APPLICATION OF CAST AND STPA TO RAILROAD SAFETY IN CHINA

by

Airong Dong

Bachelor in Engineering, Communications and Information System,
Dalian Maritime University (1997)

Master in Engineering, Communications and Information System,
Dalian Maritime University (2000)

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

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

May 2012

Signature of Author _____

Airong Dong

System Design and Management Program

May 2012

Certified by _____

Nancy Leveson

Thesis Supervisor

Professor of Aeronautics and Astronautics and Engineering Systems

Accepted by _____

Patrick Hale

Director

System Design & Management Program

Acknowledgements

I would like to thank Professor Nancy Leveson, my thesis advisor, who showed me a new way to look at system safety, which has greatly changed my view. It's this awakening learning that made me decide to apply my learning to the China railway industry to help improve system safety there. I also want to thank her for providing me the great opportunity of being in her research group and for me to learn so much about the safety world. In the mean time, I would like to thank Mr. Andrei Katz, who is visiting our research group during this time, who helped me a lot in improving my thesis.

I would like to thank Professor Tang Tao from Beijing Jiaotong University, who shared his valuable insights towards the accident analysis with me.

I would like to thank Pat Hale, Director of System Design and Management Program, for sharing my thoughts, providing me directions and exploring with me the opportunities lying ahead of me.

I would like to thank Qi Hommes, Research Associate of Engineering System Division, for helping me continuously improve during my study here.

Finally, I would like to give thanks to my family for their great support for my study here. It's they who supported me to make the decision and eventually made my long-held dream come true.

Abstract

The accident analysis method called STAMP (System-Theoretic Accident Model), developed by Prof. Nancy Leveson from MIT, was used here to re-analyze a High Speed Train accident in China. On July 23rd, 2011, 40 people were killed and 120 injured on the Yong-Wen High Speed Line. The purpose of this new analysis was to apply the broader view suggested by STAMP, considering the whole socio-technological system and not only equipment failures and operators mistakes, in order to come up with new findings, conclusions and recommendations for the High Speed Train System in China.

The STAMP analysis revealed that the existing safety culture in the whole train organization, the Ministry of Railway and all its sub organizations in both the Train Development and Train Operation channels, do not meet the safety challenges involved in a high risk system like this— running frequent trains on the same line at 250km/h, with hundreds of passenger on board. The safety hazards were not systematically analyzed (not at the top level nor at the design level), safety constraints and safety requirements were very vaguely phrased, and no real enforcement was applied on safe design and implementation nor on safe operation. It looks like no clear policy on the performance/safety dilemma existed, nor the necessary safety education and training.

Following from the STAMP analysis, one of the major recommendations in this thesis is to create a professional Train Safety Authority at the highest level, to be in charge of creating and supervising the rules for both Engineering and Operations, those two being highly interrelated with respect to safety. Specific Control Structures are recommended too, along with some detailed technical recommendations regarding the fail-safe design of the equipment involved in the accident.

Another major recommendation is to design the safety critical systems, like the signaling control system using STPA ((System Theoretic Process Analysis), a hazard analysis technique. In the second part of this thesis, STPA is applied to another signaling system—Communication Based Train Control (CBTC) system—which is similar to the one presented in the first part. The primary goal of STPA is to include the new causal factors identified in STAMP that are not handled by the older techniques. It aims to identify accident scenarios that encompass the entire accident process, including design errors, social, organizational, and management factors contributing to accidents. These are demonstrated in the STPA analysis section.

Thesis Supervisor: Nancy Leveson

Title: Professor of Aeronautics and Astronautics and Engineering Systems

Contents

List of Abbreviations

ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
CAST	Causal Analysis based on STAMP
CBTC	Communication Based Train Control
CRH	China Railway High-speed Train
CRSC	China Railway Signaling and Communication Corporation
CRSCD	Beijing National Railway Research & Design Institute of Signal and Communication
CTC	Centralized Traffic Control
CTCS	Chinese Train Control System
DCS	Data Communication System
DPL	Dedicated Passenger Line
EB	Emergency Brake
EMC	Electro Magnetic Compatibility
ETCS	European Train Control System
MAL	Movement Authority Limit
MOR	Ministry of Railway
OS	On Sight Mode
STAMP	System-Theoretic Accident Model
STPA	System-Theoretic Process Analysis
TC	Train-borne Controller
TCC	Train Control Center
TDCS	Train Dispatching Center System
TO	Train Operator
TSR	Temporary Speed Restriction
WC	Wayside Controller

1. Introduction

High Speed Rail has been developing very fast in China. The Ministry of Railway has made ambitious plans to build the High Speed Railway Network in China. The first Dedicated Passenger Line Jing-Jin Line in August 2008 marks the start of the rapid high speed railway development. According to the original MOR plans, the total length of the high speed railway will be more than 9600 kilometers by the end of this year, and the expected total length of Dedicated Passenger Lines will reach more than 16,000 kilometers in 2020.

The train to train collision accident that happened on July 23, 2011 in one of the high speed lines gave a big hit to the high speed railway development in China. Besides a great surprise, everybody is eager to know what has happened, what went wrong, whose responsibility it is. The accident investigation report published in December 2011 described the events and the software and hardware failures of the train control system equipments, pointed to the management failure in permitting the usage of the equipment without adequate testing, and listed all the people assigned responsibility for the accidents and their punishment.

Parallel with the fast development of China's high speed railway, MOR has always been trying to put safety as their top priority. "Safety is always the No. 1 priority" is all over the publicizing activities. Fail-safe design cannot be emphasized enough. Then why did this accident still happen with all those MOR safety rules? Why is the system that is supposed to be fail-safe not fail-safe anymore? Why was the accident not prevented by the advanced signaling system? How can we prevent this from happening again in the future? How can we have real confidence in the safety of our system?

All these questions require a fresh eye to look into, a new insight to answer. Together with the advanced system design, with the more and more complex socio-technology systems, we need a new model to help us understand the accident, a new technique to help us do a better safety-critical system design.

In systems theory, safety is viewed as an emergent property, it arises from the interactions among system components, rather than individual component failures; accidents are caused by inadequate control of safety constraints, rather than chains of failure events.

Most of the traditional accident analysis technique focuses on identifying root causes. Root causes can be identified, but without an effective safety control program, new accidents arising from other root causes will continue to happen. A new accident model based on systems theory called STAMP (System-Theoretic Accident Model) has been developed by Leveson to analyze accidents through a systems-theoretic view of causality. STAMP changes the emphasis in system safety from preventing failures to enforcing behavioral safety constraints. In STAMP, accidents are seen as resulting from inadequate control. The model used is a functional control diagram rather than a physical component diagram. The STAMP model of accident causation is built on three basic concepts – safety constraints, a hierarchical safety control structure, and process models.

