailment; however, these were violated.

These violations are easily understandable if his mental model flaws are considered. As shown in Figure 4.11, the accident investigation report indicated two mental model flaws. One is that he prioritized his own interests rather than safety. In this company, a driver who has caused incidents such as unjustified delay and overrun at a station is temporarily dropped from a list of drivers and forced to receive training for a certain period of time.

According to the accident investigation report, some drivers perceived this training as punitive. The contents of the training were mental rather than practical. To compose a report of a full account of the accident and an essay repenting his misdeed was a main element. One driver who experienced the training dictated that he felt heavy stress during the training because he was kept in view of other drivers and had to ask a supervisor permission to go to the bathroom. Another driver decided to resign the job of driving after the training that he suffered with for six days. The contents of this training should have been coordinated by the Transport Department, but the fact was that the department did not provide any criteria about the training. Therefore, the director of the driver's office had repeatedly determined the contents and length of the training.

The length of the training was also controversial. It ranged from 1 day to 31 days with an average of 14.7 days in the Osaka branch in 2003 and 2004. It was reported that some drivers considered the length of the training too long.

As for the driver who caused this accident, he had participated in the training three times in the past. The latest training was one when he overran a station in June 2004. It was the 13-day-long training, and his colleague found that he was badly depressed after the training.

It was obvious that he was completely distracted during driving by the prospect that he would have to take the training again. The fact that he asked the conductor to underreport the overrun distance showed that he was really afraid of it. Also, the evidence demonstrated that he was confidentially trying to listen to a radio contact between the conductor and ground control center just before the accident. The purpose was supposed to make his testimony consistent with the conductor. He was totally distracted from driving.

Another mental flaw found in the report was that it was believed that he did not understand a risk of overturning. To put it another way, he probably mistakenly thought that a slight overspeed would not cause any problem.

Table 4.1 is the questionnaire result from 53 drivers in Kyobashi Driver's Office and showed how the drivers acknowledged the limit velocity over which a train would overturn at the curve where the accident happened.

Table 4.1: Questionnaire result about the overturning velocity.

Overturning Velocity	Number of Drivers	Cumulative Percentage
Over 150 km/h	0	0%
From 140 km/h to 150 km/h	9	18%
From 130 km/h to 140 km/h	9	36%
From 120 km/h to 130 km/h	7	50%
From 110 km/h to 120 km/h	5	60%
From 100 km/h to 110 km/h	14	88%
From 90 km/h to 100 km/h	6	100%
Below 90 km/h	0	100%

According to a classic calculating formula that is called Kunieda Formula, the velocity at which the train overturns is 106 kilometers per hour when a train vibration is taken into account. This means that over 60 percent of the drivers were overestimating the overturning velocity at that time. This was truly a threatening situation. For this accident, it was supposed that the driver of this accident did not recognize risks of overturning at all while driving around the curve at a velocity over the speed limit. This is categorized as his mental model flaws.

The drivers' misunderstanding about the overturning velocity is largely attributed to the mental model flaws in the Transport Department. As well as drivers, it was reported that the Transport Department did not understand risks of overturning.

On the day of the accident, the company announced that the overturning velocity is estimated at 133 kilometers per hour, which was not the case. This announcement demonstrated that the company had not accurately calculated the overturning velocity and that it did not recognize risks of overturning at all as a consequence.

In summary, the Transport Department did not provide any criteria of training for drivers. In particular, it never tried to let drivers understand risks of overturning because it itself did not recognize that risk. As a result, the training program became very unpractical and some drivers thought it was punitive. This resulted in the driver's two mental flaws: (1) He prioritized his own interests than safety. (2) He believed a slight overspeed to be safe. At the end, he drove the train above the speed limit, being distracted by his fear of having to undergo training in the future.

4.2.5 Rolling stock development

As mentioned in the previous section, it was reported that there was a gap between the actual speed and the in-car speed meter. When the train was running at a speed of about 120 kilometers per hour, the speed indicated by the meter was smaller than the actual speed by 2 to 3 kilometers per hour. It may be an exaggeration to say that this gap caused the accident, but this is considered as one of many factors that contributed to this accident.

This gap was not an accidental one but an inevitable consequence. The speed meter utilized a velocity sensor that is attached to an axle and that generates 90 pulses per rotation of the axle. The speed was finally calculated using the number of pulses generated during a specified period, a wheel diameter, and an appropriate coefficient. The problem was that the integrated coefficient was based on the condition that the specified period was 250 milliseconds while the actual period was set to 248 milliseconds. As a result, the in-car speed meter necessarily indicated a smaller value than the actual velocity. When a train whose wheel diameter is 794 millimeters runs at a speed of 155 kilometers per hour, the in-car speed meter would indicate 150 kilometers per hour, which means the gap would be as many as 5 kilometers per hour.

This situation did not fulfill a regulation enforced by the Japanese government, although the specification that the Rolling Stock Department provided for a manufacturing company required applying the regulation to the speed meter. An engineer in charge in the manufacturing company testified that he knew the existence of the regulation but did not know that it regulated an in-car speed meter.

Another problem regarding the in-car speed meter was that this design error had been passed through regular inspections although it should not have been passed. A regulation for inspections enacted by the director at the Rolling Stock Department required the inspection of the speed meter. The investigation report did not describe the details, but it was clear that the inspections of the speed meter were inadequate and that the Rolling Stock Department failed to enforce the regulations appropriately.

This analysis of the flaws by the vehicle development components, namely the manufacturing company and Rolling Stock Department, is summarized in Figure 4.12.

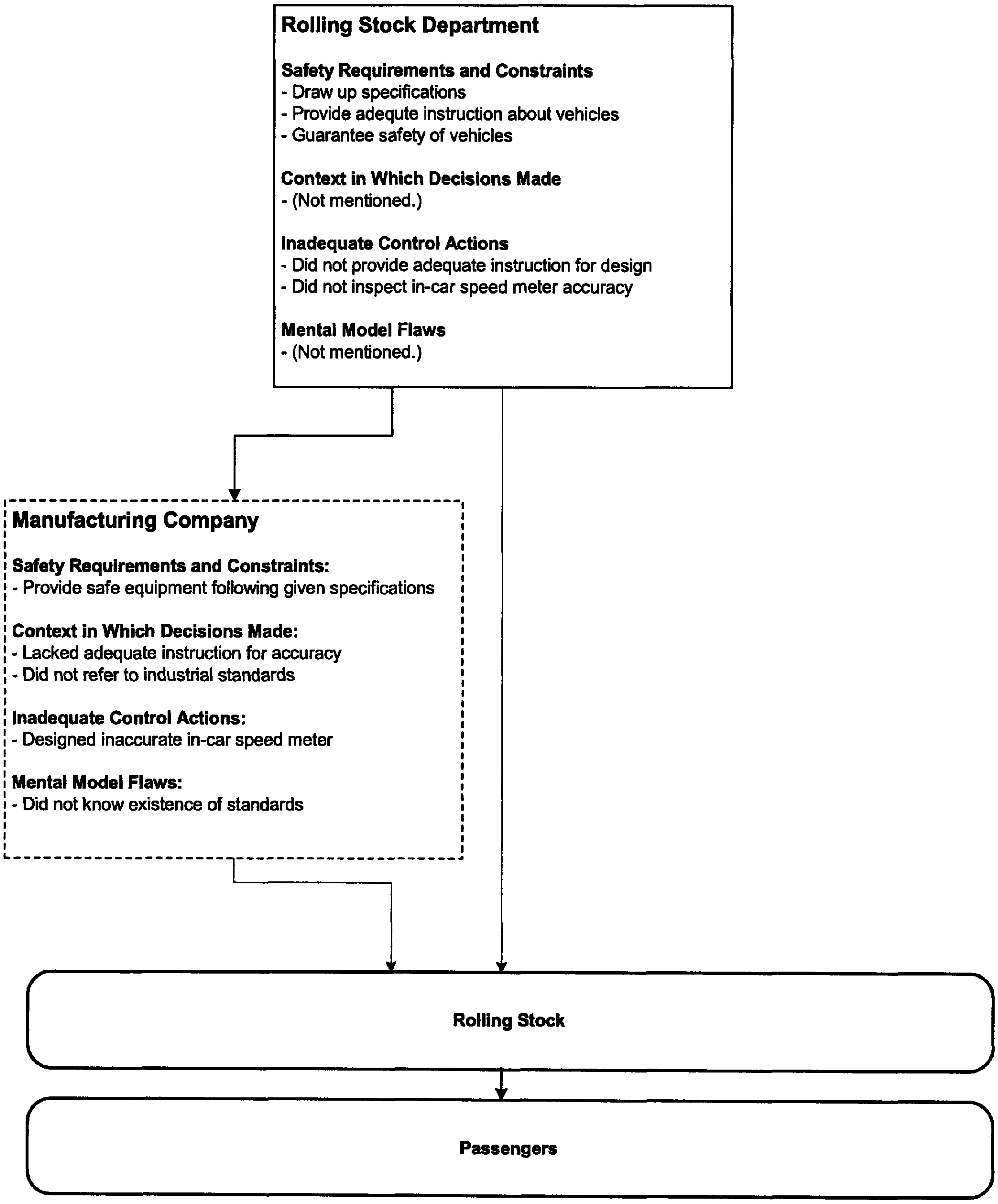

Rolling Stock Department
Safety Requirements and Constraints
- Draw up specifications
- Provide adequte instruction about vehicles
- Guarantee safety of vehicles
Context in Which Decisions Made
- (Not mentioned.)
Inadequate Control Actions
- Did not provide adequate instruction for design
- Did not inspect in-car speed meter accuracy
Mental Model Flaws
- (Not mentioned.)
Manufacturing Company
Safety Requirements and Constraints:
- Provide safe equipment following given specifications
Context in Which Decisions Made:
- Lacked adequate instruction for accuracy
- Did not refer to industrial standards
Inadequate Control Actions:
- Designed inaccurate in-car speed meter
Mental Model Flaws:
- Did not know existence of standards
Rolling Stock
Passengers

Figure 4.12: Physical and rolling stock development components of the railway safety control structure.

4.2.6 Ground equipment development

In this section, the flaws in the ground equipment development are described. The organizations that are involved in the development are the Transport Safety Department, Truck & Structure Department, Electrical Engineering Division in the Osaka Branch, and Osaka Signal Station. Figure 4.13 illustrates a result of a STAMP analysis.

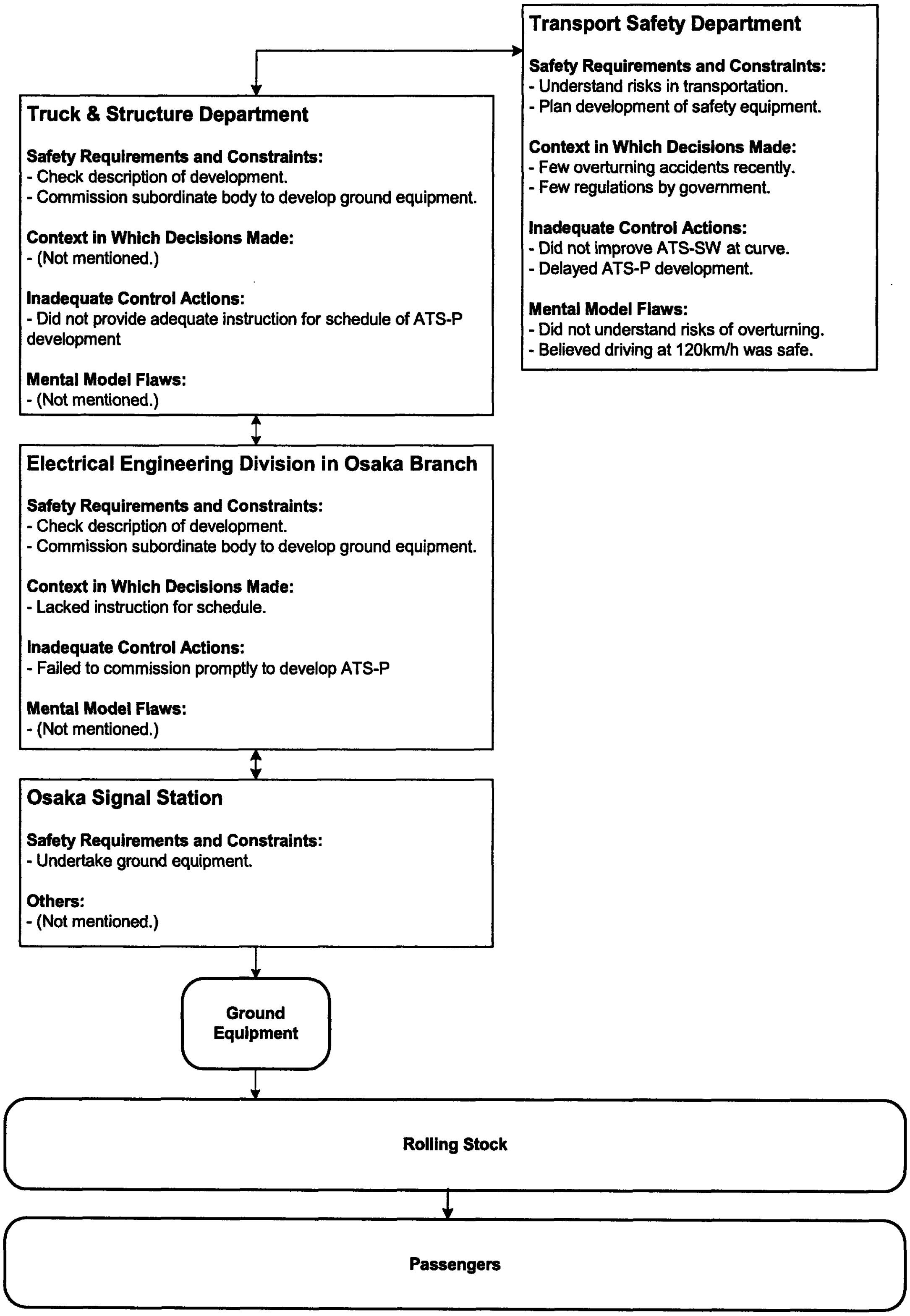
The flaws in the ground equipment development phase can be condensed into those by the Transport Safety Department. The safety requirements and constraints for the department are to understand risks in transportation systems and to draw up a plan to introduce safety equipment. As for the accident, it committed two inadequate control actions. One is that it did not improve ATS-SW at the curve where the accident occurred, and the other is that it delayed an introduction of ATS-P.

It may be beneficial to explain the ATS systems here. As described before, Automatic Train Stop (ATS) system is, in general, safety equipment that has an ability to stop a train automatically in certain situations. It consists of an onboard device and ground equipment, and the combination of the two determines the functions that the ATS system provides. Table 4.2 shows all the functions that the existing ATS can provide. It is important to note that a company can choose which function to provide. For example, a company can introduce the curve-speed-checking function only at a specified curve where the company considers it necessary.

Table 4.2: Functions that ATS system provides.

Function	**Description**
Signal-Checking	Stop a train automatically when it ignores a stop signal.
Point-and-Crossing-Speed-Checking	Stop a train automatically when it passes through a point and crossing at a speed over the limit.
Curve-Speed-Checking	Stop a train automatically when it runs around a curve at a speed over the limit.
Prevent-Missing-Stops	Stop a train automatically when it misses stops.

In the company, there were two types of ATS: ATS-SW and ATS-P. ATS-SW is a longstanding, simple system, and its first model was introduced in Japan in the middle of the 1960s. The ATS-P was first introduced in the late 1980s and is rather an advanced, complicated system compared to the ATS-SW. Although there are small functional differences in the details, both types can provide all the functions in Table 4.2.



Transport Safety Department

Safety Requirements and Constraints:
- Understand risks in transportation.
- Plan development of safety equipment.

Context in Which Decisions Made:
- Few overturning accidents recently.
- Few regulations by government.

Inadequate Control Actions:
- Did not improve ATS-SW at curve.
- Delayed ATS-P development.

Mental Model Flaws:
- Did not understand risks of overturning.
- Believed driving at 120km/h was safe.

Truck & Structure Department

Safety Requirements and Constraints:
- Check description of development.
- Commission subordinate body to develop ground equipment.

Context in Which Decisions Made:
- (Not mentioned.)

Inadequate Control Actions:
- Did not provide adequate instruction for schedule of ATS-P development

Mental Model Flaws:
- (Not mentioned.)

Electrical Engineering Division in Osaka Branch

Safety Requirements and Constraints:
- Check description of development.
- Commission subordinate body to develop ground equipment.

Context in Which Decisions Made:
- Lacked instruction for schedule.

Inadequate Control Actions:
- Failed to commission promptly to develop ATS-P

Mental Model Flaws:
- (Not mentioned.)

Osaka Signal Station

Safety Requirements and Constraints:
- Undertake ground equipment.

Others:
- (Not mentioned.)

Figure 4.13: Physical and ground equipment development components of the railway safety control structure.

The company began introducing the ATS-SW in February 1991 and all lines except for those with ATS-P were equipped with the ATS-SW by September 1993. However, it was March 2002 when the curve-speed-checking function was first added into some ATS-SWs. The criteria for this addition at that time were to provide the curve-speed-checking function for a curve with a radius less than 600 meters where a train possibly ran at a speed of 130 kilometers per hour. (The latter criterion corresponds to a condition that a speed limit before a curve is set to 130 kilometers per hour.) Consequently, by March 2003, the curve-speed-checking function was incorporated into seventeen curves that did not include the curve of the accident where the speed limit before it was 120 kilometers per hour. The person in charge in the company said that driving at a speed of 120 kilometers per hour has been conducted for a long time and that he did not recognize any need to introduce the curve-speed-checking function into a curve where a speed limit before it is 120 kilometers per hour.

On the other hand, the company decided in March 1989 to introduce the ATS-P sequentially into primary lines. In this instance, the ATS-P curve-speed-checking function was incorporated into a curve with a radius less than 450 meters. As a result, some of the primary lines, such as the Osaka Kanjo Line and Tokaido Line, were equipped with ATS-P by the time of the accident. The company also decided to introduce ATS-P into the Fukuchiyama Line where the accident occurred, and Table 4.3 shows the time-line regarding movements of the introduction of the ATS-P into the Fukuchiyama Line.

In short, the introduction was delayed. The ATS-P was supposed to be in operation at the time of the accident, but it was not. With the ATS-P including the curve-speed-checking function, this accident could have been prevented. The manager of the Corporate Planning Headquarters dictated that the first discussion took place in the beginning of April 2003 and it took five months to take it to the board meeting on September 29, 2003. He also stated that this kind of delay was not unusual in the company. The person who was solely in charge in the Electrical Engineering Division in the Osaka branch said that it required five months to check the description of the construction, which delayed the delegation to the head of the Osaka Signal Station until March 2004 while it was supposed to be in October 2003. The interviews conducted by the accident investigation team revealed that most of the people involved did not pay attention to its schedule.