In systems theory, systems are viewed as hierarchical structures, where each level imposes constraints on the activity of the level beneath it. Events leading to losses only occur because safety constraints were not successfully enforced. [1]

Process models are an important part of control theory. In order to control a process, four conditions are required: Goal condition, Action condition, Model condition and Observability condition. [1]

Accidents can be understood, using STAMP, by identifying the safety constraints that were violated and determining why the controls were inadequate in enforcing them. Accidents result from inadequate enforcement of the behavioral safety constraints on the process, as shown in Figure 1-1. CAST (Causal Analysis based on STAMP) is a framework built to assist in understanding the entire accident process and identifying the most important systemic causal factors involved. [1]

Based on the STAMP model, Leveson also developed a new hazard analysis technique, called STPA (System-Theoretic Process Analysis), which can be used to guide the system design interactively in the design process. It's developed for the more and more complex socio-technical systems used today, in which the traditional techniques are no longer adequate. The primary goal of STPA is to include the new causal factors identified in STAMP that are not handled by the older techniques. More specifically, the hazard analysis technique should include design errors, including software flaws; component interaction accidents; cognitively complex human decision-making errors; and social, organizational, and management factors contributing to accidents. In short, the goal is to identify accident scenarios that encompass the entire accident process, not just the electro-mechanical components. [1].

In the first part of this thesis, the Train to Train Collision Accident that happened in China on July 23rd, 2011 is analyzed using the CAST process, in order to help us understand the accident better and to improve system safety. The purpose of using CAST is not to assign blame, but rather to focus on why the accidents happened and how to prevent future accidents. This accident was chosen due to its great impact in China's high speed railway development and the publication of the accident investigation report. The CAST accident analysis is based on the accident investigation report, which not only described the events, the software and hardware failures and the management failures but also put much emphasis in listing the punishments for the responsible people.

The STAMP accident analysis helps to identify the scenarios, the inadequate controls, the dysfunctional interactions, and the incorrect process models, which can be further utilized in the STPA hazard analysis and design processes.

The second part of this paper takes the safety-guided design approach using STPA analysis and applies it to the Communication Based Train Control system. This system was chosen due to the fact it is an advanced signaling and train control system currently used in the world and because of the availability of its standard (IEEE 1474).

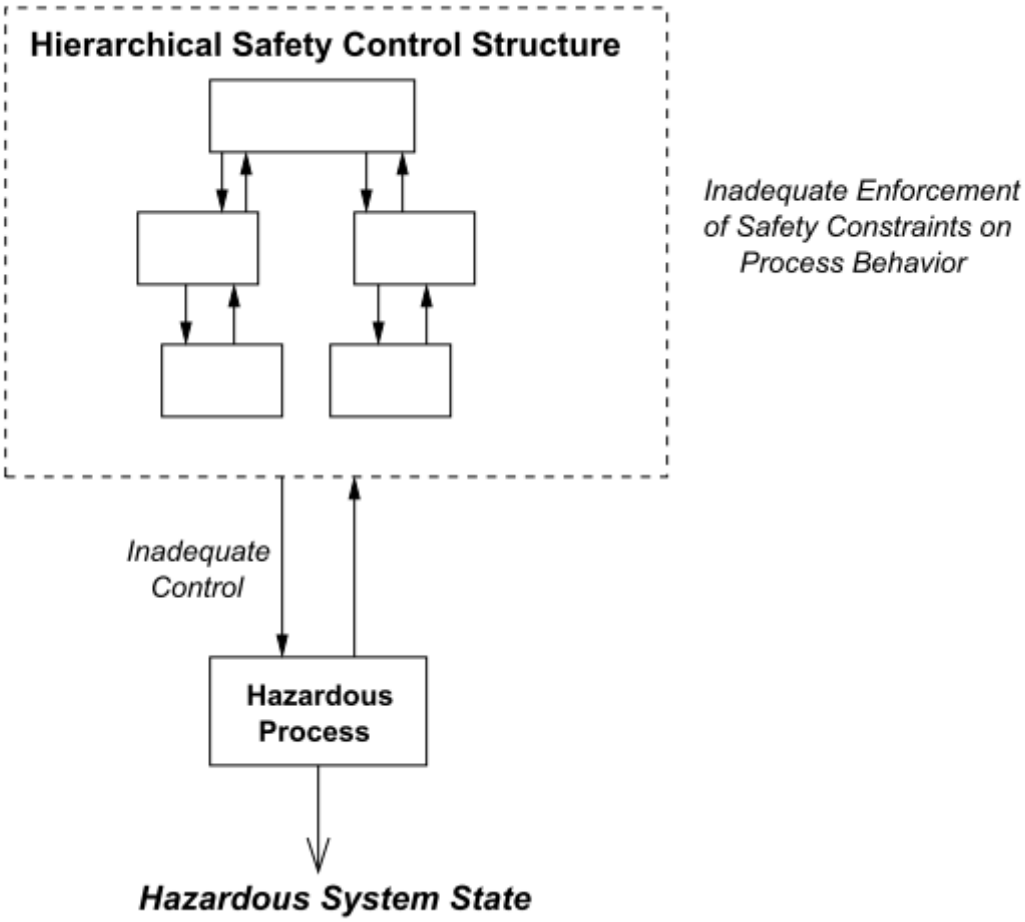


Figure 1-1. Systems-Theoretic Accident Model and Process [1]

2. CAST Analysis of the 7.23 Train to Train Collision Accident

At the time this paper was developed, Dajiang Suo in parallel also analyzed this accident using CAST analysis and presented his analysis, "A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident" at the MIT STAMP/STPA workshop in April 18th.

We both used the CAST model developed by Leveson to analyze the accident, but we did our analysis entirely separately, and the results of our analysis were very different. I have made a comparison between what I have done and the presentation from the workshop [14], in Appendix section of this thesis.

2.1. Background

In order to cope with the increasing demand for railway transportation in China, between 1997 and 2007, there were six railway speed increases in the Chinese railway system. In the first speed increase in 1997, there were high speed trains running at an average speed of 90km/h, with the highest speed of 140km/h. After the sixth big area speed increase in 2007, the CRH trains would be operated on the speed increased mainlines, the passengers train travel speed would reach 200km/h~250km/h. After this speed increase in the existing lines, the China railway development will focus on the building of the dedicated passenger lines, with the target speed of 350km/h.