Table 4.3: Time-line regarding the introduction of ATS-P into the Fukuchiyama Line.

August 1990	ATS-P was first introduced into the company's operating line.
March 1991	The speed limit on the Fukuchiyama Line increased from 100 to 120 kilometers per hour.
December 1996	The radius of the curve of the accident was reduced to 304 meters from 600 meters.
Summer 1998	The company's medium- to long-term investment scheme referred to 200 million-yen investments for the introduction of ATS-P into Fukuchiyama Line in fiscal 2003.
Summer 1999 - Summer 2003	The company's medium- to long-term investment scheme referred to 200 million-yen investments in fiscal 2003 and 600 million-yen in fiscal 2004. (This implied that ATS-P was supposed to be introduced by the end of fiscal 2004, namely March 2005.)
March 2003	The curve-speed-checking function was added into seventeen ATS-SWs.
September 2003	The management committee gave an approval for the investment.
October 2003	The head of the Electrical Engineering Division in the Osaka branch received an official notice about the budget.
March 2004	The head of the Osaka Signal Station was delegated.
Summer 2004	The company's medium- to long-term investment scheme referred to 10 million-yen investments (actual achievements) in fiscal 2003, 770 million-yen in fiscal 2004, and 30 million-yen in fiscal 2005. ATS-P was supposed to be launched in June 2005.
April 25, 2005	The Fukuchiyama Line Derailment Accident

It is important to note that the speed limit on the Fukuchiyama Line of the accident increased from 100 kilometers per hour to 120 kilometers per hour in March 1991. Additionally, the radius of the curve of the accident was reduced from 600 meters to 304 meters in December 1996. These alterations could have triggered an introduction of the curve-speed-checking function of ATS-SW or an introduction of ATS-P in the early stages, but it did not. The Transport Safety Department did not fully understand the risks of overturning and believed driving at a speed of 120 kilometers per hour was safe.

4.2.7 Timetable development

The accident investigation report also pointed out a problem about a timetable on the Fukuchiyama Line. The Transport Division in the Osaka Branch is in charge of drawing up a timetable for the line, and Figure 4.14 shows its two inadequate control actions: (1) It drew up an inappropriate timetable in terms of time margins. (2) It utilized incorrect data when calculating the basic time. (The basic time refers to the minimum required time by calculation.)

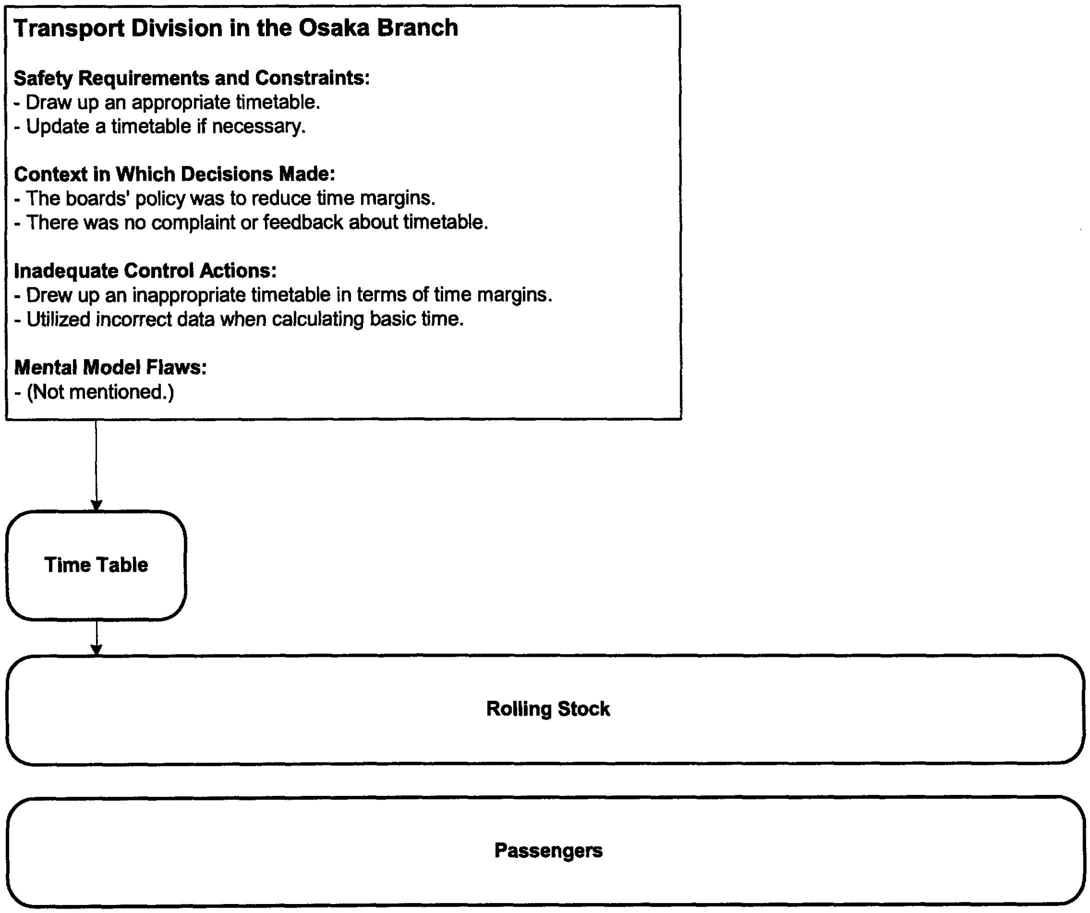

Transport Division in the Osaka Branch
Safety Requirements and Constraints:
- Draw up an appropriate timetable.
- Update a timetable if necessary.
Context in Which Decisions Made:
- The boards' policy was to reduce time margins.
- There was no complaint or feedback about timetable.
Inadequate Control Actions:
- Drew up an inappropriate timetable in terms of time margins.
- Utilized incorrect data when calculating basic time.
Mental Model Flaws:
- (Not mentioned.)
Time Table
Rolling Stock
Passengers

Figure 4.14: Physical and timetable development components of the railway safety control structure.

Table 4.4 shows the transitions of the timetable on the Fukuchiyama Line. Time margins were reduced by 20 seconds in both 2002 and 2003 and by 10 seconds in 2004. Reducing time margins was the boards' policy at that time. With smaller time margins, time required was reduced. Also, a higher frequency of trains, which was one of the most significant factors in train operations, was achieved so that more and more passengers preferred its trains. As a result, driving time was almost the same as the basic time, which is the minimum required time by calculation. Besides, the stoppage time at stations were also reduced sometimes.

The problem was that its reduction was not reasonable at all. For example, the stoppage time of 5418M at Itami Station was reduced from 20 seconds to 15 seconds on December 2003. A person in charge dictated that it was not possible to shorten driving time since it was almost the same as the basic time and that all he could do was to reduce the stoppage time. He actually measured the stoppage time at Itami Station and found that it took about 18 seconds. Then he finally set the stoppage time to 15 seconds without adequate consideration.

Table 4.4: Transitions of the timetable on the Fukuchiyama Line.

Station	March 1997	March 2002	March 2003	December 2003	October 2004	Basic Time
Takarazuka						
	5’50”	5’50”	5’40”	3’15”	3’15”	3’11”
Nakayamadera						
				3’10”	3’10”	3’08”
Kawanishi-Ikeda						
	2’30”	2’30”	2’20”	2’20”	2’20”	2’21”
Kita-Itami						
	1’30”	1’30”	1’30”	1’30”	1’30”	1’31”
Itami						
	2’40”	2’20”	2’20”	2’20”	2’20”	2’12”
Tsukaguchi						
	3’10” (2’50”)	3’10” (2’40”)	3’10” (2’40”)	3’10” (2’40”)	3’00” (2’40”)	3’11” 3’11”
Amagasaki Platform 6 (Platform 7)						
Total	15’40”	15’20”	15’00”	15’45”	15’35”	15’07”

# “Basic Time” refers to the minimum required time by calculation.

Another problem was that the way to calculate the basic time was incorrect because of incorrect data. For example, the length of the train was set to 10 meters while the actual length was 140 meters, and four ascending slopes on the line were regarded as descending slopes. It is reported that the total basic time should have been 15’34” instead of 15’07” in Table 4.4.

As a result, many trains were constantly behind schedule. For example, 5418M trains tended to arrive at Amagasaki Station 100 seconds late on average at that time. On the other hand, the company was serious about a delay caused by drivers. The supervisors required drivers to report a delay that was more than 30 seconds and brought a charge against drivers if there was an unjustified delay more than 1 minute. It is fair to say that the company's policy lacked consistency.

Tables 4.5 and 4.6 are the questionnaire results from 51 drivers in Kyobashi Driver's Office. Table 4.5 shows under what conditions the drivers tend to feel pressure, and Table 4.6 shows what kind of delays in terms of their length causes the drivers to feel considerable pressure. According to Table 4.6, more than 60 percent of the drivers felt the greatest pressure from one to three-minute delay, within which the average delay fell. Consequently, these tables demonstrate that the drivers in the office tended to feel great pressure under the condition where there were smaller time margins.

In conclusion, the tight train schedule made drivers feel pressure, and this is considered as one of the factors of this accident.

Table 4.5: Questionnaire results about the reasons of delay: This table shows under what conditions the drivers tend to feel pressure.

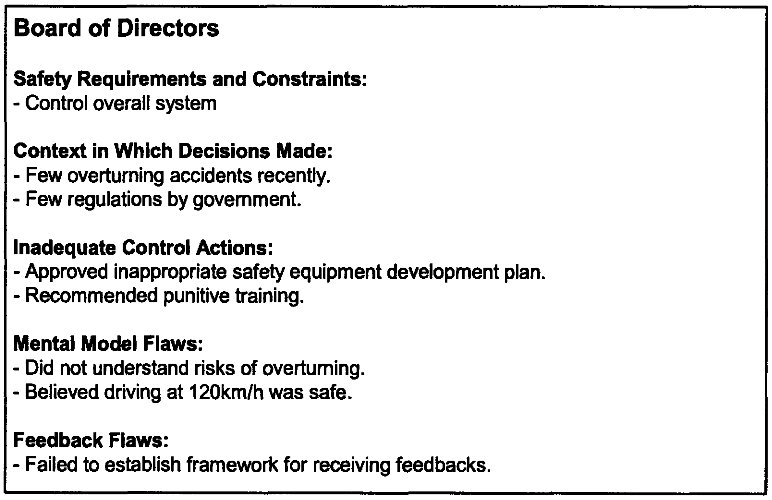
Reasons of Delay	Number of Drivers
(1) Due to smaller time margins, the train becomes behind schedule even when they operate in a designated way.	28 (55%)
(2) Due to a precedent train that is behind schedule, the train also becomes behind schedule when they operate in a designated way.	11 (22%)
(3) Due to smaller time margins, the train becomes behind schedule.	12 (24%)

Table 4.6: Questionnaire results about the length of delay: This table shows what kind of delays in terms of their length causes the drivers to feel the greatest pressure.

Length of Delay	Number of Drivers
(1) Less than 1 minute	12 (24%)
(2) 1 to 3 minutes	31 (61%)
(3) 3 to 10 minutes	4 (8%)
(4) More than 10 minutes	5 (10%)

4.2.8 Board of Directors

The safety requirements and constraints of the Board of Directors were to control the overall system for safety. It might have been possible to reject the inappropriate safety equipment development plan proposed by the Transport Safety Department, but they did not. The investigation report indicated that the Board of Directors suffered from the same mental flaws as the Transport Safety Department. They did not understand the risks of overturning and believed driving at a speed of 120 kilometers per hour was safe. It was estimated that these mental flaws were related to the fact that there had been few overturning accidents recently and few regulations by the government. Figure 4.15 shows the result of a STAMP analysis of the Board of Directors component.



Board of Directors

Safety Requirements and Constraints:
- Control overall system

Context in Which Decisions Made:
- Few overturning accidents recently.
- Few regulations by government.

Inadequate Control Actions:
- Approved inappropriate safety equipment development plan.
- Recommended punitive training.

Mental Model Flaws:
- Did not understand risks of overturning.
- Believed driving at 120km/h was safe.

Feedback Flaws:
- Failed to establish framework for receiving feedbacks.

Figure 4.15: Board of Directors component of the railway safety control structure.

One of the most important things concerning the Board of Directors was that they failed to establish an efficient framework for receiving feedback from operations. At the same time, they recommended punitive trainings for operators who committed a mistake or even a small incident.

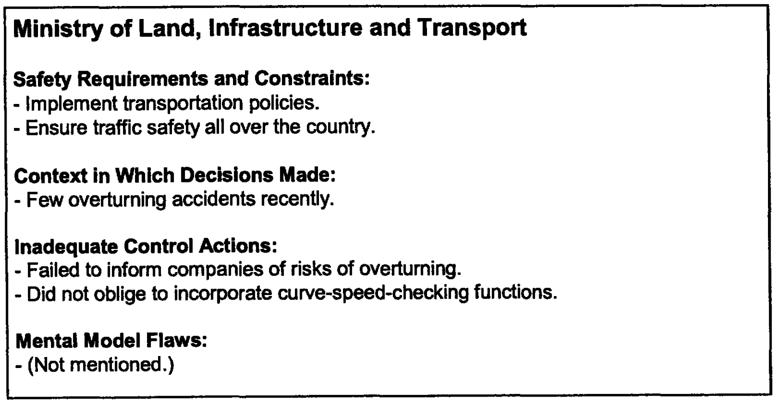
At a meeting of the directors in October 2003, one commission member proposed that the company should not bring a charge against an operator who made a report of his small incident. However, its proposal was rejected as being premature. This interaction showed well how the company was not so eager to receive feedback from operators.

There was another example that demonstrates inadequate feedback in the company. As described earlier, it was revealed after the accident that the configuration of ATS in JR Tozai Line including Kashima Station was set to a wrong number. As a result, the maximum regular brake was very often activated by ATS, namely every fifty trains on average. This was an unusual situation, and it was anticipated that the company could have easily noticed the wrong configuration by the appalling number of ATS activations. However, it was after the accident that they found the wrong configuration.

The accident investigation team came across a driver who previously experienced overspeed at the curve of the accident. He had applied an emergency brake before the curve, which distracted him. Therefore, he failed to apply a brake, so that the train was moving at a speed of 80 to 85 kilometers per hour at the point where the speed limit was reduced to 70 kilometers per hour. He recognized risks of overturning at that curve, but did not report the incident to supervisors because he was afraid that supervisors would impose punitive trainings on him.

4.2.9 Ministry of Land, Infrastructure and Transport

To ensure traffic safety all over the country by policies is the safety requirement of the Ministry of Land, Infrastructure and Transport or MLIT. In the report, two inadequate control actions are described: (1) It failed to inform companies of risks of overturning. (2) It did not oblige companies to incorporate the curve-speed-checking functions into the ATS.



Ministry of Land, Infrastructure and Transport

Safety Requirements and Constraints:
- Implement transportation policies.
- Ensure traffic safety all over the country.

Context in Which Decisions Made:
- Few overturning accidents recently.

Inadequate Control Actions:
- Failed to inform companies of risks of overturning.
- Did not oblige to incorporate curve-speed-checking functions.

Mental Model Flaws:
- (Not mentioned.)

Figure 4.16: Ministry of Land, Infrastructure and Transport component of the railway safety control structure.

Overturning accidents are very rare events. For 18 years from April 1989 to March 2005, the number of railway accidents accounts for 19,576 cases while 6,721 people were killed and 10,742 people injured. Among them, the overturning accidents happened merely twice in 1990 and 1996. Moreover, a freight company, which is relatively smaller than major railway companies, caused these accidents, and no one was injured. It is obvious that this trend made the MLIT not pay enough attention to overturning accidents although they have a potential to suffer a large number of casualties. The MLIT insisted that it informed railway companies of overviews of the overturning accidents when they happened, but it was not instructive enough to make railway companies recognize risks of overturning.

As for the curve-speed-checking function, regulations at that time did not necessarily require it. This also stems from the fact that there had been few overturning accidents recently. The MLIT revised the regulations in March 2006 after the accident, and the curve-speed-checking functions are now mandatory in Japan.

4.2.10 Modeling the dynamics of the Fukuchiyama Line derailment

Figure 4.17 shows a System Dynamics model of the Fukuchiyama Line Derailment accident. The model does not provide any new information about the accident. However, it demonstrates a summary of relationships between many factors. It considers the system to be dynamic, not static, and shows how each component of the system was affected by the others and how the system has changed over time.

One of the most important variables in the model is Risk Awareness by Company. In this model it is assumed that the level of Risk Awareness by Company was affected by five factors: Number of Accidents, Damage by Accidents, Effectiveness of Government Announcements, Operation Frequency, and High-Speed Operation. These relationships are shown in Figure 4.18.

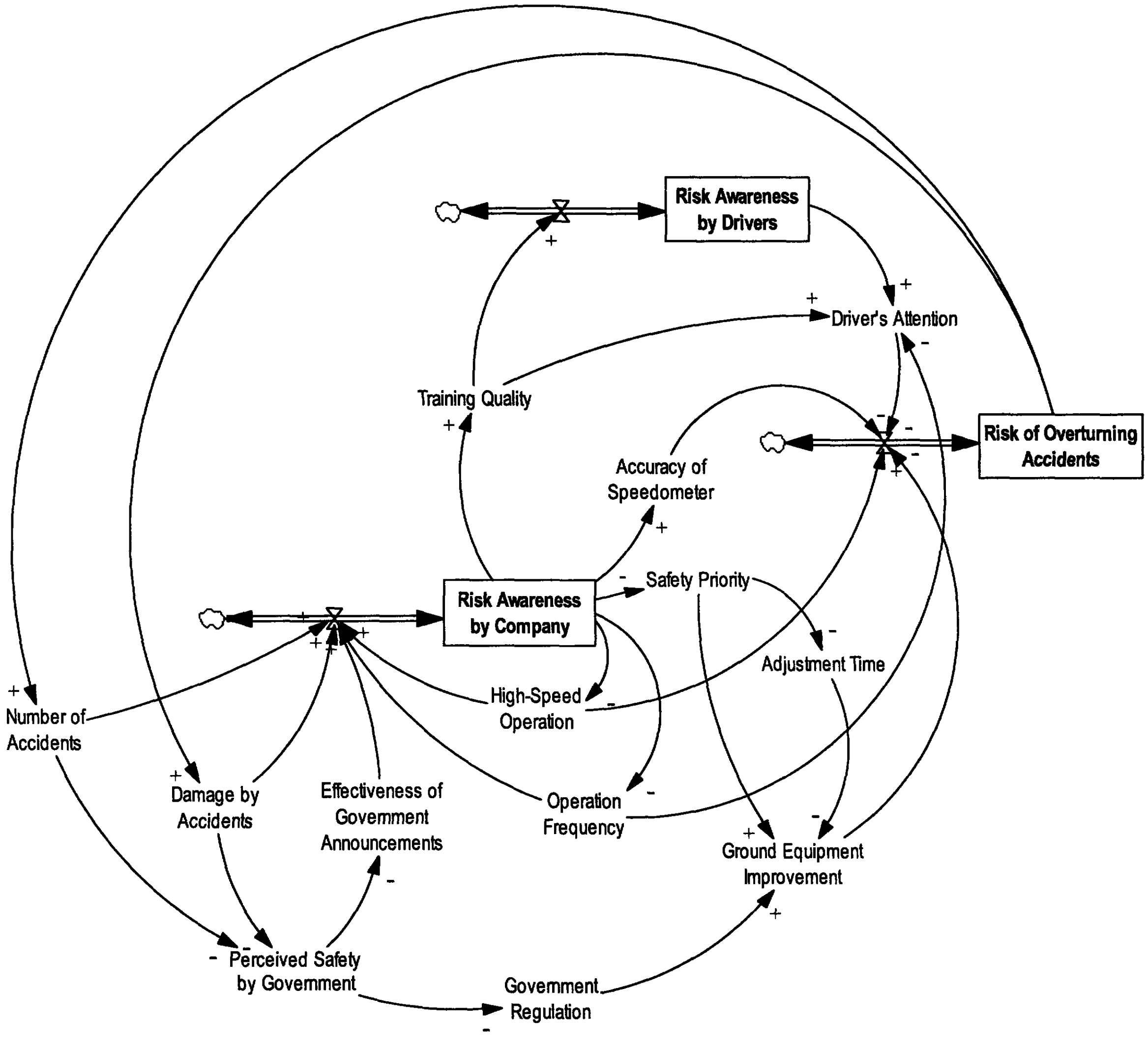


Figure 4.17: Systems Dynamics model for the Fukuchiyama Line derailment.