The traditional signaling system relies mainly on the track circuits sending movement authority commands to wayside signals and train operators operating the train based on the signal display. When the train speed is over 160km/h, it's not practical any more to run trains under this kind of signaling system. There has to be a highly safe and effective system to ensure the safe operation of the trains running in high speeds.

After studying the European Train Control System (ETCS) and other train control systems used worldwide, in 2004, Ministry of Railway (MOR) decided to develop the new train operation system which suits the national conditions, called the Chinese Train Control System (CTCS) system. MOR then issued a temporary provision of "CTCS General Technical Requirement" in 2004, in which it proposed 5 levels (CTCS0 ~ CTCS4) for the system and determined the basic functional requirements for each level.

At the same time, MOR decided to use the CTCS-2 system together with the sixth speed increase in the existing mainline railway system. The CTCS-2 onboard equipment will be installed on the CRH trains, and the mainline railway sections involved in the speed increase will be upgraded with the CTCS-2 wayside control equipment.

CTCS-2 system is composed of onboard control system (including the ATP system), wayside equipment (including track circuits, transponders and signals) and station control equipment (including the Train Control Center and station interlocking computer). Refer to Figure 2-5 for the system control structure.

The CTCS-2 system uses track circuits and transponders to transmit movement authority information to the train. The target distance-speed control method is used to control train movement. The target

distance-speed control algorithm determines the train braking profile, using the target distance, target speed and the train performance. In Figure 2-1, the solid line (monitoring profile) is the target distance-speed profile; the dotted line is the train driving profile. The actual train speed needs to be always under the monitoring line. If it goes over the monitoring profile, the onboard ATP system will automatically trigger the service brake or emergency brake to prevent the train from running over speed.

In order for the onboard ATP to calculate the target distance-speed profile, the track circuits transmit the movement authority limit (MAL) and the number of free blocks (composed of one or more track circuits) ahead of the train to ATP. The transponders send the fixed line data such as block length, line speed and slope to the train AT. Using this information, the onboard ATP calculates real time the target distance and monitoring speed profile.

The Train Control Center (TCC) controls the encoding of track circuits and block signal opening and determines the train movement authority.

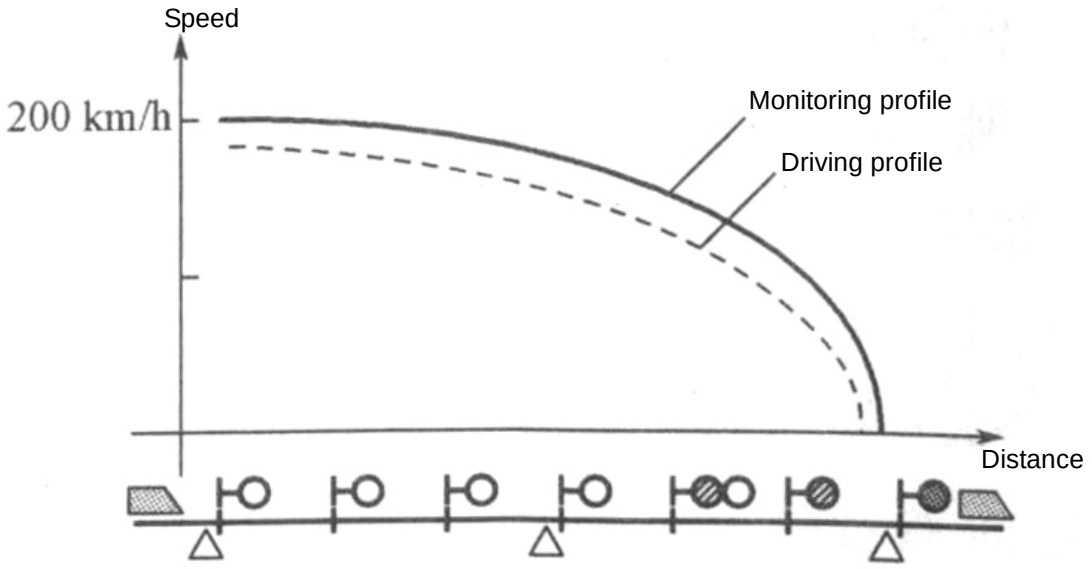


Figure 2-1. Target Distance-Speed Control [16]

At the CTCS-2 level, there are several kinds of train operating modes. When the onboard ATP system has all the information it needs to control the train, it can operate in Full Supervision (FS) mode. When there are fixed ATP data (line parameter, line speed, etc.) missing, the train can be operated in Partial Supervision (PS) mode. When ATP receives certain kinds of forbidden signal or no signal from the track circuit, after the train stops, the train can switch to On Sight (OS) mode. The ATP system can also be isolated and thus the train operates in Isolate mode. There are a couple of other modes as well in shunting and other situations.

Under the CTCS-2 system, for mainlines operating both passenger and freight trains, the train operation interval is designed to be 4 minutes for passenger trains, and 5 minutes for freight trains.

The Yong-Wen line locates in the east coastal area in China, starts from NingBo city from the north, ends at WenZhou city, all inside of ZheJiang province. The length of the line is 282.38 kilometers, and it

is operated by the Shanghai Railway Bureau. This high speed line was built from February 2006 and put into revenue service on September 2009. The CTCS-2 system is used on this line, and the line opening operating speed is 250km/h for CRH trains.

2.2. The Accident

On July 23rd, 2011, at 20:30:05, inside of Wenzhou city, Zhejiang province, on the Yong-Wen High Speed Line, a China Railway High-speed (CRH) train D301, running at a speed of 99km/h, crashed into another CRH train D3115, which was running in the same direction at a speed of 16km/h.

The accident caused the derailment of the last two cars of D3115 and the first five cars of D301. Besides different levels of damages to the multiple unit train vehicles, 40 people died, 120 were injured, the following traffic was stopped for 32 hours and 35 minutes, and the direct economic loss was estimated at 193.7 million Yuan.

About one hour before the accident happened, there were abnormally strong lightening activities along the rail lines from WenZhou South to YongJia station. Lightening hit the ground more than 340 times, and for more than 11 times the lightening strength was over 100 kilo ampere.

The abnormal lightening created several electronic equipment failures, including track circuit 5829AG failure, TCC equipment failure (PIO board), data communication failure between TCC and track circuits, and GSM-R dispatching communication interruptions between the train operator and the CTC dispatcher. As a result, the leading train D3115 was stopped by its onboard ATP system, and it later had problems for 7 minutes in restarting, while the following train D301 was not given any warning either by the automatic control system or the dispatcher. The lack of dispatching communication prevented the D3115 operator from alerting the dispatcher in the CTC center.