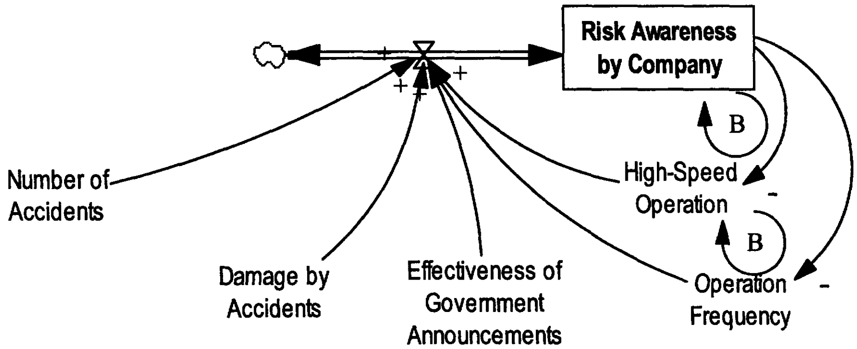


Figure 4.18: Variables in the model that affected the level of Risk Awareness by Company.

As described previously, the number of overturning accidents and amount of damage from the accidents had been negligible recently. This trend made Risk Awareness by Company decrease. Besides the company, the government also had too much confidence in safety measures introduced against overturning accidents, leading to a decrease in Effectiveness of Government Announcements. Decreasing Risk Awareness by Company increased both High-Speed Operation and high operation Frequency. The speed limit on the Fukuchiyama Line increased from 100 to 120 kilometers per hour in 1991, and time margins had been continuously reduced until a point where driving time was almost the same as the basic time.

It is important to note that two negative loops, including High-Speed Operation and Operation Frequency, would theoretically act to balance Risk Awareness by Company: More High-Speed Operation and higher Frequency should have led to an increase in Risk Awareness by Company. However, this was not the case, as the Board of Directors believed driving at a speed of 120 kilometers per hour was safe. The two negative loops were not dominant in the model.

Less Risk Awareness by Company caused a decrease in Training Quality for drivers, Accuracy of Speedometer, and Ground Equipment Improvement as well as an increase in Adjustment Time. (Adjustment Time in the model means speed of the introduction of the ground equipment. More Adjustment Time means more time taken to introduce the ground equipment.) The relevant portion of the model is shown in Figure 4.19.

Driver's Attention was affected by three variables, namely Risk Awareness by Drivers, Training Quality, and Frequency, as shown in Figure 4.20. First, it was assumed that the driver did not understand the risk of overturning, according to the questionnaire result. This was mainly due to the contents of the training, which was criticized as being very impractical. Next, the training program was perceived as punitive, and this fact was considered to distract the driver from paying enough attention to driving because of his fear of having to undergo training in the future. This direct relationship between Training Quality and Driver's Attention was a unique characteristic in this accident, and one of the reasons the accident drew unprecedented public attention (Yamaguchi, 2007). Finally, high frequency of trains with smaller time margins forced drivers to feel great pressure as discussed in the previous section. All three factors caused a decrease in Driver's Attention while driving.

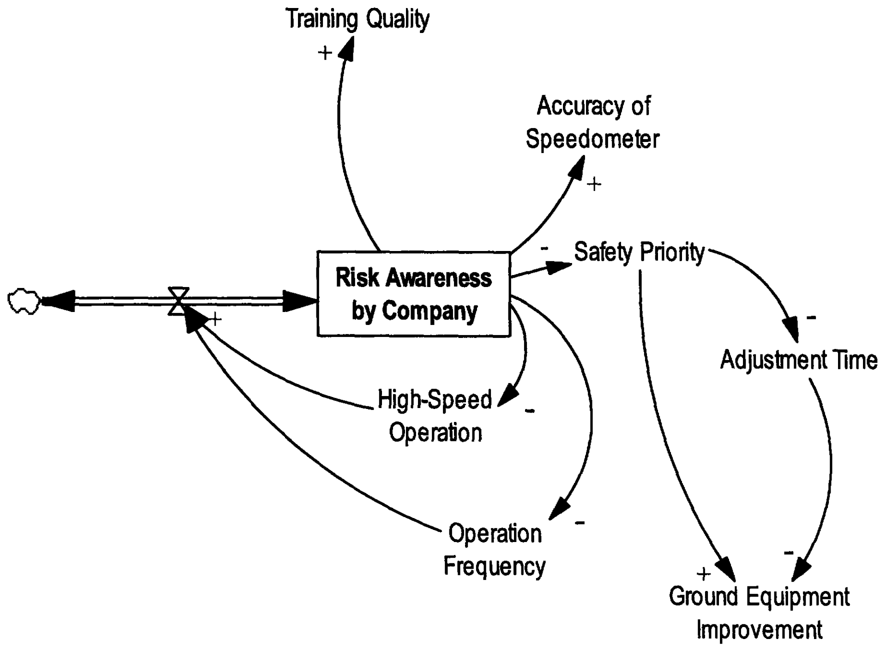


Figure 4.19: Variables in the model that were affected by Risk Awareness by Company.

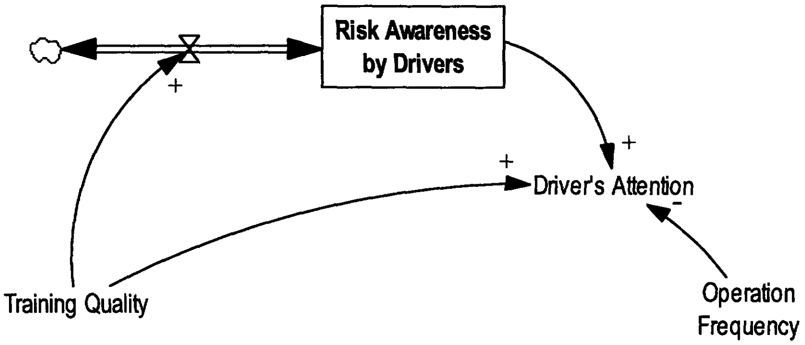


Figure 4.20: Variables in the model that affected Driver's Attention.

A decrease in Accuracy of Speedometer, Driver's Attention, and Ground Equipment Improvement in addition to an increase in High-Speed Operation resulted in an increase in Risk of Overturning Accidents, which led, in the end, to the tragic accident (Figure 4.21).

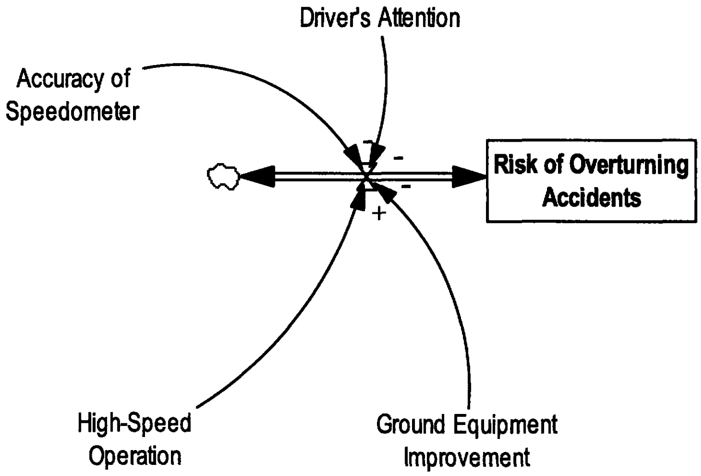


Figure 4.21: Variables in the model that affected the level of Risk of Overturning Accidents.

4.3 Lessons learned from the Fukuchiyama Line derailment

By analyzing the Fukuchiyama Line derailment accident using Systems Theory Accident Modeling and Processes (STAMP) and System Dynamics models, valuable lessons are learned. Some of them are:

(1) This is not a component failure, but a system accident, with which the reliability engineering approach cannot deal;

(2) This type of accident, a derailment accident, is extremely rare; however, it still has great potential to cause enormous damage;

(3) Risk/hazard analysis is the key to assuring safety in today's complex systems;

(4) The accident deeply involves human factors, which play a major role in current railway systems;

(5) It is almost impossible to figure out the probability of this type of accident;

(6) The railway systems are prone to asynchronous evolutions, which could be one of the factors that cause an accident.

In the remaining section, these lessons learned will be explained in detail.

(1) This is not a component failure, but a system accident, with which the reliability engineering approach cannot deal.

The concept of a system accident is originally defined by Perrow (1999) as those that involve the unanticipated interaction of multiple failures. On the other hand, it is helpful to introduce another definition of system accidents here. Noting that accidents occur even in systems where there have been no component failures, Leveson (2002) defines system accidents and component failure accidents as follows: (Hereafter, Leveson's definition will be applied in this thesis.)

- **System accident**: an accident that arises from the interactions among components (electromechanical, digital, and human) rather than from the failure of individual components;
- **Component failure accident**: an accident that arises from component failures, including the possibility of multiple and cascading failures.

This accident, the Fukuchiyama Line derailment accident, is certainly a system accident based on Leveson's definition. The driver committed the violation; however, other than this, there was no malfunction in the vehicles and in the ground equipment, and every component was working as designed.

Leveson (2002), through various kinds of accident analyses in fields such as the airline and space industry, claims that it is system accidents that closer attention should be paid to, in order to minimize risk in today's complex systems, because the reliability of every component is considerably improved these days. This accident demonstrates that her argument is also applicable in today's railway systems, including the high-speed maglev systems. (It is a pity that no statistical data that supports this argument is available, since, as Braband (2004) states, the causes of railway accidents are not investigated systematically.)

The concept of the system accident is certainly included in the international railway standards. Figure 4.22 is an excerpt from IEC 62278: *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*, and it shows some of the factors that influence railway RAMS. As shown in the figure, internal disturbances comprise systematic failures and random failures. Furthermore, systematic failures, which are defined as failures due to errors in any safety life cycle activity, within any phase, which cause it to fail under some particular combination of inputs or under some particular environmental condition, are comprised of errors in requirements, design and realization inadequacies, software errors, and others. Although there is no failure in the system accident and the term failures, therefore, is not appropriate to include the system accident, the concept of the system accident definitely corresponds to systematic failures. Also, regarding safety integrity, IEC 62278 states the following, clearly distinguishing between random failures and systematic failures:

> Safety integrity can be viewed as a combination of quantifiable elements (generally associated with hardware, i.e. random failures) and non-quantifiable elements (generally associated with systematic failures in software, specification, documents, processes, etc.).

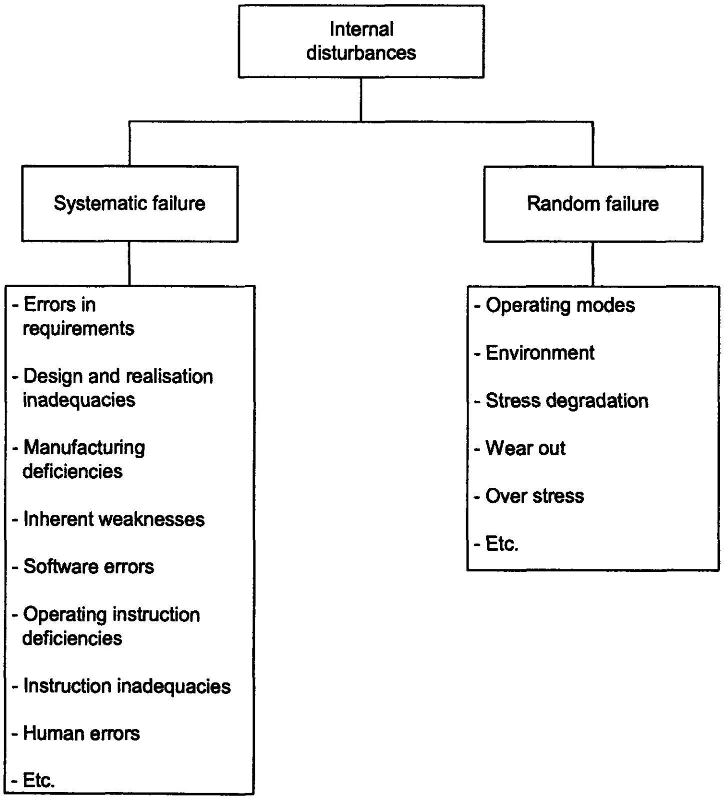


Figure 4.22: Factors influencing railway RAMS (Source: IEC 62278). Internal disturbances comprise systematic failures and random failures.

The inconsistency is, however, that the underlying concept of IEC 62278 is the reliability engineering approach, which is failure oriented, as described in Chapter 3. Since there was no failure in this accident, it is apparent that the reliability engineering approach could have not contributed to preventing the Fukuchiyama Line derailment accident. It is fair to argue that the approach recommended in IEC 62278 contributes little to preventing a system accident, to which closer attention should be paid, and that a different approach is required.

In conclusion, the Fukuchiyama Line derailment accident demonstrates that system accidents definitely occur in the railway industry as well as other industries, and suggests that special care should be taken to minimize the risk of system accidents, which should be clearly distinguished from the risk of component failures. It is important to note again that the reliability engineering approach, which IEC 62278 advocates, cannot deal with system accidents.

(2) This type of accident, a derailment accident, is extremely rare; however, it still has great potential to cause enormous damage.

The Fukuchiyama Line derailment accident was the third overturning accident in eighteen years in Japan, which means this is an extremely rare event. In addition, this was the first overturning accident that caused fatalities during that period. (In the overturning accidents in 1990 and 1996, no one was injured.) Although overturning has been one of the most critical hazards in railway operation, this rarity led the Ministry of Land, Infrastructure, and Transport (MLIT) to pay inadequate attention to overturning accidents, and they failed to inform railway companies of the risks of overturning, as mentioned previously.

However, the consequences of this accident were extremely serious: No less than 106 passengers and the driver were killed in this accident. This was the most serious accident in Japan in forty years.

It is important to note that the topic of "acceptable risk" is outside of the scope of this thesis. A considerable controversy currently exists about acceptable risk. The following is a list of standpoints that could be used as a basis for assessing acceptability of risk (Mizoguchi & Sato, 2006).

- A risk is acceptable when it falls below an average death rate from all factors such as old age, illness, and accidents.
- A risk is acceptable when it falls below a rate of fatal occupational injuries.
- A risk is acceptable when it falls below some level that is already tolerated.

However, as Leveson (1995) claims, the discussion about the acceptable risk is not a truly scientific question because it largely depends on cultural views. (For example, according to Mizoguchi and Sato (2006), Japanese people have totally different views from others as to safety and never even accept the concept of the acceptable risk: the Japanese seek zero risk.) Consequently, the argument about the acceptable risk is not within the scope of this thesis. To put it another way, some people may argue that the Fukuchiyama Line derailment accident is acceptable because the probability is extremely low; however, this thesis does not address that point.

To sum up, the important lesson learned from this accident is that in the railway industry there exists a potential accident that is very rare but causes enormous damage.

(3) Risk/hazard analysis, which was inappropriate to prevent this derailment, is the key to assuring safety in today's complex systems.

It is apparent that the entire company did not recognize the risk of overturning because of a poor risk/hazard analysis.

First, the company had not accurately calculated the overturning velocity. As described before, on the day of the accident the company announced that the velocity at which the train might overturn was estimated at 133 kilometers per hour, while it is 106 kilometers per hour according to the classic calculating formula. Later, the accident investigation revealed that the company did not take vehicle vibrations into account, which made the calculated overturning velocity unrealistic. This announcement demonstrated that as a consequence of the error, the company did not correctly assess the risk of overturning at all as a consequence.

Next, the Transport Safety Department and the Board of Directors believed that driving at a speed of 120 kilometers per hour was safe, simply because driving at a speed of 120 kilometers per hour had been done for a long time, according to the interviews after the accident. This judgment was not valid, and the tragic accident actually happened while driving at a speed of 120 kilometers per hour. Their flawed mental models prevented them from identifying the risk of driving at a speed of 120 kilometers per hour. If an appropriate risk/hazard analysis had been conducted, they might have rectified their flawed mental models.

It is worthy of note, again, that the top management did not recognize the risk at all. In some cases, such as Northeast Utilities' three nuclear plants in Connecticut, top management (and the board) knowingly takes risks in violation of regulatory laws, and causes accidents (Perrow, 2007). However, this is not the case in this Fukuchiyama Line derailment accident; the management never recognized the risk.

Finally, according to the questionnaire results in Table 4.1, over 60 percent of the drivers in Kyobashi Driver's Office were overestimating the overturning velocity at that time. To put it another way, most of the drivers mistakenly thought that a slight overspeed would not cause any problem, which was not the case. This was another flawed mental model. In the space shuttle Challenger accident, engineers on the line recognized a risk of the launch in such cold weather. However, the management did not acknowledge it due to lack of appropriate communication (Tufte, 1997). This causation in the Challenger accident does not apply to the Fukuchiyama Line derailment accident: the drivers did not recognize the risk themselves, either.

It is important to recognize the difference between hazard analyses and reliability analyses (Miller, 1988). In reliability analyses, engineers identify the failure of the component that is critical for the system, and try to reduce the failure rate of that component. In hazard analyses, engineers are required to identify the situation that might lead to an accident even if everything is functioning as designed without a failure. It is hazard analyses, rather than reliability analyses, that could have prevented the Fukuchiyama Line derailment accident.

Consequently, an essential lesson learned is the importance of appropriate risk/hazard analyses that make an entire company recognize a risk. If the company had recognized the risk of overturning, the accident could have been prevented.

Figure 4.23 is the modified System Dynamics model for this accident, and it demonstrates how an appropriate risk/hazard analysis can prevent accidents. Primarily, the risk/hazard analysis contributes to an increase in Risk Awareness by Company. As described before, a decrease in Risk Awareness by Company was one of the factors that caused this accident. In that sense, the risk/hazard analysis is expected to compensate for its decline. At the same time, the risk/hazard analysis can improve a quality of training for drivers.

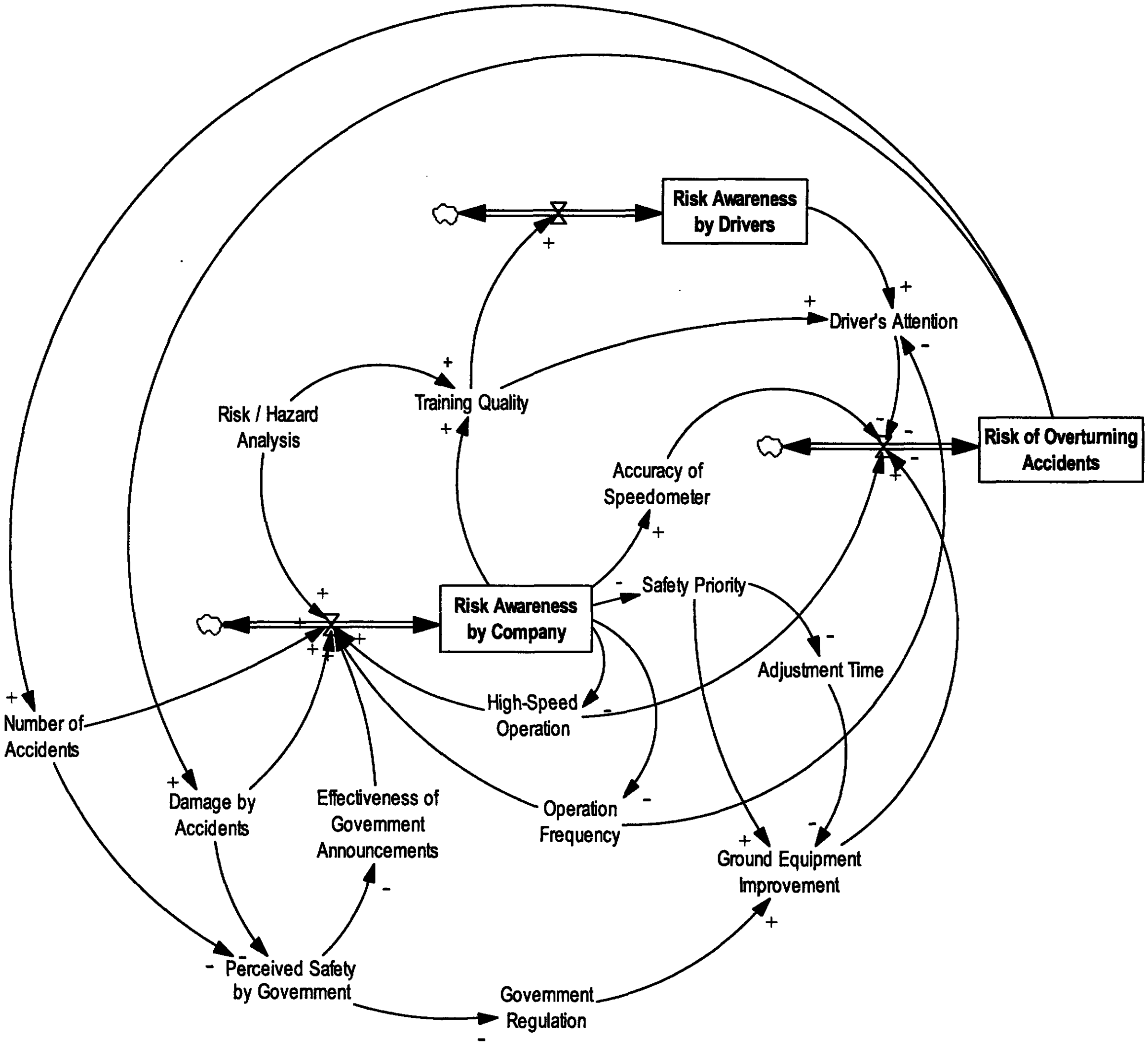


Figure 4.23: Modified System Dynamics model for the Fukuchiyama Line derailment. A variable of Risk/Hazard Analysis is added so that this model demonstrates how an appropriate risk/hazard analysis can work.

(4) The accident deeply involves human factors, which play a major role in current railway systems.

It is helpful first to define human factors. Sanders and McCormick (1993) propose the definition of human factors as below.

> Human factors discovers and applies information about human behavior, abilities, limitations, and other characteristics to the design of tools, machines, systems, tasks, jobs, and environments for productive, safe, comfortable, and effective human use.

Also, they declare two objectives of human factors:

(1) To enhance the effectiveness and efficiency with which work and other activities are carried out;

(2) To enhance certain desirable human values, including improved safety, reduced fatigue and stress, increased comfort, greater user acceptance, increased job satisfaction, and improved quality of life.

Based on the definition and objectives of human factors above, it is fair to say that the Fukuchiyama Line derailment accident deeply involved human factors. Three points, which will be described below, support this argument.

First, the direct cause of the derailment was the overspeed at the curve, which occurred because the driver failed to apply the brake ahead of the curve. According to the investigation report, a delay of merely sixteen seconds in applying the brake caused the derailment. To put it another way, the system necessarily caused an accident with a sixteen-second hiatus, although it was equipped with the safety devices such as ATS. It is hard to argue that information about human abilities and limitations was understood well and applied to the design from the viewpoint of human factors, since a sixteen-second hiatus is not so improbable when human limitations are considered.

Another point is that the smaller time margins in the timetable forced drivers to feel great pressure, as shown in Table 4.5 and 4.6. The Transport Division in the Osaka branch reduced the time margins, as shown in Table 4.4, without careful consideration of drivers' stress. The accident investigation found no evidence that showed the existence of any trade-off analysis between frequency of operation and human factors. (For details, see Section 4.2.7.)

Finally, the driver of the accident was certainly distracted before the accident by the prospect that he would have to take the training, which he was really afraid of. As described in Section 4.2.4, some drivers thought the training program was punitive. Some people may say that punitive training is effective because it motivates trainees. However, it had an adverse effect on this driver, at least.

These three arguments demonstrate that the railway system lacked proper consideration of human factors and, at the same time, indicate the significance of human factors in today's railway systems. It is widely recognized that human factors play a major role in the current aviation industry (Edwards, 1998; Wiegmann & Shappell, 2003). This is also true in the railway industry. An important lesson to be learned from this accident is that close attention should be paid to human factors.

(5) It is almost impossible to figure out the probability of this kind of accident, because this is not a component failure and because human factors are deeply involved in this accident.

Another lesson is the difficulty of figuring out the probability of this kind of accident. Several factors are involved here.

First, this was not a component failure, but a system accident. Since system accidents arise from inadequate interactions rather than hardware failures, it is practically impossible to predict the probability of a system accident. IEC 62278, the railway international standard, regards systematic failures as non-quantifiable elements, as mentioned before.

Furthermore, human factors crucially involved in this accident, as described in (4). Various attempts have been carried out to assign a probability to human errors (Sanders & McCornick, 1993). However, there exists a limitation. In particular, as Leveson (1995) claims, human behavior under great pressure is hard to understand, although it is human behavior under great pressure that tend to cause errors. In fact, the driver of this accident was completely distracted during driving by the prospect that he would have to take the training again and was confidentially trying to listen to a radio contact between the conductor and ground control center just before the accident. It is obvious that no one can calculate the probability that he would fail to apply the brake under these circumstances.

As a result, determination of the probability of this kind of accident is impossible.

(6) The railway systems are prone to asynchronous evolution, which could be one of the factors that cause an accident.

As described at the beginning of this chapter, Leplat (1987) considers asynchronous evolution where a process in a subsystem of a system changes without appropriate change of other system components to be one of the categories that often cause an accident, and Leveson (2002) pays close attention to its concept.

It would not be an exaggeration to say that this accident resulted from asynchronous evolution. The speed limit on the Fukuchiyama Line increased from 100 kilometers per hour to 120 kilometers per hour in March 1991. Additionally, the radius of the curve where the accident happened was reduced from 600 meters to 304 meters in December 1996. These alterations, obviously, degraded the level of safety to some degree. However, the ground equipment on the line was not improved to compensate for its deterioration: Neither ATS-P nor the curve-speed-checking function of ATS-SW was incorporated. This is precisely an instance of asynchronous evolution.

There are two reasons that the railway systems are prone to asynchronous evolution. One is that railway operations are achieved by various kinds of functions and by various kinds of organizational components. The STAMP analysis above demonstrated that the accident primarily involved six functions: operations, rolling stock development, ground equipment development, timetable development, corporate management, and regulation management. Also, the safety control structure shown in Figure 4.9 revealed that the organizational components in the company were intricately intertwined with each other.

The other reason is that the railway systems are semi-permanently in operation once an operation begins. In the meantime, changes are frequently introduced into subsystems, due to the modernization or degradation of some equipment. These changes should be carefully designed. However, there is always a possibility of neglect of their consequences for other parts of the systems. More opportunities for changes over a long span of time result in a higher likelihood of neglect and error. As a result, the railway systems are vulnerable to asynchronous evolution.

To sum up, vulnerability to asynchronous evolution in the railway systems should be recognized.

Chapter 5

Hazard Analysis Requirements for High-Speed Maglev Systems

The analysis of the Fukuchiyama Line derailment accident indicates the importance of appropriate risk/hazard analyses that make an entire company recognize a risk. Subsequently, requirements of risk/hazard analysis are derived in this chapter, based on the characteristic features of high-speed maglev systems and lessons learned from the Fukuchiyama Line derailment accident. Finally, the fundamentals of System Safety are introduced to compare the requirements obtained through this thesis with System Safety approaches.

5.1 Appropriate hazard analysis for maglev systems

5.1.1 Hazard-related definitions

As yet, no specific definitions of hazard and risk are provided in this thesis. Instead, the term of "risk/hazard" has been preferred. It is helpful to introduce the definitions of these terms at this point. Two standards introduced in Chapter 3 provide the definitions as follows. Although the expressions are slightly different from each other, the concept is almost the same. Hereafter, the definitions in IEC 62278 will be applied in this thesis.

Hazard

- Physical situation with a potential for human injury and/or damage to environment (IEC 62278: *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*).
- Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment (MIL-STD-882D: *Standard practice for system safety*).

Risk

- Probable rate of occurrence of a hazard causing harm and the degree of severity of the harm (IEC 62278).
- An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (MIL-STD-882D).

It is important to note that hazard and risk are defined in various ways and that the expressions above are rather simply defined. For example, Leveson (1995) defines as follows:

- A hazard is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event).
- Risk is the hazard level combined with (1) the likelihood of the hazard leading to an accident (sometimes called danger) and (2) hazard exposure or duration (sometimes called latency).

Leveson clearly distinguishes between the likelihood of the hazard occurring and the likelihood of the hazard leading to an accident, and introduces the concept of exposure or duration of a hazard. (The probability of an accident increases if the hazard is present over long periods.) Her idea is summarized in Figure 5.1.

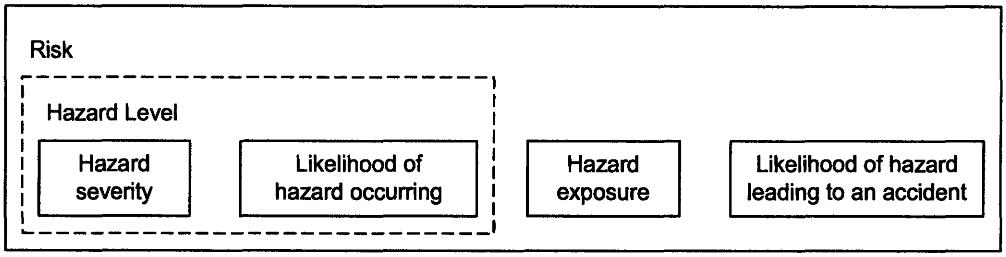

Risk
Hazard Level
Hazard severity
Likelihood of hazard occurring
Hazard exposure
Likelihood of hazard leading to an accident

Figure 5.1: Components of risk (Source: Leveson, 1995). There is a clear distinction between the likelihood of hazard occurring and the likelihood of hazard leading to an accident.

There are some things to note about these definitions.

(a) Hazard is completely different from risk.

It is important to recognize the difference between hazard and risk. In short, hazard is a condition that may lead to the accident, while risk is characterized by the combination of the probability of occurrence of a hazardous event and the severity of the hazard consequence. They are totally different concepts.

Take, for an example, the Fukuchiyama Line derailment accident. The system hazard related to this accident is derailment of vehicles. Then, the risk is characterized by the severity and probability associated with this hazard: (1) The probability is extremely low, since this was the first derailment accident that caused fatalities in eighteen years in Japan; and (2) The severity is high, since this hazard has potential to kill no less than one hundred people. As a result, the risk category associated with the derailment would be high or serious, depending on the criteria.

(b) There exists an important distinction between hazard analysis and risk analysis.

While the concepts of hazard and risk in the standards are clearly defined and are consistent with each other, there exists no clear consistency in the use of the term hazard analysis and risk analysis between them. (Neither standard provides the definitions of these terms.)

In IEC 62278, the term risk analysis is frequently used, while the term hazard analysis is rarely used. As described in Chapter 3, IEC 62278 lays great emphasis upon risk analysis, which is the third stage in the entire system life cycle, consisting of fourteen stages. The objectives of risk analysis are described as follows:

a) identify hazards associated with the system;
b) identify the events leading to the hazards;
c) determine the risk associated with the hazards;
d) establish a process for on-going risk management.

As for MIL-STD-882D, the term risk analysis is never used, while the term hazard analysis is sometimes used. The standard states that a systematic approach to achieve acceptable risk is comprised of hazard analysis, risk assessment, and risk management. Although the definitions of hazard analysis and risk management are not available, Appendix A provides the definition of (mishap) risk assessment as follows:

- Mishap risk assessment: The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions.

A further examination reveals that the objectives of a) and b) in IEC 62278 correspond with hazard analysis in MIL-STD-882D, c) corresponds with risk assessment, and d) corresponds with risk management, while the term risk analysis in IEC 62278 corresponds with a systematic approach to achieve acceptable risk. Table 5.1 summarizes these relationships. Consequently, hazard analysis should be regarded as a subset of risk analysis. Hereafter, the concepts above will be firmly adhered to concerning the terms of risk analysis, hazard analysis, risk assessment, and risk management.

Table 5.1: Comparisons of risk-related analysis terms in IEC 62278 and MIL-STD-882D.

IEC 62278	**MIL-STD-882D**
Risk Analysis	↔ Systematic Approach
a) identify hazards b) identify events leading to the hazards	↔ hazard analysis
c) determine the risk associated with the hazards	↔ risk assessment
d) establish a process for on-going risk management	↔ risk management

(c) Risk analysis, especially hazard analysis and risk assessment, is the key to assuring safety in today's complex railway systems.

In Chapter 4, one of the important lessons learned from the Fukuchiyama Line derailment accident was described as "risk/hazard analysis is the key to assuring safety in today's complex systems." Based on the concepts above, however, it would be more accurate to say that risk analysis, especially hazard analysis and risk assessment, is the key to assuring safety in today's complex railway systems.

As mentioned in the previous chapter, the entire company, including the management and the drivers, did not recognize the hazard of overturning, which was one of the factors that caused the accident. If an appropriate hazard analysis had been conducted and the hazard of overturning had been identified, the company might have been able to prevent the accident.

In addition, the poor hazard analysis led to the poor risk assessment. The company had an opportunity to mitigate the hazard of overturning, but it failed. As described in Section 4.2.6, the curve-speed-checking function was added into some ATS-SWs in March 2002. However, the company did not incorporate the function into the curve of the accident, because the company believed that driving at a speed of 120 kilometers per hour was sufficiently safe. It is important to note that it is not clear whether the company could have incorporated the function, even if the hazard of overturning had been identified. To put it another way, there was a possibility that the company might have failed because of poor risk assessment even if they successfully had identified the hazard. In short, appropriate hazard analyses alone are no longer enough to assure safety. They should be followed by appropriate risk assessment. Consequently, both hazard analysis and risk assessment are the key to assure safety.

5.1.2 Overview of hazard analysis

Hazard analysis is carried out to identify hazards associated with the system and to identify the events leading to the hazards. There are two categories of hazard analyses: types and techniques. While types address an analysis category such as analysis timing and system coverage, techniques define a unique analysis methodology such as Fault Tree Analysis (FTA) and Failure Mode Effect Analysis (FMEA). Generally, several different techniques are available for each of the various types (Ericson, 2005).

Many different techniques have been developed. For example, System Safety Society (1993) consolidates as many as ninety techniques into one reference, but still states that the techniques are not exhaustively covered.

Each hazard analysis technique has its own attributes, which are used to determine the hazard analysis technique to apply. Ericson (2005) lists the most significant attributes for a hazard analysis methodology as shown in Table 5.2. Some of these major attributes will be discussed further in the next subsection from the viewpoint of applying to high-speed maglev systems.

Table 5.2: Major attributes of hazard analysis techniques (Source: Ericson, 2005).

	Attribute	Description
1	Qualitative/quantitative	Analysis assessment is performed qualitatively or quantitatively
2	Level of detail	Level of design detail that can be evaluated by the technique
3	Data required	Type and level of design data required for the technique
4	Program timing	Effective time during system development for the technique
5	Time required	Relative amount of time required for the analysis
6	Inductive/deductive	Technique uses inductive or deductive resoning
7	Complexity	Relative complexity of the technique
8	Difficulty	Relative difficulty of the technique
9	Technical expertise	Relative technical expertise and experience required
10	Tools required	Technique is standalone or additional tools are necessary
11	Cost	Relative cost of the technique
12	Primary safety tool	Technique is a primary or secondary safety tool

While there are a number of hazard analysis techniques available, none of the standards, such as IEC 62278 and MIL-STD-882D, specifies any technique in particular to perform hazard analysis, as described in Chapter 3. It is engineers' responsibility to determine hazard analysis technique, since the choice of the technique should largely depend on the system under consideration (MIL-STD-882D). Therefore, selecting appropriate hazard analysis techniques among many has significant importance (Ericson, 2005; Leveson, 1995). Leveson (1995) describes a problem with regard to conducting hazard analysis as follows:

> No one method is superior to all others for every objective or even applicable to all types of systems. Perhaps the most important fact to keep in mind is that very little validation of any of these techniques has been done, and so all results should be treated with appropriate skepticism.