The accident investigation report concluded the cause of the accident was the design error of the LKD2-T1 TCC equipment designed by Beijing National Railway Research & Design Institute of Signal and Communication (CRSCD), and the contributing factors were the permission to use this equipment by the Ministry of Railway (MOR) and the weak safety awareness of the Shanghai Railway Bureau:

“Investigation has determined the reason led to the accident: Due to the management confusion of CRSCD in the LDK2-T1 TCC research and development project, and the ineffectiveness in China Railway Signaling and Communication Corp (CRSC)’s integrator role in the Yong-Wen line project, there existed serious design defect and potential safety hazards in the LKD2-T1 equipment provided to the Wenzhou South station. MOR violated related regulations in the bidding, technical review and service operation processes of the TCC equipment, and didn’t provide enough control, which led to the equipment being used in the Wenzhou South Station.

Shanghai Railway Bureau operation personnel had weak safety awareness, were not effective in handling failure, and not able to prevent or mitigate the accident. ” [2]

About one-fourth of the pages of the accident report were dedicated to assigning responsibilities and giving suggestions as to how to punish the responsible people. There were totally 54 people identified responsible for the accident and they were all assigned various punishments.

To fully understand why the accident occurred, we need to understand why the error was introduced into the design process, why the error was not controlled in the operation process, and why the control structure involved in this system was not effective to prevent this accident. The Causality Analysis based on STAMP (CAST) analysis provides us with the framework to examine the entire socio-technology system involved in the accident, to get a complete picture of what went wrong, to understand the most important systematic causal factors, and to identify how to prevent similar losses in the future. The purpose of using CAST is not to assign blame, but rather to focus on why the accidents happened and how to prevent future accidents.

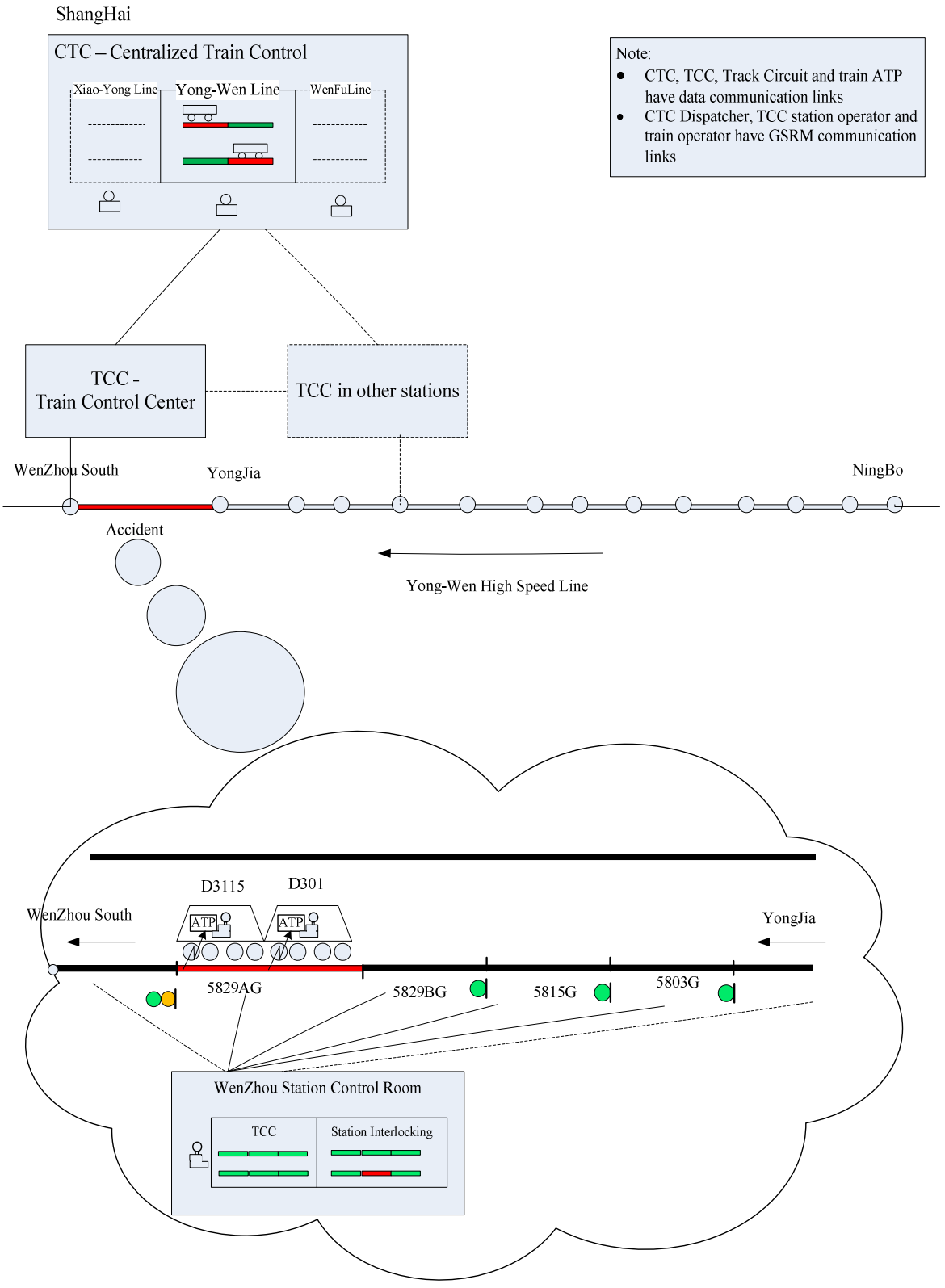


Figure 2-2. The Yong-Wen High Speed Line and the Accident (Reference to [2])

2.3. The System(s) and Hazard(s) Involved in the Loss

The signaling and train control system used on this line is the CTCS-2 system. China Railway Signaling and Communication Corp. (CRSC) is the integrator of the CTCS-2 system on this line. The TCC (LKD2-T1 Type) involved in this accident is located in WenZhou South station, and is designed by Beijing National Railway Research & Design Institute of Signal and Communication (CRSCD), belonging to the CRSC group.

The TCC equipment in Wenzhou South station is manufactured by Shanghai Railway Communication Company (SRCC), which also belongs to the CRSC group.

The Centralized Traffic Control is located in Shanghai Railway Bureau, which belongs to the Ministry of Railway (MOR), and is one of the 18 railway bureaus in China.

The high level hazard involved in this loss is the following train crashes into the leading train.

The following control structures describe the controls and interactions between the systems involved in controlling this hazard and enforcing safety constraints.