In these circumstances, it is worth deriving the requirements of hazard analysis for high-speed maglev systems, which will be described in the next subsection.

5.1.3 Hazard analysis and risk assessment requirements for maglev systems

The requirements of hazard analysis and risk assessment for high-speed maglev systems are derived in this section, based on the characteristic features described in Chapter 2 and lessons learned from the Fukuchiyama Line derailment accident discussed in Chapter 4. The derived requirements are:

(1) Hazard analysis techniques must emphasize qualitative analyses, rather than quantitative analyses;
(2) Hazard analysis techniques must adopt a deductive (top-down) approach;
(3) Hazard analysis techniques must be able to identify the future hazards that result from asynchronous evolution;
(4) Hazard analysis techniques must be able to consider human errors closely;
(5) Risk assessment must pay closer attention to the severity of accidents, rather than the probability.

It is important to note that hazard analysis techniques that are applied to system development should not be limited to one methodology. Ericson (2005) recommends applying several kinds of techniques in order to identify all the hazards within the system. The requirements here are derived on the assumption that multiple hazard analysis techniques are being applied.

(1) Hazard analysis techniques must emphasize qualitative analyses, rather than quantitative analyses.

Qualitative and Quantitative analysis

As shown in Table 5.3, the qualitative-quantitative factor is one of the major attributes of hazard analysis techniques. Ericson (2005) states:

> Analysts are often in a quandary as to whether to use a qualitative analysis technique or a quantitative analysis technique. Understanding which analysis type to use, and when, often seems more of an art than a science.

Ericson also lists the advantages and disadvantages of qualitative and quantitative approaches as shown in Table 5.3. In short, objective numerical results can be acquired through quantitative hazard analyses. However, the analyses have several disadvantages such as higher cost and longer time.

Table 5.3: Advantages and disadvantages of qualitative and quantitative approaches (Source: Ericson, 2005).

	Attribute	Qualitative	Quantitative
1	Numerical results	No	Yes
2	Cost	Lower	Higher
3	Subjective/objective	Subjective	Objective
4	Difficulty	Lower	Higher
5	Complexity	Lower	Higher
6	Data	Less detailed	More detailed
7	Technical expertise	Lower	Higher
8	Time required	Lower	Higher
9	Tools required	Seldom	Usually
10	Accuracy	Lower	Higher

Requirement for high-speed maglev systems

The conclusion in this thesis is that the hazard analysis techniques should place emphasis on a qualitative approach, rather than a quantitative approach.

The most important reason is that determination of the probability of the accidents that do not stem from a simple component failure is impossible, while it is this kind of accident that the current railway engineers must pay close attention to. The Fukuchiyama Line derailment accident demonstrates that the accidents that resulted from inadequate interactions among socio-technical components definitely occur in the railway industry as well as other industries. The argument suggests that the railway industry should be especially concerned about non-component-failure accidents at this time. It may be manageable to figure out the probability of a simple component failure. However, there is no reasonable way to determine the likelihood of accidents caused by inadequate interactions among socio-technical components. In fact, IEC 62278: *Railway applications – Specification and demonstration of* *reliability, availability, maintainability and safety (RAMS)* categorizes systematic failures as non-quantifiable elements.

In addition, software intensiveness and human involvement make determination of the likelihood of an accident even more difficult. (1) The high-speed maglev systems require more extensive use of software than conventional railway systems, as described in Chapter 2, and software performs many safety-critical control and monitoring functions in today's rail transit systems (Hermann, 1999). However, it is difficult at best to determine the probability of failure of software since it cannot be based on historical data. (2) Human factors are crucially involved in today's railway systems, including the high-speed maglev systems, as the Fukuchiyama Line derailment demonstrates. However, there exists a limitation in assigning a probability to human errors, especially human errors occurring under great pressure (Leveson, 1995).

Consequently, a qualitative analysis should be emphasized for high-speed maglev systems.

Inconsistency with the current approaches

As described in Chapter 3, in the German Transrapid maglev systems, the quantitative safety target, such as 10^{-6}/year, is designated first, and its fulfillment is demonstrated later (Steiner & Steinert, 2006). On the contrary, the finding in this thesis proposes that qualitative safety analysis, rather than quantitative analysis, should be emphasized. Given that resources such as time and workforce are limited, quantitative analysis, which is prevalent in the Transrapid systems, should be minimized. (In this sense, the Japanese approach, in which a quantitative analysis is discounted, is rather consistent with the finding.)

(2) Hazard analysis techniques must adopt a deductive (top-down) approach.

Inductive and Deductive techniques

Another important attribute of the hazard analysis technique is whether it is inductive or deductive. It is helpful first to explain the concepts of inductive analysis and deductive analysis briefly from a practical viewpoint. Ericson (2005) describes them as follows and summarizes the relationship in Figure 5.2.

An inductive analysis can be thought of as a "what-if" analysis. The analyst asks: What if this part failed, what are the consequences? A deductive analysis can be thought of as a "how-can" analysis. The analyst asks, if this event were to occur, how can it happen or what are the causal factors?

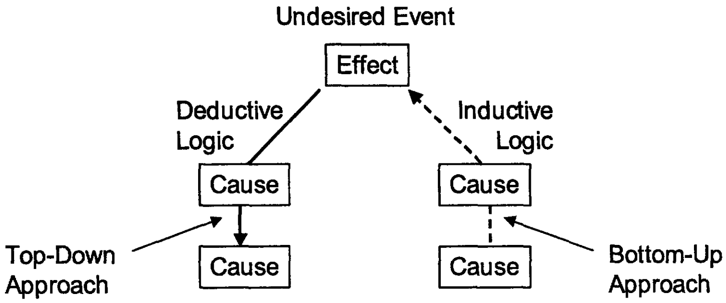


Figure 5.2: Inductive and deductive analysis relationship (Source: Ericson, 2005).

The Fault Mode Effect Analysis (FMEA) is representative of an inductive analysis: It supposes failure of a sub-element first and determines the results or effects of it. The Fault Tree Analysis (FTA) is representative of a deductive analysis: It identifies an undesirable event first and examins the range of potential events that could lead to the event. Ericson (2005) also lists the advantages and disadvantages of inductive and deductive approaches as shown in Table 5.4.

Table 5.4: Inductive and deductive analysis characteristics (Source: Ericson, 2005).

	Inductive	**Deductive**
Applicability	• Systems with few components • Systems where single-point failures (SPFs) are predominant • Preliminary or overview analysis	• All sizes of systems • Developed for complex systems • Designed to identify hazards caused by multiple failures
Potential pitfalls	• Difficult to apply to complex systems • Large number of components to consider • Consideration of failure combinations becomes difficult	• Detailed system documentation required • Large amount of data involved • Time-consuming

Requirement for high-speed maglev systems

The finding in this thesis is that deductive analysis is more appropriate for high-speed maglev systems than inductive analysis. Two arguments, which will be described below, support this finding.

First, an inductive approach does not work well for system accidents, which today's railway industry should pay closer attention to. As mentioned, an inductive approach supposes failure of a sub-element first. However, system accidents are those that arise from inadequate interactions among components, and there is no component failure in the system accidents. As long as the approach assumes that there is a component failure, it cannot identify all the hazards in high-speed maglev systems.

It may be possible to start from an inadequate interaction and follow an inductive approach. However, it is not practical for complex systems such as high-speed maglev systems. As shown in Table 5.5, one of the disadvantages of the inductive approach is that it becomes difficult to apply to complex systems because many components should be considered. It may be manageable to consider all failures of components, but examining all interactions of components becomes much more difficult because the number of component interactions to be considered is much larger than the number of simple component failures.

Next, the long history of the railways has already identified the general nature of the hazards: All of the system hazards in railway systems are crash, derailment, and fire. This is also true for high-speed maglev systems, and is considered to be an appropriate condition for a deductive approach, in which it identifies an undesirable event first and examines the range of potential events that could lead to the event. Since an undesirable event must be one of the three, it is easy to start a deductive approach. This is another reason that a deductive analysis is more appropriate than an inductive analysis.

Inconsistency with the current approaches

As described in Chapter 3, the FTA (deductive approach) and FMEA (inductive approach) analysis techniques are currently applied to analyze safety in the Transrapid maglev systems (Steiner & Steinert, 2006; Steinert, 2004). They are also recommended for safety analyses in the Japanese railway industry (Mizoguchi & Sato, 2006).

Another common technique in the railway industry is HAZOP, the Hazard and Operability Analysis (Ericson, 2005). The HAZOP is a method of organized brainstorming about the significance of the event in which a process element malfunctions or is incorrectly operated. It utilizes short guide words to stimulate the imagination of a deviation of the design intent in system parameters, such as pressure, temperature, vibration, and startup. The guide words include no, more, fluctuation, late, before, and faster. Using the system parameters and guide words is the key in the HAZOP analysis. Since it assumes the deviation of an element first, this is classified as an inductive approach (System Safety Society, 1993).

The conclusion in this thesis shows that the FMEA and HAZOP analysis techniques, which are prevalent in the current railway industry, cannot identify all the hazards in high-speed maglev systems, since they adopt an inductive approach. Among these, only the FTA analysis is a qualified technique for high-speed maglev systems from the viewpoint of the inductive/deductive attribute.

(3) Hazard analysis techniques must be able to identify the future hazards that result from asynchronous evolution.

Requirement for high-speed maglev systems

Another requirement of the hazard analysis techniques for the high-speed maglev systems is that it must be able to identify the future hazards that result from asynchronous evolution. To put it another way, the hazard analysis must identify future evolution that might lead to new hazards that do not currently exist.

Take the Fukuchiyama Line derailment accident, for example. The company increased the speed limit on the line by 20 kilometers per hour and reduced the radius of the curve by 300 meters. These alterations (evolution) eventually created the new hazard of overturning at the curve. What this requirement proposes is that the company should have recognized, before the alterations, that these alterations could cause a new hazard. If the company had recognized that, they could have canceled the alterations or could have introduced an improved safety device along with the alterations, which could have prevented the accident.

It is important to note that the concept of these future hazards caused by asynchronous evolution is not universally considered among hazard analysis techniques: Table 5.3 does not include an attribute of manageability of future hazards, and no hazard analysis technique explained in System Safety Society (1993) or Ericson (2005) claims that these techniques can deal adequately with future hazards. An inductive hazard analysis approach supposes that there is a failure of a component (FMEA) or a deviation in the system parameters (HAZOP). However, it never considers modification or evolution of a subsystem, which is common practice in high-speed maglev systems.

There are two ways to fulfill this requirement. One is to update or re-conduct the hazard analysis whenever a modification plan emerges. If the hazard analysis is appropriate and can identify all new hazards, the hazards can be eliminated or mitigated by changing the design or introducing additional devices. This process is considered to be passive in the sense that an alteration plan comes first, before the hazard analysis.

The other way is to identify, in the first place, future evolution that might lead to new hazards and to forbid such evolution. It is useful to introduce the concept of constraints here. Leveson (2002) states that accidents result from a lack of constraints imposed on the system design, rather than component failures, and that the design constraints to assure safety in the system should be identified through hazard analyses. (Based on these ideas, Leveson develops an original hazard analysis technique named STPA, the STAMP-based hazard analysis. The STPA analysis will be further explained and applied in the next chapter.) Once not only the hazards but also the constraints in the system are identified through hazard analysis and enforced appropriately, there is no room for asynchronous evolution. In that sense, identifying the constraints in the first place is considered to help prevent future hazards. This is just one example, but it shows that asynchronous evolution is actively manageable through hazard analyses.

Inconsistency with the current approaches

IEC 62278, the railway international standard, recognizes the concept of asynchronous evolution, and it demands that risk analysis be re-applied whenever there is a modification or upgrade, which is an important process. However, the standard should also recognize that some appropriate hazard analysis techniques can actively manage asynchronous evolution in the first place.

(4) Hazard analysis techniques must be able to consider human errors closely.

Requirement for high-speed maglev systems

The conclusion in this thesis is that hazard analysis techniques for high-speed maglev systems must be able to deal adequately with human errors. As the Fukuchiyama Line derailment accident reveals, human factors play a major role in current railway systems, including high-speed maglev systems. It is definitely important to take human factors into consideration through hazard analyses in the railway industry as well as other industries. The difference from the former requirement is that the importance of human errors is widely recognized in various industries, while asynchronous evolution (as described in the former requirement) is hardly addressed. Therefore, manageability of human factors is already considered to be one of the important attributes of hazard analysis techniques, and well explained. For example, Ericson (2005) states:

- **FMEA**: Provides limited examination of human error (disadvantage);
- **FTA**: Combines hardware, software, environment, and human interaction (advantage);
- **Operating and Support Hazard Analysis (O&SHA)**: Hazardous procedures, design conditions, failure modes, and human errors that could lead to the occurrence of an undesired event can be identified (advantage).

Looking into every hazard analysis technique to see if it works well for human errors is outside the scope of this thesis. What this thesis insists is that a hazard analysis technique that can examine human error closely must be incorporated when necessary.

Inconsistency with the current approaches

Although IEC 62278, the railway international standard, includes human errors in systematic failure as shown in Figure 4.22, and claims that they are inside the scope of the standard, it is not clear how human errors are taken into consideration during hazard analyses in the railway industry. For example, Mizoguchi and Sato's (2006) reference book about RAMS methods for Japanese railway engineers provides no information about human errors, which implies that human factors are not considered important.

(5) Risk assessment must pay closer attention to the severity of accidents, rather than the probability.

Requirement for high-speed maglev systems

The conclusion in this thesis is that the severity of accidents, rather than the probability, should be primarily considered during risk assessment.

The Fukuchiyama Line derailment accident reveals that in the railway industry, there exists a potential accident that is very rare but causes enormous damage. This would be true in high-speed maglev operations. On the other hand, the arguments in (1) demonstrate that it is impossible to determine the probability of this kind of accident quantitatively. Also, the same arguments will show that the probability of accidents will not be accurate even if it is qualitatively analyzed. Consequently, when assessing risk, which is characterized by the severity and probability of accidents, it is not appropriate to focus on the probability because of its uncertainty. The severity of accidents can be estimated with accuracy to some degree, and it is the severity that should be primarily assessed.

Inconsistency with the current approaches

As described in Chapter 3, the current international standard, IEC 62278, proposes the formation of a "frequency-consequence" matrix for risk assessment. This matrix, of which an example is shown in Table 3.4, evenly considers the severity and the probability of accidents.

On the other hand, the finding in this thesis is that the severity of accidents should be emphasized during risk assessment, since the probability of accidents cannot be determined correctly. Considering its uncertainty, use of the probability should be minimized.

5.2 System Safety and high-speed maglev systems

In this section, System Safety approaches will be described first, and their applicability to high-speed maglev systems will then be addressed. System Safety is an organized and established method to assure safety in complex systems, and it is comparable to other approaches to safety, such as industrial safety and reliability engineering. (In order to emphasize this point, the term System Safety will be capitalized in this thesis.)

5.2.1 Overview of the System Safety approach

History

According to Miller (1998), the concept of System Safety appeared after World War II. Amos L. Wood of the Boeing Company presented the paper ("The organization and utilization of an aircraft manufacturer's air safety program") in 1946, emphasizing "continuous focus of safety in design," "advance analysis and post accident analysis," "safety work ... most effective when it is not fettered by administrative pitfalls." William I. Stieglitz of the Republic Aircraft Corporation added his own idea in the paper ("Engineering Safety," published in *Aeronautical Engineering Review* in 1948) as follows:

> Safety must be designed and built into airplanes, just as are performance, stability and structural integrity. A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or weights group.... A safety program can be organized in numerous ways and there is probably no one best way.

These perspectives above are considered to be origins of the System Safety approach. Subsequently, Charles O. Miller, who is one of the co-founders of the System Safety Society in the U.S., described System Safety in broader terms in a 1984 study for the Office of the Secretary of Defense:

> a highly technical discipline employing a variety of safety engineering and management tasks ... which addresses all aspects of safety, having its greatest impact when applied during the early design and development stages of a new system ... the process by which hazards are identified and controlled throughout the life cycle of a system.

The formal requirements of System Safety were established in the 1960s along with the development of ballistic missiles and other space vehicles with high-energy and toxic rocket propulsion system fuels. The U.S. Air Force established MIL-S-38130: *General requirements for safety engineering of systems and equipment* in 1963, and the Army constituted MIL-S-58077: *Safety engineering of aircraft systems, associated subsystems, and equipment; General requirements for* in 1964. Afterwards, in 1969, MIL-STD-882: *System safety program for systems and associated subsystems and equipment* finally appeared, and all of the Department of Defense-procured products and systems were required to adhere to this standard. The latest version of MIL-STD-882 (MIL-STD-882D: *Standard practice for system safety*), which was issued in 2000, defines System Safety as:

> The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

General Principles

General principles of System Safety are derived as follows, from the Air Force System Safety Handbook (2000), Ericson (2005), Leveson (1995), Miller (1988), MIL-STD-882, Software System Safety Handbook (1999), and System Safety Analysis Handbook (1993).

(a) The goal of System Safety is to prevent accidents before they occur for the first time, utilizing analysis.

System Safety emphasizes advance analysis to prevent first time accidents. It is important to note that this approach to safety is different from the fly-fix-fly approach, in which safety engineers wait for accidents to demonstrate design problems. Behind this change is the fact that the previous approach becomes economically and ethically unacceptable as the system becomes hugely expensive and as the potential for catastrophic accidents increase.

(b) System Safety deals with systems, rather than components.

As implied in the name, the scope of System Safety is system. MIL-STD-882D defines system as:

- **System**: An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

In short, a system is a combination of subsystems to accomplish the system objective. As long as the goal of System Safety is to prevent accidents caused by the system, the System Safety analysis should consider all components associated with systems, such as people, products, and processes. Additionally and most importantly, System Safety should examine interfaces between them and the overall system itself.

(c) Safety must be built into the system, rather than added to the system, by timely analysis throughout all phases of the system life cycle.

System Safety demands that safety analysis be conducted in a timely manner, especially during the early design and development stages of the system because it is the most effective and economical time to do so. System Safety is a discipline employed from the initial design steps through system disposal, and there exists appropriate analysis techniques in every phase of the system life cycle.

(d) The key to System Safety is hazard analysis, which identifies, eliminates, mitigates, and controls hazards in the system.

Hazard and risk inevitably exist in today's systems. The concept of System Safety is that, if a hazard is eliminated or mitigated, the corresponding accident is also mitigated or controlled. To successfully control hazards, it is necessary to know how to identify them. Consequently, System Safety pays much attention to hazard analysis, which can identify hazards and events that could lead to the hazards.