2.4. The Hierarchical Safety Control Structure to Prevent the Train to Train Collision Accidents

Figure 2-3 shows the system control structure for the Yong-Wen line project development and operations in China.

Figure 2-4 is the TCC system control structure, which is inside of the operating and physical processes of the overall system control structure.

The following sections will analyze the failures, inadequate controls, dysfunctional interactions and incorrect mental models for each level of the system control structure.

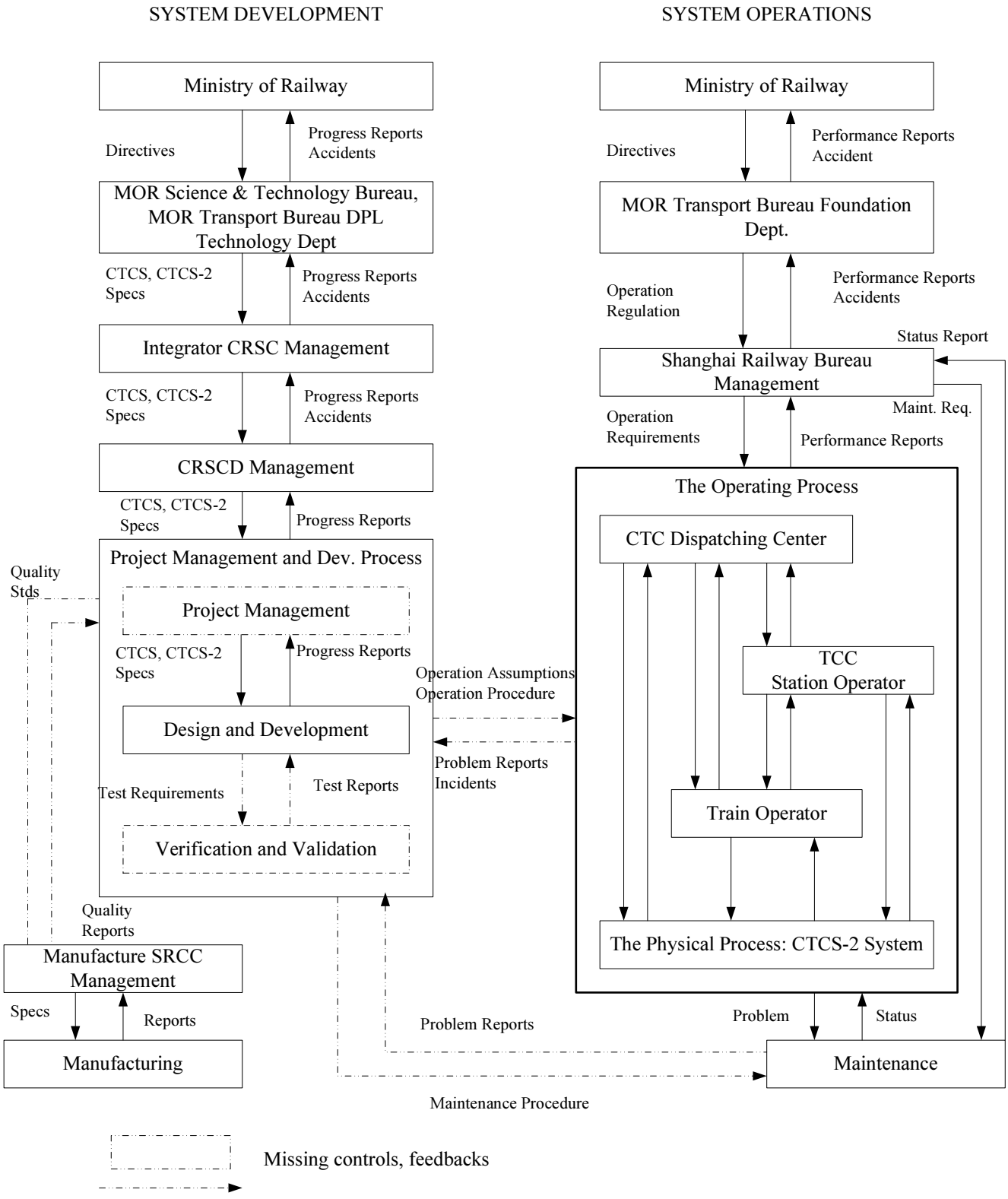


Figure 2-3. The Wenzhou line CTCS-2 Project Development and Operations Control Structure

The WenZhou line project development and operations control structure is also a generalized control structure for China railway projects. But in this project, there is no formal project management and development team and thus no project management, no formal test, and no operational and maintenance procedures for the equipment developed.

Based on information in the accident investigation report, we understand that, inside of the system development process of the control structure, the only technical requirements flows from MOR Science and Technology Bureau to the project development team are the CTCS and CTCS-2 Specifications. There are no further specific safety standards developed for the project, no hazard analysis for project reviews, and no safety constraints for verification and validation.

Even the CTCS and CTCS-2 specifications are still preliminary. The safety requirements are very vaguely developed. The following are all the safety requirements in the CTCS and CTCS-2 specifications:

In the General Technical Specification [15]:

1. Design the system according to fail safe principle;

2. Adopt a redundancy structure;

3. Satisfy the EMC and related standards.

In the CTCS-2 Train Control Center (TCC) Technical Specification [3]:

1. MTBF > = 10^5h;

2. TCC should be designed to SIL(Safety Integrity Level) level 4, the average interval between dangerous output > = 10^9 h;

3. RAMS requirements should satisfy requirements in IEC62278:2002, IEC62279:2002 (EN-50128:2001), IEC62280:2002 (EN-50129:2003). [17][18][19]

4. Safety information and transmission, coding should use redundant checking, the probability of dangerous output should be < = 10^{-10}.

5. Safety related circuit design in TCC must satisfy the fail-safe principle.

For a safety critical system like the high speed train signaling control system, these safety requirements are just too weak to achieve an effective safety control. Following the STAMP analysis, we will understand the need to establish safety constraints for each level of the control structure, Using the STPA analysis in the second part the thesis, we can learn how to develop effective safety requirements.

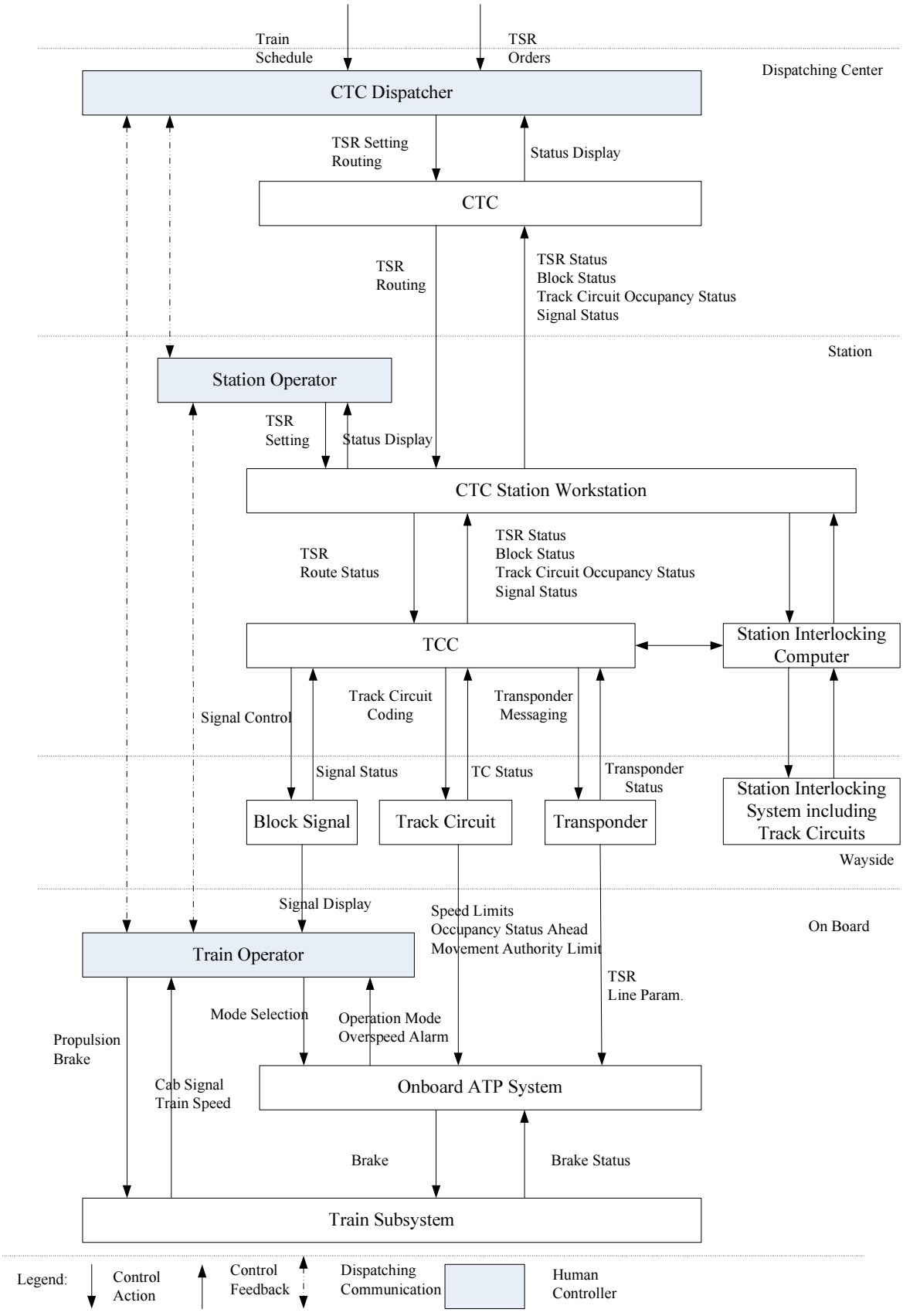

Train Schedule
TSR Orders
Dispatching Center
CTC Dispatcher
TSR Setting Routing
Status Display
CTC
TSR Routing
TSR Status
Block Status
Track Circuit Occupancy Status
Signal Status
Station
Station Operator
TSR Setting
Status Display
CTC Station Workstation
TSR Route Status
TSR Status
Block Status
Track Circuit Occupancy Status
Signal Status
TCC
Station Interlocking Computer
Signal Control
Track Circuit Coding
Transponder Messaging
Signal Status
TC Status
Transponder Status
Block Signal
Track Circuit
Transponder
Station Interlocking System including Track Circuits
Wayside
Signal Display
Speed Limits
Occupancy Status Ahead
Movement Authority Limit
On Board
Train Operator
TSR Line Param.
Mode Selection
Operation Mode
Overspeed Alarm
Propulsion
Brake
Cab Signal
Train Speed
Onboard ATP System
Brake
Brake Status
Train Subsystem
Legend:
Control Action
Control Feedback
Dispatching Communication
Human Controller

Figure 2-4. The Operating and Physical Process Control Structure

2.5. The System Safety Constraints and System Requirements Related to the Accident

Ministry of Railway (MOR)

On top of the control structure, MOR establishes railway business development strategy, planning and rail industry regulations; MOR manages the safety of rail operations and the quality of rail transportation services; MOR manages the rail transportation organization and the centralized dispatching work; and MOR establishes the rail industry technology policy, standards and management regulations.

There are 11 departments within the MOR organization. MOR Science and Technology Bureau establishes rail technology development planning, regulations, standards and management regulations; it organizes the research and application work of new technology and new product development.

The MOR Transportation Bureau establishes rail operations policy and regulations; it is responsible for centralized national railway dispatching management.

System Level Safety Constraints Related to this Accident:

1. The MOR must establish a control structure that provides the ability to prevent train to train collisions.

2. The safety regulations generated by MOR must be capable of preventing train to train collisions.

3. The quality control regulations generated by MOR must be capable of preventing train to train collisions.

China Railway Signaling and Communication Corp. (CRSC)

CRSC is the integrated signaling and communications system provider for the Yong-Wen Line. Beijing National Railway Research & Design Institute of Signal and Communication (CRSCD) belongs to CRSC group who designed the signaling system for this line, including interlocking and the Train Control Center integration systems. Shanghai Railway Communication Company also belongs to the CRSC group; it is one of the designated manufacturers for railway signaling and communication equipment. It manufactured the TCC equipment in WenZhou South station.

Design Management Level Safety Constraints Related to this Accident:

1. CRSC must follow safety regulations provided by MOR.

2. CRSC must establish safety system design guidelines that satisfy MOR safety regulations.

3. CRSC must establish quality control requirements that satisfy MOR quality control regulations.

Shanghai Railway Bureau

Shanghai Railway Bureau is one of the 18 railway bureaus belonging to the MOR. It manages the railway operation of four provinces: Anhui, Jiangsu, Zhejiang and Shanghai. Shanghai Railway Bureau is composed of Operation department and Maintenance department.