It is important to note that the principles above are merely general ones. The term System Safety is widely used, some corresponding to the System Safety approach, and some meaning simply safety of the system. Furthermore, even if it refers to the System Safety method, there are many variations. Miller (1988) describes this situation as follows:

> Agreement is not complete even among experienced practitioners in the field, although the varying interpretations can most often be traced to the particular part of a system's life cycle in which the commentator is engaged.

The statement above is definitely valid, and not only the system's life cycle but also the nature of the systems, such as simple, complex, hardware intensive, and software intensive, affects the engineers' interpretations.

For example, Nancy Leveson, who significantly contributed to Software System Safety, adds some other principles. One of them is:

- System Safety emphasizes qualitative rather than quantitative approaches (Leveson, 1995).

Marais, Dulac, and Leveson (2004) further propose "*systems* approach to safety," distinguishing it from "standard system safety." (The author assumes that their *systems* approach to safety is still in the category of System Safety.) Its principles are:

- *Systems* approach to safety applies top-down systems thinking, rather than a bottom-up, reliability engineering focus;
- *Systems* approach to safety focuses on the integrated socio-technical system as a whole and the relationships between the technical, organizational, and social aspects.

In short, the principles of the System Safety approach are clear and totally different from those of reliability engineering and industrial safety. Based on these principles, there exist various System Safety derivatives, which are especially developed to deal with the nature of every system under consideration.

Current situations

The System Safety approaches are applied to various industries in the U.S.. One of the industries is the Air Force, who constituted the standard of the System Safety (MIL-S-38130) for the first time in 1963. They developed their own System Safety approach, which is summarized in the Air Force System Safety Handbook (2000). The handbook provides one example of the F-4 and F-14 aircrafts, which had similar missions through 1981. The cumulative material failure accidents for the F-4, which did not have a formal System Safety program, occurred at a rate of 9.52/100,000 hours, while the comparable rate of the F-14, which had a formal System Safety program, was 5.77/100,000 hours. The handbook does not state that the difference in the rate stemmed from the existence/nonexistence of the System Safety program because there were many other factors such as different operational environments and different contractors. However, this example is worth noting because there is a possibility that this example demonstrated the effectiveness of the System Safety program. The handbook also provides several cases, in which the System Safety program identified hazards and corrected them before accidents occurred. These examples, which are in Figure 5.3, demonstrate the effectiveness of the System Safety program in the U.S. Air Force.

- During the design of the F-18, fire hazard was minimized when a system safety engineer convinced program decision makers that a proposed increase in allowable bleed air duct temperature was dangerous and that a similar hazard could be avoided by ensuring that the bleed air shutoff valve closed when power was removed.
- During a modification to the B-52, a system safety engineer noted that if the front lugs of the air launched cruise missile attachment retracted, but the rear ones did not, parts of the pylon would tear from the wing and, together with the missile, would inflict severe structural damage on the wing and possibly the horizontal stabilizer.
- A Safety engineer found in the PAVE LOW helicopter system that loss of voltage in a radar circuit would cause a command to the aircraft to fly at zero altitude with no warning to the pilot. He also checked with personnel on the RF-4C and A-7D programs, knowing they used the same system. All aircraft were quickly prohibited from flying certain low-level missions until the systems were corrected.

Figure 5.3: Examples that show contributions of the U.S. Air Force (Source: Air Force System Safety Handbook, 2000).

The U.S. Navy developed the Submarine Safety (SUBSAFE) program in 1963 and 1964, after the nuclear submarine Thresher sank off the New England coast and killed all 129 men on board in April 1963. The SUBSAFE program covers a broad range of topics. It is not clear if the SUBSAFE program is considered to be the System Safety approach in a precise sense. In any case, the SUBSAFE program is a well-organized and well-established approach to assure safety in the submarines. Since then, no submarine that followed the SUBSAFE program has sunk, which shows the effectiveness of the SUBSAFE program. (The Scorpion sank in May 1968. However, the Scorpion had not been given the full SUBSAFE update.) (Polmar, 2004).

The space industry also actively applies the System Safety approaches in a disciplined fashion. An accident, in which three astronauts were killed in a fire while testing their Apollo capsule on the pad in 1967, forced NASA to introduce the System Safety approach, rather than traditional industrial worker safety. Since then, the System Safety program was set up for space projects, using examples from the Air Force and DoD programs (Leveson, 1995).

As shown in the examples above, the non-commercial industry such as the Air Force and NASA have been pioneers in the System Safety approaches.

5.2.2 Applicability of System Safety approaches to maglev systems

Table 5.5: Comparison between lessons learned from the Fukuchiyama Line derailment accident and the general principles of the System Safety approaches.

Lessons learned from the accident	General principles of System Safety
1) This is not a component failure, but a system accident, with which the reliability engineering approach cannot deal. 2) This type of accident, a derailment accident, is extremely rare; however it still has great potential to cause enormous damage. 3) Risk/hazard analysis is the key to assuring safety in today's complex systems. 4) The accident deeply involves human factors, which play a major role in current railway systems. 5) It is almost impossible to figure out the probability of this type of accident.	a) The goal of System Safety is to prevent accidents before they occur for the first time, utilizing analysis. b) System Safety deals with systems, rather than components. c) Safety must be built into the system, rather than added to the system, by timely analysis throughout all phases of the system life cycle. d) The key to System Safety is hazard analysis, which identifies, eliminates, mitigates, and controls hazards in the system.

Valuable lessons are learned through analyzing the Fukuchiyama Line derailment accident described in Chapter 4. Compared to the basic concepts of the System Safety described in this chapter, the lessons learned from the accident demonstrate the need for System Safety approaches in high-speed maglev systems.

Table 5.5 provides a summary and comparison between the lessons learned from the Fukuchiyama Line derailment accident and the general principles of the System Safety approaches. To be more accurate, the first three lessons definitely point out the need for the System Safety approaches.

The first lesson is that (1) close attention should be paid to a system accident, rather than a component failure. This finding corresponds to the second principle, which is that (b) System Safety deals with systems, rather than components. Since a system accident results from inadequate interactions between components, the System Safety approach is appropriate in the sense that it examines interfaces between subsystems and the overall system itself.

The second lesson learned from the accident is that (2) in the railway industry, there exists a potential accident that is very rare but causes enormous damage. Furthermore, as described in Chapter 2, the potential severity of accidents in high-speed maglev systems is much higher than that in traditional railway systems. This implies that the traditional fly-fix-fly approach is not allowed in railway systems. The railway industry must prevent the accident from the beginning, which is consistent with the System Safety principle (a).

The third one is that (3) risk/hazard analysis is the key to assuring safety in today's complex systems. This coincides, in a straightforward manner, with the System Safety principle (d), which is that the key to System Safety is hazard analysis, which identifies, eliminates, mitigates, and control hazards in the system.

All these arguments suggest that the System Safety approach is necessary in railway systems, including high-speed maglev systems. To put it another way, there is ample room to introduce System Safety approaches in high-speed maglev systems.

Suppose that the general concepts of the System Safety program are incorporated into system development of high-speed maglev systems; the remaining task is to determine what kind of System Safety approach, among various derivatives, is appropriate. In regard to this matter, the five requirements of hazard analysis/risk assessment, derived in the first half of this chapter, definitely identify solutions.

In conclusion, the System Safety approach is necessary in system development of high-speed maglev systems. It is necessary to require the application of an appropriate System Safety approach among many System Safety approaches, based on the derived requirements of hazard analysis and risk assessment.

Chapter 6

Organizational Requirements for High-Speed Maglev Systems

Finally, organizational risk analysis is conducted for high-speed maglev systems. The arguments so far demonstrate that one of the most critical system hazards in high-speed maglev systems is poor risk analysis, and that the engineers must pay closer attention to the quality of risk analysis. This chapter derives the organizational requirements to prevent poor hazard analysis from happening, applying a STAMP (System-Theoretic Accident Modeling) risk analysis.

6.1 Brief reviews of STAMP risk analysis

A STAMP risk analysis, as well as the STAMP model of accident causation, has been developed by Nancy Leveson at Massachusetts Institute of Technology (MIT). This method will be applied to examine the organizational requirements for high-speed maglev systems. In this subsection, first, the STAMP risk analysis is briefly reviewed. (Leveson (2002), and Leveson and Dulac (2005) are the sources for this review if not otherwise specified.)

The basic concepts of the STAMP risk analysis are the same as those of the STAMP model of accident causation, which were described in Chapter 4. In short, safety is considered to be a control problem, and accidents are viewed as a result of inadequate control interactions among components, including physical system components, socio-technical components, and operators. In accident modeling, inadequate control actions that actually occurred are examined for each component in the control structure. Similarly, in the risk analysis, inadequate control actions that may lead to an accident in the future are examined for each component, which is an essential process in the STAMP risk analysis.

In practice, there are six steps, which are shown in Figure 6.1. The first step, preliminary hazard analysis, is similar to those performed in other analysis techniques. The safety requirements and design constraints are identified in this step. After establishing a control structure in Step 2, the safety requirements are assigned to each component in the control structure (Step 3), and the inadequate control actions are subsequently identified for each component in Step 4. Step 4 is specifically named as STPA (STAMP-based hazard analysis).

1. Perform a high-level system hazard analysis, i.e., identify to be the focus of the analysis and then the system requirements and design constraints necessary to avoid those hazards.
2. Create the STAMP hierarchical safety control structure using either the organizational design as it exists (as in the case) or creating a new design that satisfies the system requirements and constraints. This control structure will include the roles and responsibilities of each component with respect to safety.
3. Identify any gaps in the control structure that might lead to a lack of fulfillment of the system safety requirements and design constraints and places where changes or enhancements might be helpful.
4. Perform an STPA to identify the inadequate controls for each of the control structure components that could lead to the component's responsibilities not being fulfilled. These are the system risks.
5. Categorize the risks as to whether they need to be assessed immediately or whether they are longer-term risks that require monitoring over time. Identify some potential metrics or measures of effectiveness for each of the risks.
6. Create a System Dynamics model of the non-linear dynamics of the system and used the models to identify the most important leading indicators of risk and perform other types of analysis.

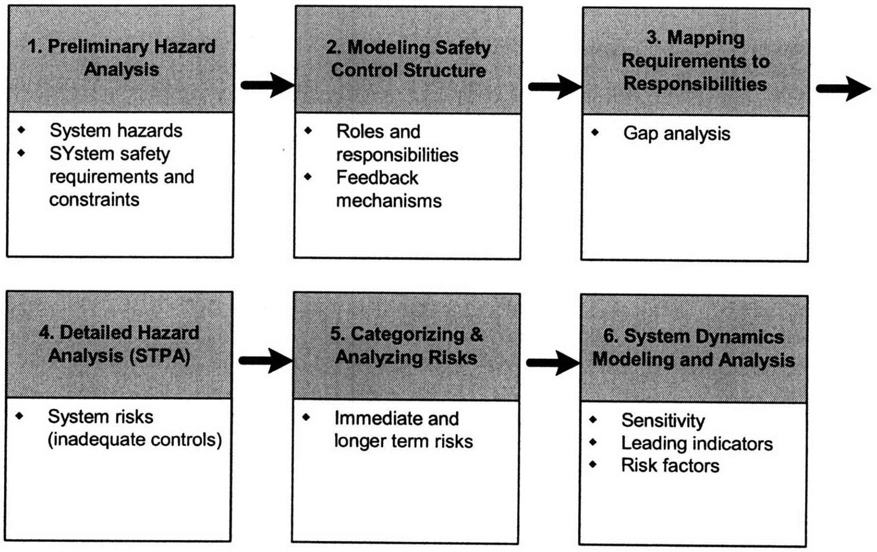

1. Preliminary Hazard Analysis
• System hazards
• SYstem safety requirements and constraints
2. Modeling Safety Control Structure
• Roles and responsibilities
• Feedback mechanisms
3. Mapping Requirements to Responsibilities
• Gap analysis
4. Detailed Hazard Analysis (STPA)
• System risks (inadequate controls)
5. Categorizing & Analyzing Risks
• Immediate and longer term risks
6. System Dynamics Modeling and Analysis
• Sensitivity
• Leading indicators
• Risk factors

Figure 6.1: Process of a STAMP risk analysis (Source: Leveson & Dulac, 2005).

6.2 Risk analysis of high-speed maglev system organizations

6.2.1 STAMP risk analysis process outcomes

The purpose of the risk analysis in this chapter is to identify the organizational requirements that prevent poor risk analysis. As discussed in Chapter 4, poor risk analysis is one of the important factors that caused the Fukuchiyama Line derailment, and risk analysis is the key to assuring safety in high-speed maglev systems. Although there exist several system hazards that lead to an accident in general, this analysis focuses clearly on one hazard, which is poor risk analysis leading to an accident.

It is important to note that this is a limited analysis in the sense that all of the system hazards are not considered. Dulac, Owens, and Leveson (2007) demonstrate the importance of balancing multiple risk components including safety, cost, performance, and schedule, through risk analysis for NASA's constellation program. There is a possibility that technical decision is inappropriately made based on some considerations other than safety, such as cost and schedule, recognizing the risk of the decision. However, this analysis does not take such a possibility into consideration. Furthermore, this analysis assumes that execution of the decision poses no problem. There might exist some problems during the execution phase. However, they are not considered in this risk analysis. Again, the main concern here is to improve the quality of risk analysis.

Below are the outcomes of every step in the risk analysis. In order to avoid confusion, only the outcomes are simply described, without comments. Further discussions about the outcomes will be followed in the next subsection. Among six steps proposed in Leveson and Dulac (2005), only the first four steps and part of Step 6 are performed in this thesis. Since the target is high-speed maglev system organization in general and it is not a concrete target, specific details about the organization are no longer available. Without details, it is not fair to categorize the risks (Step 5) and to complete a System Dynamics analysis (Step 6). In Step 6, only a simplified System Dynamics model about quality of risk analysis is developed, as shown in Figure 6.4. It is important to note that more complicated model is required to conduct simulation. This model does not provide any new information, but serves as a short summary of Step 4.

Step 1: Preliminary hazard analysis

The first step of the STAMP risk analysis is to identify the high-level system hazard. Since the objective of this risk analysis is to derive the organizational requirements to avoid poor risk analysis, the system hazard in this analysis is:

System Hazard: ***Poor risk analysis leading to an accident***

Subsequently, the system-level requirements and constraints to avoid the system hazard are derived below.

System-level requirements and constraints:

1. Risk analysis must be conducted in a consistent and systematic manner.

a. All the people involved in system development including the executives and development engineers must recognize the importance of risk analysis.

b. The process of risk analysis must be explicitly incorporated into the standards or specifications.

2. The results of risk analysis must be of high quality and cover all risks of the system.

a. People in charge must have sufficient ability to conduct advanced risk analysis.

b. The entire workforce, including the executives and operators, must contribute to improving the quality of risk analysis.

3. Risk analysis must be carried out in a timely manner when necessary.

a. Considerable efforts must be devoted to risk analysis during the early design and development stages of the system.

b. The result of risk analysis must be updated when there is a modification of the system, or when the environment surrounding the system changes.

Step 2: Modeling the safety control structure

The safety control structure for this risk analysis is shown in Figure 6.2. The base of this model is the one that was developed in Chapter 4 to analyze the Fukuchiyama Line derailment accident, and this model is slightly modified to make it general. Details of the requirements of each organization will be explained in Step 3. In short, the assumptions about this control structure are: (1) Transport Safety Department establishes a safety program policy and monitors whether subordinate organizations adhere to its policy; (2) Transport Department (TD), Truck & Structure Department (TSD), and Rolling Stock Department (RSD) not only develop the system, but also actually implement the safety program for operations including a timetable, ground equipment, and rolling stocks, respectively; and (3) Signal Station (SS), Manufacturing Company (MC), and Driver's Office (DO) work in a field of ground equipment, rolling stocks, and operations, respectively.

It is important to note that there exists significant difference in terms of the organizational structure between the Japanese railway industry and European industry. While an operation company in Japan acts as a system integrator to develop the system in addition to operating the system, a prime contractor intervenes directly in the system development in Europe (Mizoguchi & Sato, 2006). These frameworks are summarized in Figure 6.3. From this point of view, the control structure in Figure 6.2 represents the Japanese railway system.

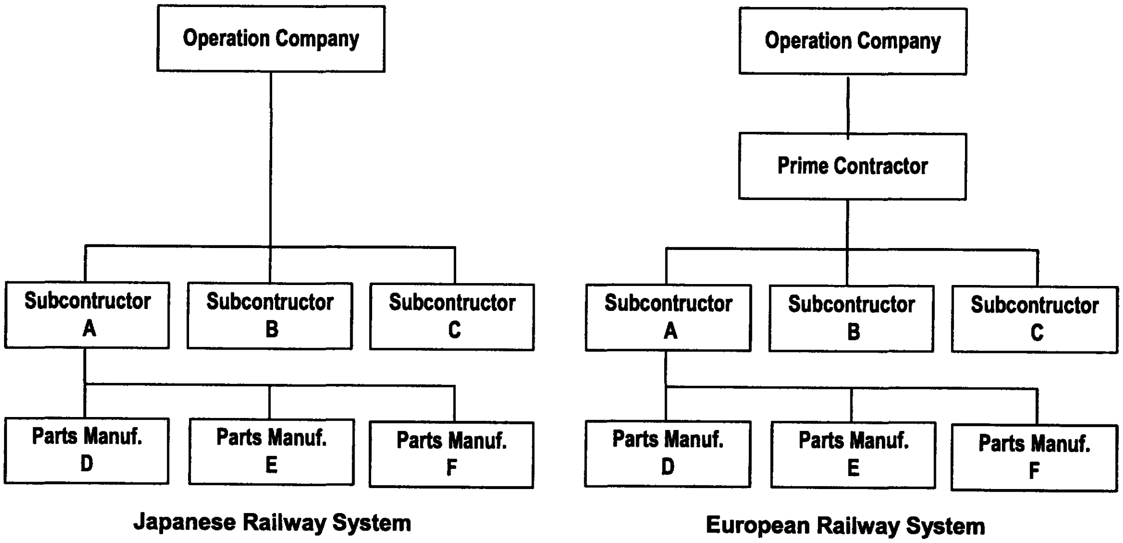


Figure 6.3: Comparison between the Japanese railway organizational structure and European railway organizational structure (Source: Mizoguchi & Sato, 2006): There exists a prime contractor in the European railway system.

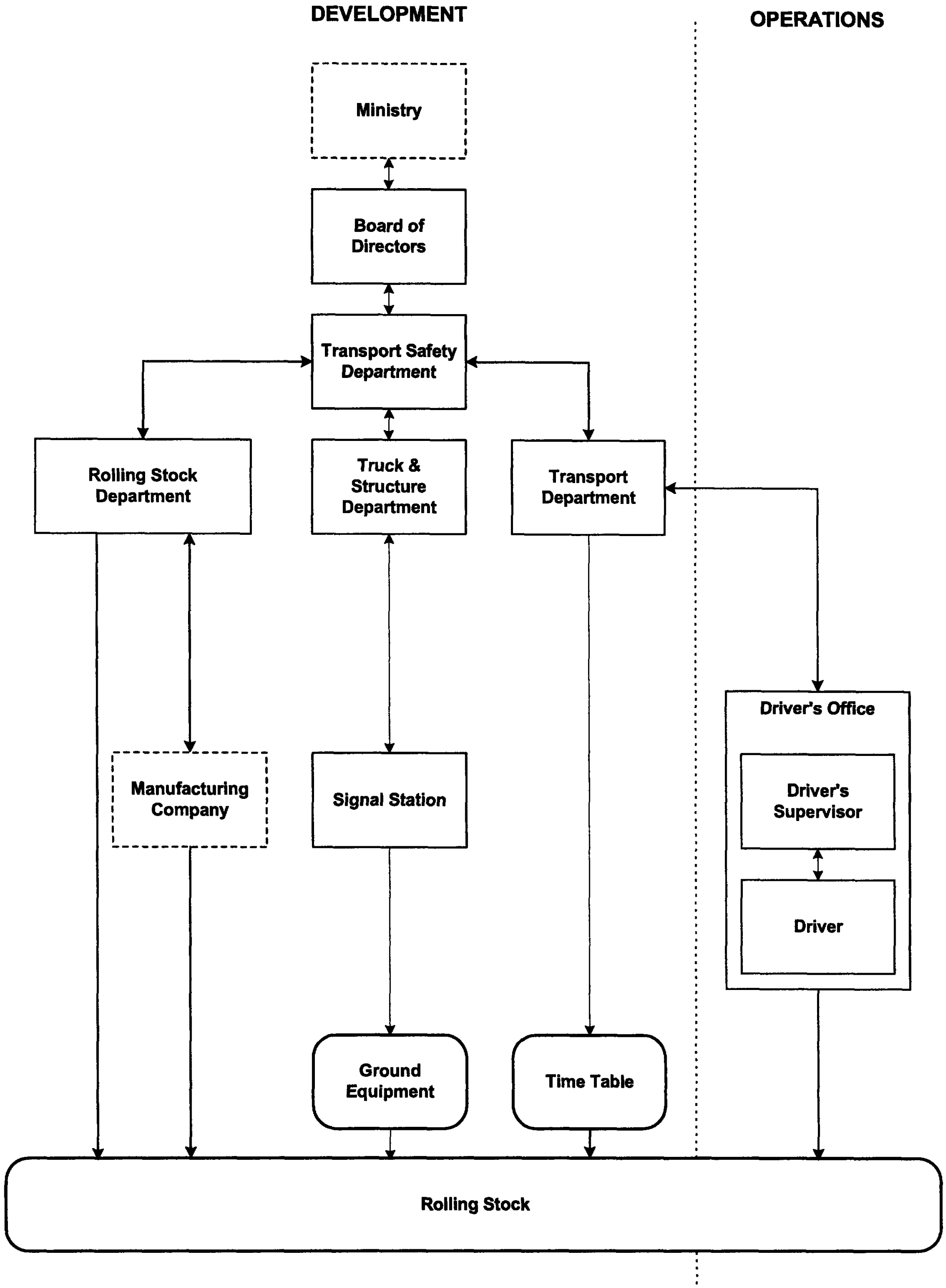


Figure 6.2: Basic high-speed maglev system safety control structure: Rectangles with sharp corners are controllers while rectangles with rounded corners represent material or immaterial products. In addition, rectangles with continuous lines are organizations within the operation company while rectangles with dashed lines are outside the operation company.

Step 3: Mapping requirements to responsibilities

1. Risk analysis must be conducted in a consistent and systematic manner.

1a. All of the people involved in system development, including the executives and development engineers, must recognize the importance of risk analysis.

Ministry: Effectively inform railway companies of the accidents that have happened all over the world to set the stage for them to think about the risk.

Board:

- Provide funding and authority to Safety Department to enforce risk analysis across the company.
- Monitor whether the safety program is adequately managed by Safety Department.

Safety Dept.:

- Analyze the accidents that have happened all over the world to realize the importance of risk analysis as well as to recognize possible new risks in the system.
- Effectively inform other organization components of the results of the analysis of the accidents.
- Reflect findings from accident analyses in technical specifications.

1b. The process of risk analysis must be explicitly incorporated into standards or specifications.

Ministry: Require railway companies to report to the ministry the safety program standards or specifications that stipulate the system development process, and approve them.

Board: Approve the safety program standards or specifications into which the process of risk analysis is explicitly incorporated.

Safety Dept.:

- Establish the standards or specifications that put great emphasis on risk analysis.
- Monitor whether the subordinate bodies (Transport Department, Truck & Structure Department, and Rolling Stock Department) adhere to the standards or specifications.

TD, TSD, and RSD: Adhere to the standards or specifications that incorporate risk analysis.

2. The results of risk analysis must be of high quality and cover all risks of the system.

2a. People in charge must have sufficient ability to conduct advanced risk analysis.

Board: Possess adequate skills to conduct risk analysis, especially risk assessment.

Safety Dept.: Provide advanced safety training in risk analysis for engineers who conduct risk analysis, in the subordinate bodies (Transport Department, Truck & Structure Department, and Rolling Stock Department).

TD, TSD, RSD:

- Take safety training in risk analysis seriously.
- Acquire adequate skills to conduct risk analysis.

2b. The entire workforce, including the executives and operators, must contribute to improving the quality of risk analysis.

Board:

- Participate actively in risk analysis, especially risk assessment.
- Determine rational acceptable risk, and make it known to everybody involved.

Safety Dept.:

- Enforce the entire workforce's active participation in risk analysis.
- Monitor whether the entire workforce contributes to improving the quality of risk analysis.

TD, TSD, RSD:

- Have executives involved in risk assessment.
- Have engineers at the work site (Signal Station, Manufacturing Company, and Driver's Office) involved in hazard analysis, paying serious attention to feedback from them.

SS, MC, DO: Provide accurate information about the current status of the system for conducting risk analysis.

3. Risk analysis must be carried out in a timely manner when necessary.

3a. Considerable efforts must be devoted to risk analysis during the early design and development stages of the system.

Safety Dept.:

- Enforce risk analysis at the early stages of the project.
- Monitor whether risk analysis is being conducted at the early stages of the project by the subordinate bodies (Transport Department, Truck & Structure Department, and Rolling Stock Department).

TD, TSD, RSD: Initiate risk analysis from the beginning of the system development.

3b. The results of risk analysis must be updated when there is a modification of the system, or when the environment surrounding the system changes.

Safety Dept.:

- Enforce an update of risk analysis when necessary.
- Monitor whether the results of risk analysis are updated when necessary by the subordinate bodies (Transport Department, Truck & Structure Department, and Rolling Stock Department).

TD, TSD, RSD:

- Keep the results of risk analysis, as well as the process for attaining the results, accessible to other people in later years.
- Update risk analysis when there is a modification of the system.
- Continually review safety conditions, and update risk analysis when there is a change in the environment surrounding the system.

SS, MC, DO: Provide accurate information about the current status of the system to higher organizational levels to give them opportunities to examine if an update is necessary.

Step 4: Detailed hazard analysis (STPA)

Item	Responsibility	Inadequate Control (Risk)	Organizational Requirements
Ministry			
1	Effectively inform railway companies of the accidents that have happened all over the world to set the stage for them to think about the risk.	Fails to assemble information on the accidents.	→ Need for adequate communication.
2		Fails to inform railway companies of the accidents effectively.	→ Need for adequate communication.
3	Require railway companies to report to the ministry the safety program standards or specifications that stipulate the system development process, and approve them.	Approves inadequate standards (specifications).	
Board of Directors			
4	Provide funding and authority to Safety Department to enforce risk analysis across the company.	Does not provide funding or leadership and power to Safety Department to enforce risk analysis.	
5	Monitor whether the safety program is adequately managed by Safety Department.	Makes no attempt to monitor Safety Department.	
6		Fails to monitor Safety Department because adequate channels are not available.	→ Need for adequate communication.
7	Approve the safety program standards or specifications into which the process of risk analysis is explicitly incorporated.	Approves inadequate standards (specifications).	
8	Possess adequate skills to conduct risk analysis, especially risk assessment.	Does not have skills to conduct risk analysis.	
9	Participate actively in risk analysis, especially risk assessment.	Makes no attempt to participate in risk analysis actively.	
10	Determine rational acceptable risk, and make it known to everybody involved.	Specifies irrational criteria of acceptable risk.	
11		Fails to spread the criteria of acceptable risk across the company.	→ Need for adequate communication.
Transport Safety Department			
12	Analyze the accidents that have happened all over the world to realize the importance of risk analysis as well as to recognize new risks in the system.	Does not consider the accident reports seriously.	
13		Analyzes the accidents inadequately because of poor knowledge and skills in analyzing the accidents.	→ Need for safety training.

14	Effectively inform other organization components of the results of the analysis of the accidents.	Does not inform other organizations of the analysis results effectively because no channels to inform are available.	→ Need for adequate communication.
15	Reflect findings from accident analyses in technical specifications.	Does not reflect findings in technical specifications.	
16		Inadequately reflects findings in technical specifications.	
17	Establish the safety program standards or specifications that put great emphasis on risk analysis.	Incorporates risk analysis in the standards (specifications) inadequately.	
18	Monitor whether the subordinate bodies (TD, TSD, and RSD) adhere to the standards or specifications.	Makes no attempt to monitor the subordinate bodies.	
19		Fails to monitor the subordinate bodies because adequate channels are not available.	→ Need for adequate communication.
20	Provide advanced safety training in risk analysis for engineers who conduct risk analysis, in the subordinate bodies (TD, TSD, and RSD).	Does not provide safety training for engineers.	→ Need for safety training.
21		Provides poor quality safety training in risk analysis.	→ Need for safety training.
22	Enforce the entire workforce's active participation in risk analysis.	Fails to enforce the entire workforce's active participation because no means of enforcement are available.	
23	Monitor whether the entire workforce contributes to improving the quality of risk analysis.	Makes no attempt to monitor the entire workforce.	
24		Fails to monitor the subordinate bodies because adequate channels are not available.	→ Need for adequate communication.
25	Enforce risk analysis at the early stages of the project.	Fails to enforce risk analysis at the early stages because no means of enforcement are available.	
26	Monitor whether risk analysis is being conducted at the early stages of the project by the subordinate	Makes no attempt to monitor the risk analysis at the early stages.	

27	bodies (TD, TSD, and RSD).	Fails to monitor the subordinate bodies because adequate channels are not available.	→ Need for adequate communication.
28	Enforce an update of risk analysis when necessary.	Fails to enforce risk analysis at the early stages because no means of enforcement are available.	
29	Monitor whether the results of risk analysis are updated when necessary by the subordinate bodies (TD, TSD, and RSD).	Makes no attempt to monitor the results of risk analysis.	
30		Fails to monitor the subordinate bodies because adequate channels are not available.	→ Need for adequate communication.
Transport Department **Truck & Structure Department** **Rolling Stocks Department**			
31	Adhere to the standards or specifications that incorporate risk analysis.	Does not have knowledge of the standards (specifications).	
32		Does not consider the standards (specifications) carefully.	
33	Take safety training in risk analysis seriously.	Does not take safety training seriously.	
34	Acquire adequate skills to conduct risk analysis.	Does not have adequate skills to conduct risk analysis.	→ Need for safety training.
35	Have executives involved in risk assessment.	Makes no attempt to have executives involved in risk analysis.	
36	Have engineers at the work site (SS, MC, and DO) involved in hazard analysis, paying serious attention to feedback from them.	Makes no attempt to have engineers at the work site involved in risk analysis.	
37		Does not consider feedback from engineers at the work site carefully.	
38	Initiate risk analysis from the beginning of the system development.	Delays the start of risk analysis.	
39	Keep the results of risk analysis, as well as the process for attaining the results, accessible to other people in later years.	Does not document the results and process of risk analysis for access in later years.	→ Need for configuration management.
40		Does not accessibly retain the documents about risk analysis.	→ Need for configuration management.
41		The documents about risk analysis are hard for engineers in later years to understand.	→ Need for configuration management.
42	Update risk analysis when there is a modification of the system.	Makes no attempt to update risk analysis when there is a modification.	

43		Cannot adequately update risk analysis because the safety policy has greatly changed.	→ Need for consistent approaches.
44	Continually review safety conditions, and update risk analysis when there is a change in the environment surrounding the system.	Makes no attempt to review safety conditions.	
45		Does not recognize a change in the environment surrounding the system because adequate channels are not available.	→ Need for adequate communication.
46		Makes no attempt to update risk analysis when a change in the environment is recognized.	
47		Cannot adequately update risk analysis because the safety policy has greatly changed.	→ Need for consistent approaches.
Signal Station **Manufacturing Company** **Driver's Office**			
48	Provide accurate information about the current status of the system for conducting risk analysis.	Fails to acquire necessary information.	
49		Fails to report the current status to the higher organizations (TD, TSD, RSD) because adequate channels are not available.	→ Need for adequate communication.
50	Provide accurate information about the current status of the system to higher organizational levels to give them opportunities to examine if an update is necessary.	Does not feel a personal obligation to provide information.	
51		Fails to acquire necessary information.	
52		Fails to report the current status to the higher organizations (TD, TSD, RSD) because adequate channels are not available.	→ Need for adequate communication.

Step 6: System Dynamics modeling and analysis (Partial)

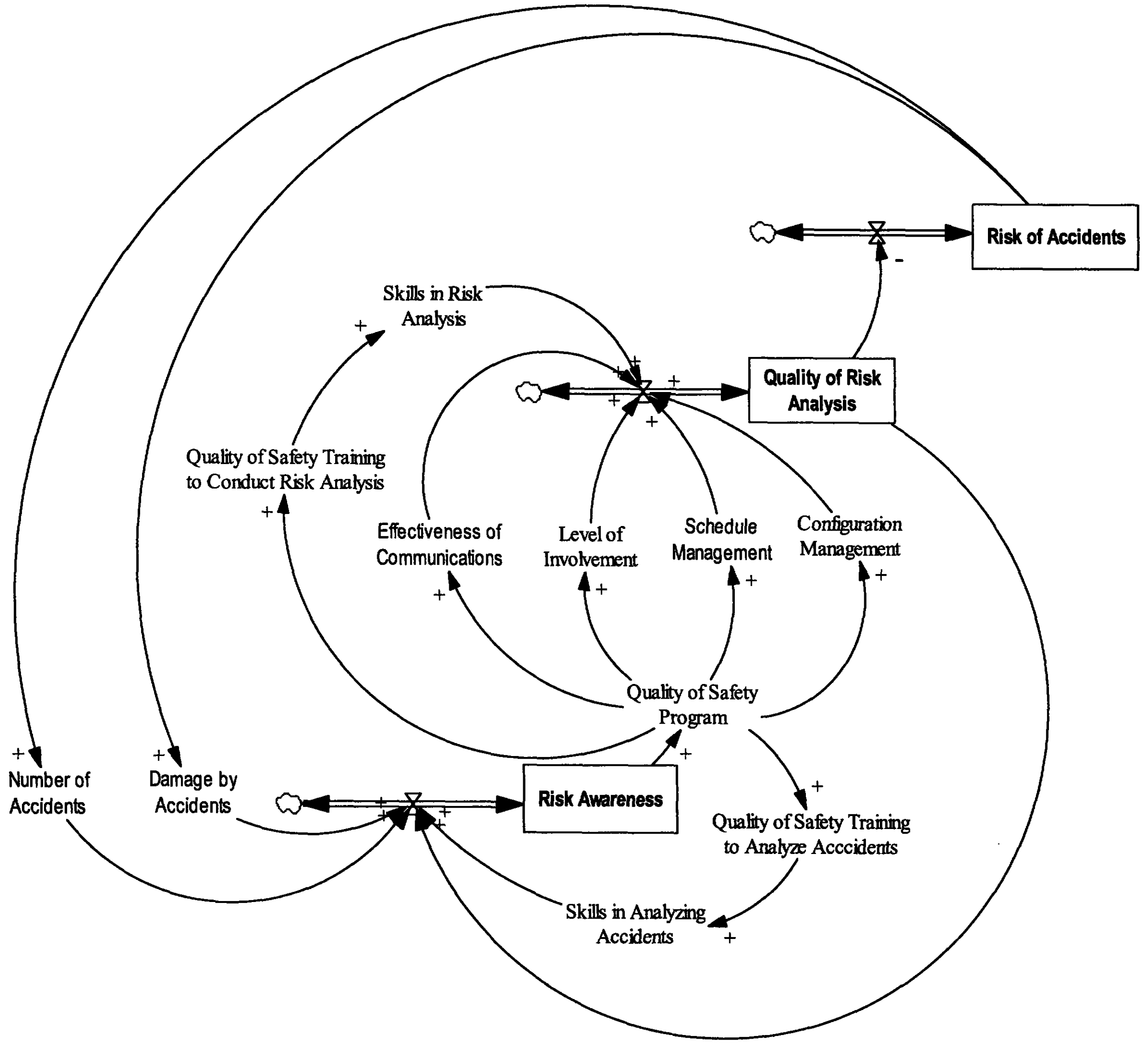

Risk of Accidents
Skills in Risk Analysis
Quality of Risk Analysis
Quality of Safety Training to Conduct Risk Analysis
Effectiveness of Communications
Level of Involvement
Schedule Management
Configuration Management
Quality of Safety Program
Number of Accidents
Damage by Accidents
Risk Awareness
Quality of Safety Training to Analyze Acccidents
Skills in Analyzing Accidents

Figure 6.4: Simplified System Dynamics model about quality of risk analysis. (It is important to note that more complicated model is required to conduct simulation. This model does not provide any new information, but serves as a short summary of Step 4.)

6.2.2 Requirements and recommendations from risk analysis

Through assigning the safety constraints and requirements to each of the control structure components, the STAMP risk analysis revealed various kinds of inadequate control actions (risks), which lead to the requirements for high-speed maglev system organizations. Among them, four organizational requirements, which will be described below, are considered to be relatively unique to high-speed maglev systems, and particularly significant in order to avoid poor hazard analysis in high-speed maglev systems.

(a) Advanced safety training must be systematically provided for both engineers who conduct risk analysis and those who analyze accidents.

Several inadequate control actions identified in Step 4 indicate the need for advanced safety training. First of all, a possible problem is that engineers in the Transport, Truck & Structure, and Rolling Stocks Departments do not have adequate skills to conduct risk analysis. Another problem is that engineers in the Transport Safety Department cannot adequately analyze accidents that have happened all over the world because of their poor knowledge and skills, yet analyzing accidents could help them realize the importance of risk analysis as well as a new risk in the system. These considerations lead to the organizational requirement that advanced safety training must be systematically provided for both engineers who conduct risk analysis and those who analyze accidents.