The CTC center is responsible for the train operation and dispatching work inside of its jurisdiction area. Within the total 27 train dispatching station, the Costal dispatching station is responsible for the train dispatching work of the Yong-Wen line. The Costal dispatching terminal displays the occupancy status and train status on 520 blocks from NingBo to TaiLaoShan, in total 21 stations. [2]

Operation Management Level Safety Constraints:

1. Shanghai Railway Bureau must follow MOR safety regulations for train operation management.
2. Shanghai Railway Bureau must establish safety operation requirements that specify safety operation rules in abnormal situations.
3. Shanghai Railway Bureau must ensure the safe operation rules are followed by all operations personnel.

CTC Dispatcher:

The dispatchers continually monitor the train operation status on the line, provide commands to adjust train operation according to schedule, and set temporary speed restrictions.

Safety Constraints Related to the Accident:

1. CTC dispatcher must know and follow the correct operational procedures in failure situations.
2. CTC dispatcher must track the route status in failure situations.
3. CTC dispatcher must track train status in failure situations.
4. CTC dispatcher must not dispatch trains in a way that could lead to a train to train collision.
5. CTC dispatcher must put priority of safe train operation before on-schedule operation.

Station Operator:

The station operator organizes passenger train operation and monitors the train operation and station equipment operation. The station operator can directly set station speed restrictions under certain situations.

Safety Constraints Related to the Accident:

1. Station Operator must know and follow the correct operational procedures in failure situations.
2. Station Operator must report the track and train status to people above in the control structure.

3. Station Operator must enforce joint train control with the train operator when in failure or hazardous situations.

Train Operator:

The train operator runs the train under the protection of the onboard Automatic Train Protection (ATP) system normally. In CTCS-2 system, the train can be operated in different operation modes depending on wayside and onboard situations. In normal operation the train can be operated in Full Supervision mode, the onboard train control equipment determines train location, stopping point and generates target braking speed profile, and provides vital train speed control and over speed alarm. Under certain failure situations, the train can be switched to On Sight (OS) mode. In this operation mode, the onboard equipment only provides minimum train speed control (e.g. 20km/h) where the train can only run under a minimum speed. The switch between operation modes is done manually by the train operator when the ATP system receives certain kind of codes or no codes from the track circuit.

Safety Constraints Related to the Accident:

1. Train Operator must know and follow the correct operational procedures in failure situations.
2. Train Operator must be able to know the failure situations on the wayside.
3. Train Operator must be able to communicate with Station and CTC personnel about the train status.

Maintenance:

Maintenance personnel are responsible for the maintenance of the system equipment.

Safety Constraints Related to the Accident:

1. Maintenance personnel must know and follow the correct maintenance procedures in failure situations.

2.6. The Proximate Events Leading to the Loss

Based on the accident investigation report, the events directly related to the accidents are listed in the following table:

Table 2-1. The Proximate Events Leading to the Accident

	Leading Train D3115	Following Train D301	WenZhou South Station (TCC)	Shanghai CTC
			One fuse of the power circuit of TCC data collection unit burnt out due to lightening hitting.	
19:30			Communication bus between track circuit 5829AG and TCC was also damaged by lightening.	
19:39			Station operator report to CTC dispatcher about the "failed" track circuit.	
19:40			Maintenance personnel started the inspection and recovery on track circuit failure.	
19:51	D3115 entered YongJia station. 4 minutes behind schedule.			
19:54				CTC dispatcher commanded three stations YongJia, Wenzhou South, and OuHai station to switch from Centralized Control mode to Abnormal Station Control mode after he found out the inconsistency between CTC display and station display.
20:09				CTC dispatcher notified D3115 train operator to switch to On Sight mode and continue if there is restrictive signal ahead due to track circuit failure.
20:12		D301 entered YongJia station. 36 minutes late.		
20:17:01				CTC dispatcher notified D3115 train operator, switch to On Sight operation mode and continue with speed less than 20km/h.

	Leading Train D3115	Following Train D301	WenZhou South Station (TCC)	Shanghai CTC
20:21:22	D3115 on board ATP enforced emergency brake due to abnormal data transmission of 5829AG.			
20:21:46	D3115 stopped at 584.115 kilometer post.			
From 20:21:46 to 20:28:49	D3115 train operator tried three times but failed to re-start the train.			
From 20:22:22 to 20:27:57	D3115 train operator called CTC dispatcher six times, and station operator three times, but all failed.			
From 20:17 to 20:24				CTC dispatcher received and dispatched eight other trains.
20:24:25				CTC dispatcher commanded D301 to start from YongJia station normally.
20:26:12				CTC dispatcher checked with station operator about D3115 and learned that station failed to reach D3115 operator.
20:27:57			Station operator reached D3115 train operator and learned that D3115 failed to reach CTC.	

	Leading Train D3115	Following Train D301	WenZhou South Station (TCC)	Shanghai CTC
From 20:28:43 to 20:28:51	D3115 failed to reach CTC dispatcher.			
From 20:28:54 to 20:29:02	D3115 failed to reach CTC dispatcher.			
20:29:26	D3115 train finally succeeded starting in On Sight mode after stopping for 7 minutes and 40 seconds.			
20:29:32		D301 reaches kilo post 582.497	Station personnel called D301 train operator, tried to warn him of the train ahead, call ended without finishing.	
20:30:05		D301 (90km/h) crashed into D3115 (16km/h) at 583.831 kilo post.		

2.7. The Physical Process Failures and Dysfunctional Interactions

Components of the Physical Process:

The Physical Process is composed of the CTC dispatching center, the TCC station equipment, the wayside equipment and the onboard train control equipment. The interactions of these elements are shown in Figure 2-4.

Physical Process Failures:

After the traction power distribution system or the ground system near Wenzhou South station was hit by lightening, one power circuit of the TCC equipment was broken. The PIO (data input and output) board lost power for input data, and it continued to output the old data before the failure. The hardware design error is that the PIO board only had one power circuit for inputting data, not two independent power circuits according to relevant requirements.

Before the failure occurred, there was no track occupancy within the blocks. But afterwards, this board still output no occupancy status to the control system, which led to the wrong signal open and the wrong codes being sent to the track circuit when there were trains inside of the blocks. Also this led to the wrong occupancy display in the CTC center.

Another physical failure is the track circuit 5829AG failure caused by the lightening. The communication channel failed between track circuit 5829AG and TCC, which caused the 5829AG to transmit control codes abnormally.

The wrong codes sent from the track circuit caused the leading train D3115 to stop on the track circuit, while the wrong codes sent from the track circuit caused the D301 train to run normally without stopping.