Engineers' knowledge and skills in risk analysis and accident investigation, both of which fall into the category of System Safety, have been considered to be practical problems. For example, Clifton Ericson, the former president of the U.S. System Safety Society, states the difficulties of hazard analysis, in his reference book about hazard analysis techniques (Ericson, 2005), as follows:

> First, there has never been a formal description of hazard theory that defines the components of a hazard and the hazard-mishap actuation process. Second, there is a lack of good reference material or methodologies.

Nancy Leveson, who has significantly contributed to Software System Safety, has been offering a class in System Safety for graduate students at MIT. Leveson (e-mail, January 11, 2007) introduced the class to target students as follows:

> Because it [System Safety Engineering] was not developed in academia, there are few classes in universities and most engineers have to learn it on the job (often not doing so well, with resulting disasters).

The two statements above demonstrate the increasing need for training as well as the difficulties of training. The company must develop and maintain advanced safety training in conducting risk analysis and analyzing accidents. This finding is one of the most significant organizational requirements.

(b) The safety program in high-speed maglev system organizations must be consistent over a significant span of time.

The safety program in high-speed maglev system organizations must be consistent over a longer span of time. This is another organizational requirement ascertained in this risk analysis. As discussed in Chapter 4, the railway systems are prone to asynchronous evolution, which could be one of the factors that cause an accident. This vulnerability is mainly attributable to the railway system's characteristic feature of being semi-permanently in operation once operation begins. Therefore, there is necessarily a modification of the system at some time in the future and the environment surrounding the system also necessarily changes, which requires an update of risk analysis.

A potential problem here is that the Safety Department frequently changes the safety policy and that the results of the analysis in the past cannot be utilized to meet the requirements of the current safety policy. For example, suppose that the safety program has changed and begins to put great emphasis on quantitative analysis, which had not been considered to be important. In this case, engineers have to work on quantitative analysis, such as Fault Tree Analysis (FTA) and Failure Mode Effect Analysis (FMEA), from scratch. This change will require considerable efforts and result in a decrease in the quality of risk analysis. The important requirement is that the safety program is consistent over a long period of time so that engineers can utilize the past achievements.

(c) An adequate and effective configuration management of risk analysis must be established and implemented to update the system at some time in the future.

The feature of being semi-permanently in operation leads to another requirement: that the result and process of risk analysis must be accessible to the company in later years when an update of the system is required. Since the system is necessarily updated in the future, the risk analysis should be also updated. Keeping not only the result but also the process of risk analysis available for an update is very important.

This requirement is neither unique nor new. For example, the international railway standard IEC 62278: *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)* defines configuration management as follows:

- **configuration management**: discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control change to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements.

Based on this definition, IEC 62278 demands that an adequate and effective configuration management be developed. This is also true in high-speed maglev systems: An adequate and effective configuration management of risk analysis must be established and implemented to make it possible to update the system at some time in the future.

(d) Adequate communications between each of the control structure components must be established.

Finally, several inadequate control actions identified in Step 4 demonstrate the need for adequate communications between each component. In many cases, a possible problem is that a superior component fails to adequately monitor a subordinate component because of poor communication. The importance of communication (feedback) has been widely recognized, and it is where a STAMP analysis pays closer attention. Communication is still an important factor to avoid poor risk analysis in high-speed maglev systems: Adequate communications between each of the control structure components must be established.

Chapter 7

Conclusion

This thesis concludes that it is a System Safety approach that is necessary to assure safety in high-speed maglev systems, rather than a reliability engineering approach, which the international railway standard IEC 62278: *Railway applications – Specifications and demonstration of reliability, availability, maintainability and safety (RAMS)* adopts. This conclusion is derived by examining characteristic features of high-speed maglev systems and analyzing the Fukuchiyama Line derailment accident in Japan in 2005.

7.1 Summary

Magnetic levitation is a railway technology that enables vehicles to be magnetically suspended above their tracks, and maglev (magnetically levitated) systems have great potential to introduce significant changes in today's transportation networks. One of the significant characteristics of the maglev system is its speed. The absence of contact between the vehicles and ground allows the vehicles to run at an extremely high speed, about 500 kilometers per hour in the case of Japanese maglev systems. This high-speed operation, however, makes the system more potentially vulnerable because of reduced acceptable response time and of an increase in inertia force. Besides this feature, in this way, levitation technology, structural fragility, software intensiveness, and mass transportation, which are essential factors in high-speed maglev systems, leave the system more vulnerable: The likelihood and potential severity of accidents in maglev systems are higher than those in conventional railway systems. These arguments demonstrate the need for closer attention to be paid to safety in high-speed maglev systems.

The Fukuchiyama Line derailment accident, which occurred in April 2005, in Japan and killed 106 passengers and the driver, provides valuable lessons for assuring safety in high-speed maglev systems. Among them, two lessons are worthy of considering here. First, the Fukuchiyama Line derailment accident was not a component failure, but a system accident that arose from the inadequate interactions among components. This accident demonstrates that it is system accidents to which closer attention should be paid, in order to minimize risk in today's railway systems, because the reliability of every component is considerably improved. It is important to note that the reliability engineering approach, which is failure oriented, could not have contributed to preventing this accident. The inconsistency is that the underlying concept of IEC 62278 is the reliability engineering approach, as the standard puts great emphasis on safety integrity, which correlates to the probability of failure.

The other lesson is that risk/hazard analysis is the key to assuring safety in today's railway systems. In the Fukuchiyama Line derailment accident, the entire company did not recognize the risk of overturning because of a poor risk/hazard analysis. The flawed mental models of the top management, the department in charge of safety analysis, and the drivers prevented them from identifying the risk of driving at a speed of 120 kilometers per hour. If the company had recognized the risk of overturning, the accident could have been prevented. This accident demonstrates the importance of appropriate risk/hazard analyses that can make an entire company recognize a risk.

While there are a number of hazard analysis techniques available, selecting appropriate hazard analysis techniques has significant importance. In these circumstances, the requirements of hazard analysis and risk assessment for high-speed maglev systems are derived as follows: (1) must emphasize qualitative analyses, rather than quantitative analyses; (2) must adopt a deductive (top-down) approach; (3) must be able to identify the future hazards that result from asynchronous evolution; (4) must be able to consider human errors closely; and (5) must pay closer attention to the severity, rather than the probability, of accidents.

Based on these arguments, this thesis proposes the System Safety approach to assure safety in high-speed maglev systems. System Safety is an organized and established method to assure safety in complex systems, comparable to other approaches to safety, such as industrial safety and reliability engineering. General principles of System Safety are: (1) The goal of System Safety is to prevent accidents before they occur for the first time, utilizing analysis; (2) System Safety deals with systems, rather than components; (3) Safety must be built into the system, rather than added to the system, by timely analysis throughout all phases of the system life cycle; and (4) The key to System Safety is hazard analysis, which identifies, eliminates, mitigates, and controls hazards in the system. Similarities between the lessons learned from the Fukuchiyama Line derailment accident and the general principle of System Safety lead to the need for System Safety.

Finally, this thesis identifies the organizational requirements to avoid poor risk/ hazard analysis. Among them, four organizational requirements are considered to be relatively unique to high-speed maglev systems, and particularly significant: (1) Advanced safety training must be systematically provided for both engineers who conduct risk analysis and those who analyze accidents; (2) The safety program in high-speed maglev system organizations must be consistent over a significant span of time; (3) An adequate and effective configuration management of risk analysis must be established and implemented to update the system at some time in the future; and (4) Adequate communications between each of the control structure components must be established.

7.2 Future work

This thesis proposes an approach to assure safety in high-speed maglev systems. Also derived are the requirements of risk/hazard analysis, which is the key to assuring safety, and the organizational requirements to avoid poor risk/hazard analysis. The next step is to apply these requirements to actual system development of high-speed maglev systems.

Although these requirements are based on the findings by examining characteristic features of high-speed maglev systems and by analyzing the Fukuchiyama Line derailment accident, applying them to the actual system may reveal some difficulties. It is important to determine whether the requirements identified in this thesis are appropriate through a real project.

One thing that this thesis does not count on is the existence of various subsystems in high-speed maglev systems, which consist of vehicles, signal systems, electrical power systems, track systems, and so on. Although this thesis regards high-speed maglev systems as one system and does not consider differences among these systems, there exist differences. Taking differences between subsystems into account is also one of the next steps.

Maglev technology is in use in several places; however, it should be considered still under development. Further research and development are required in order to realize this next generation transport system. The author hopes this thesis contributes to system development of safer high-speed maglev systems.

References

Air Force Safety Agency. (2000). *Air Force system safety handbook: Designing the safest possible systems consistent with mission requirements and cost effectiveness.* Retrieved March 14, 2008, from http://handle.dtic.mil/100.2/ADA437098

Aircraft and Railway Accidents Investigation Commission. (2007, June). *Tetsudo jiko chosa hokokusho: Nishi nihon ryokaku tetsudo kabushiki kaisha fukuchiyamasen tsukaguchi eki - amagasaki eki ressha dassen jiko [Railway accident analysis report: West Japan Railway Company Fukuchiyama Line derailment accident].* Retrieved June 28, 2007, from http://araic.assistmicro.co.jp/railway/bunkatsu.html

Braband, J., & Brehmke, B. (2002). Application of why-because graphs to railway near-misses. *Proceedings of the first workshop on the investigation and reporting of incidents and accidents (IRIA)*, Glasgow, Scotland.

Braband, J., Evers, B., & Stefano, E. (2003). Towards a hybrid approach for incident root cause analysis. *Proceedings of the 21st international system safety conference*, Unionville, Virginia, System Safety Society.

Braband, J., Hirao, Y., & Luedeke, J. (2004). The relationship between the CENELEC railway signalling standards and other safety standards. *Signal und draft, 95.*

Braband, J. (2004). The importance of a safety culture in railway signalling. *Signal und draht, 96.*

Central Japan Railway Company [JRC]. (2007a). *Kessan Tanshin [Summary of financial report for the year ended march 31, 2007].* Retrieved January 2, 2008 from http://company.jr-central.co.jp/ir/brief-announcement/2007/_pdf/brief2007-07.pdf

Central Japan Railway Company [JRC]. (2007b). *Annual Report 2007.* Retrieved January 2, 2008 from http://jr-central.co.jp/eng.nsf/english/report/$FILE/Annual_Report_2007.pdf.

Central Japan Railway Company [JRC]. (2007c). *News letter: Central Japan Railway Company decides to promote the Tokaidho Shinkansen bypass (also known as Chuo Shinkansen) on the premise that the company would bear the cost for the project.* Retrieved January 2, 2008 from http://jr-central.co.jp/eng.nsf/english/report/FILE/P0120Bypass.pdf

Defense Acquisition University. (2002). *AT&L knowledge sharing system.* Retrieved January 17, 2008, from http://akss.dau.mil

Department of Defense. (1984). *MIL-STD-882B: System safety program requirements.* Author.

Department of Defense. (1993). *MIL-STD-882C: System safety program requirements.* Author.

Department of Defense. (2000). *MIL-STD-882D: Standard practice for system safety.* Author.

Dulac, N., Owens, B., & Leveson, N. (2007). *Demonstration of a new dynamic approach to risk analysis for NASA's constellation program.* Retrieved May 2, 2008, from http://sunnyday.mit.edu/ESMD-Final-Report.pdf

Edward, E. (1988). Introductory overview. In: Wiener, E. L., and Nagel, D. C. (Eds), *Human factors in aviation.* San Diego: Academic Place.

Ericson, C. A. (2005). *Hazard analysis techniques for system safety.* Hoboken, New Jersey: John Wiley & Sons.

Fielding, R. A. P., (2007). Aluminum in transportation systems: The resurgence of rail. *Light metal age, 65*(5).

Herrmann, D. S., (1999). *Software safety and reliability: techniques, approaches, and standards of key industrial sectors.* California, IEEE computer society.

Hirakawa, K. (2006). *Doitsu kosoku tetsudo dassen jiko no shinso [Truth of german high-speed railway derailment accident].* Tokyo, Japan: Keibunsha.

International Electromechanical Commission. (1998). *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.* Geneva, Switzerland: Author.

International Electrotechnical Commission. (2002). *IEC 62278: Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS).* Geneva, Switzerland: Author.

International Electrotechnical Commission (2002). *IEC 62279: Railway applications – Communications, signaling and processing systems – Software for railway control and protection systems.* Geneva, Switzerland: Author.

Joint Software System Safety Committee. (1999). *Software system safety handbook: A technical & managerial team approach.* U.S. Department of defense.

Kubota, H. (2000). *Tetsudo judai jiko no rekishi [History of serious railway accidents].* Tokyo, Japan: Grand-prix publishing.

Laracy, J. (2007). *A systems-theoretic security model for large scale, complex systems applied to the US air transportation system.* Cambridge, Massachusetts: Massachusetts Institute of Technology master's thesis.

Leplat, J. (1987). Occupational accident research and systems approach. In: Rasumussen, J., Duncan, K., and Leplat, J. (Eds), *New technology and human error*. New York: John Wiley & Sons.

Leveson, N. G. (1995). *Safeware: System safety and computers*. Boston: Addison-Wesley.

Leveson, N. G. (2002, June). *System safety engineering: Back to the future*. Retrieved January 17, 2007, from http://sunnyday.mit.edu/book2.pdf

Leveson, N. G., & Cutcher-Gershenfeld, J. (2004, August). What system safety engineering can learn from the Columbia accident, *International conference of the system safety society*, Providence Rhode Island.

Leveson, N. G., & Dulac, N. (2005). *Risk analysis of NASA independent technical authority*. Retrieved February 14, 2008, from http://sunnyday.mit.edu/ITA-Risk-Analysis.doc

Marais, K., Dulac, N., & Leveson, N. (2004). Beyond normal accidents and high reliability organizations: The need for an alternative approach to safety in complex systems. *MIT Engineering systems division symposium*. Cambridge, Massachusetts.

Miller, C. O. (1988). System safety. In: Wiener, E. L., and Nagel, D. C. (Eds), *Human factors in aviation*. San Diego: Academic Place.

Ministry of Land, Infrastructure and Transport. (2006). *Ministry of Land, Infrastructure and Transport: Government of Japan*. Retrieved November 15, 2007, from http://www.mlit.go.jp/english/2006/2006_pamphlet/01.pdf

Mizoguchi, M., & Sato, Y. (Eds.). (2006). *Jissen tetsudo RAMS [Railway RAMS]*. Tokyo, Japan: Seizando Shoten.

Perrow, C. (1999). *Normal accident: Living with high-risk technologies* (2^{nd} ed.). New Jersey: Princeton University Press.

Perrow, C. (2007). *The next catastrophe: Reducing our vulnerabilities to natural, industrial, and terrorist disasters*. New Jersey: Princeton University Press.

Powell, J. R. & Danby, G. R. (1966). *High speed transport by magnetically suspended trains*. ASME, Publ no. 66WA/RR5.

Polmar, N. (2004). *The death of the USS Thresher: The story behind history's deadliest submarine disaster*. Guilford, Connecticut: Lyons Press.

Railway technical research institute [RTRI]. (2006). *Kokomade kita chodendo rinia motaka [Current status of superconducting maglev]*. Tokyo, Japan: Kotsushimbunsha.

Reason, J. (1990). *Human error*. New York: Cambridge University Press.

Sakai, Y. (2007). The current state and future of aluminum alloy applications for railway rolling stock. *Light metal age, 65*(5).

Sanders, M. S., & McCormick, E. J. (1993). *Human factors in engineering and design*. New York: McGraw-Hill.

Sato, Y (2002, December). Activities of japan's aircraft and railway accidents investigation commission. *Japan Railway & Transport Review, 33.*

Sawilla, A., & Otto, Wolfgang. (2006). Safety assessment for the maglev operation control and overall system: Experience gained and lessons learned. *Proceedings of the 19th international conference on magnetically levitated systems and linear drives.* Dresden, Germany.

Siemens. (2002). *The multiple-unit train for the European high-speed network: ICE3 for German rail and netherlands railways*. Retrieved February 14, 2008, from http://references.transportation.siemens.com/refdb/link_download.jsp?file_name=ice3_en_A19100-V800-B248-V2-X-7600856.pdf&l=en

Skllingberg, M., & Green, J. (2007). Aluminum applications in the rail industry. *Light metal age, 65*(5).

Steiner, F., & Sterinert, W. (2006). Safety assessment for the maglev vehicle TR09 – an approach based on CENELEC railway standards. *Proceedings of the 19th international conference on magnetically levitated systems and linear drives.* Dresden, Germany.

Steinert, W. & Keller, U. (2004). Safety evaluation and assessment of materials and assembly technologies for vehicle TR08. *Proceedings of the 18th international conference on magnetically levitated systems and linear drives*. Shanghai, China.

Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world.* Boston: Irwin McGraw-Hill.

System safety society. (1993). *System safety analysis handbook.* Albuquerque, NM: Author.

Tao, W. (2004). Safety assessment & approval system of shanghai maglev demonstration line and its practice. *Proceedings of the 18th international conference on magnetically levitated systems and linear drives*. Shanghai, China.

Transrapid International. (2004). *The future is already here: The Transrapid maglev system in Shanghai.* Retrieved February 14, 2008, from http://www.transrapid.de/pdf/TRI_shg_10_04_E.pdf

Transrapid International. (2006). *High-tech for flying on the ground.* Retrieved February 14, 2008, from http://www.transrapid.de/pdf/tri_engl.pdf

Transrapid International. (2007). *Taking off for the future: The maglev system in Munich.* Retrieved February 14, 2008, from http://www.transrapid.de/pdf/TRI_mue_E_0307.pdf

Tufte, E. R., (1997). *Visual explanations: Images and quantities, evidence and narrative.* Cheshire, Connecticut: Graphics Press.

Tum, M., Huhn, G., & Harbeke, C. (2006). Design and development of the transrapid Tr09. *Proceedings of the 19th international conference on magnetically levitated sytesms and linear drives*. Dresden, Germany.

Yamaguchi, E. (2007). *JR Fukuchiyamasen jiko no honshitsu: Kigyo no shakaiteki sekinin wo kagaku kara toraeru [Root for the JR Fukuchiyama train incident: Rethinking corporate social responsibility from science]*. Japan: NTT publishing.

Yamanouchi, S. (2005). *Naze okoru tetsudo jiko [Why do railway accidents happen?]*. Tokyo, Japan: Asahi Bunko.

West Japan Railway Company. (2006). *Annual report 2006.* Retrieved April 19, 2007, from http://www.westjr.co.jp/english/english/company/con02/ar/2006/index.html

Wiegmann, D. A., & Shappell, S. A. (2003). *A human error approach to aviation accident analysis: The human factors analysis and classification system*, Vermont: Ashgate Publishing Company.

Wolfgang, O. (2004). System safety verification of the shanghai maglev line. *Proceedings of the 18th international conference on magnetically levitated systems and linear drives*. Shanghai, China.