Other physical failures not mentioned in the investigation report include the CTC equipment did not provide adequate alert or alarm to the station operator in case of its equipment failure. The station operator knew there was inconsistency between the TCC display and the station interlocking computer (the station interlocking computer also connects to the wayside equipment and the track circuits, but its primary purpose is to provide interlocking control for stations, not block controls), but he could not know what went wrong or the extent of the failure. Also there was no alarm provided to the CTC dispatcher when the system could not track the leading train D3115.

Dysfunctional Interactions:

Dysfunctional Interactions between wayside and station equipments:

One dysfunctional interaction is the communication failure between TCC station equipment and wayside equipment. The communication failure caused the wayside track circuit 5829AG to send abnormal codes, which further led to the onboard system being unable to switch to OS mode.

Dysfunctional Interactions between wayside and onboard equipments:

The investigation report did not comment much on this dysfunctional interaction besides mentioning that it was due to the abnormal code transmission from the track circuit.

After the track circuit 5829AG failure, the onboard ATP system stopped the train by enforcing emergency braking. But after the train stopped, the train failed to start in On Sight (OS) mode due to the abnormal code transmission from the track circuit. The OS mode is a degraded mode with a fixed speed protection (e.g.20k/h) where the driver is responsible for the safe train operation. The condition to switch to OS mode is for the onboard equipment to receive certain kind of codes or no codes from the track circuit.

When the track circuit sent out abnormal codes, the ATP would not let the operation mode switch to OS mode. The onboard ATP system did exactly what it supposed to do, but is this the kind of result that we want? The train could not start after stopping for 7 minutes and 40 seconds, just waiting for the right kinds of code for it to switch to OS mode. At the same time we also know that the designed tracking interval for this line is 4 minutes for passenger trains.

Furthermore, if the system cannot switch to OS mode after the required 2 minutes, due to certain failure situations, does the operation manual tell the driver to switch to other manual mode operations, for example, isolation mode, instead of trying again and again and waiting for orders from the dispatcher?

Further investigation is needed to address this dysfunctional interaction. Detailed hazard analysis needs to be done for this interface specification. An alternate solution would be to allow ATP to switch to OS mode if the conditions to operate in other modes are not met. Not letting the train start in OS mode contributed to the hazard.

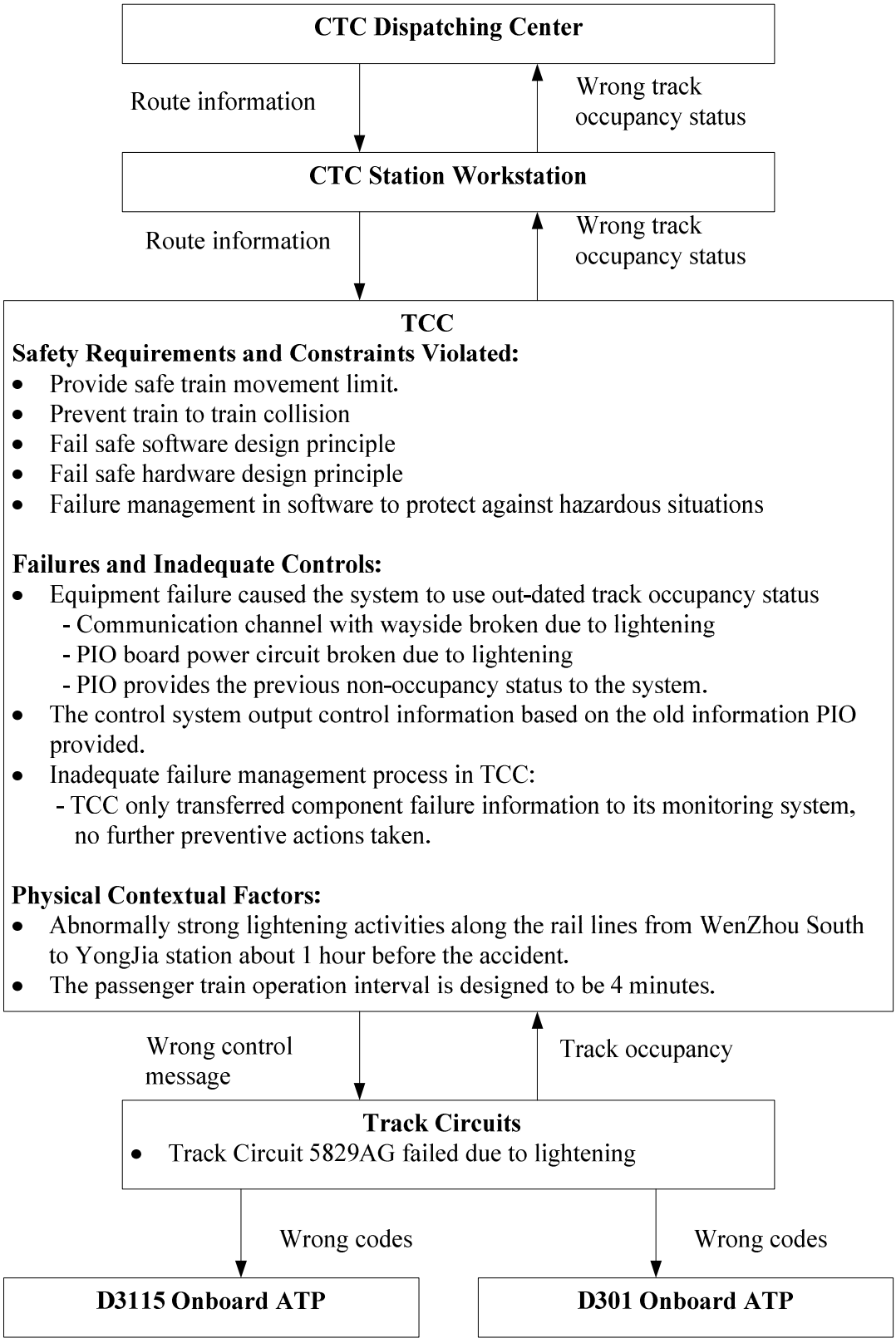


Figure 2-5. STAMP Analysis at Physical Level

2.8. The Operating Process

Context

The Yong-Wen line is operated by Shanghai Railway Bureau. Shanghai Railway Bureau is one of the busiest railway bureaus in China. It manages the rail transportation dispatching work of three provinces and one municipality (Jiangsu, Zhejiang, Anhui, and Shanghai). Four (JingHu, LongHai, JingJiu, HuKun) of the six busiest main lines in China are in its dispatching area. [5]

Before 2005, the railway system employed the "MOR-Railway Bureau-Branch of Railway Bureau-Station" control structure in order to improve efficiency. The structure was changed to "MOR-Railway Bureau-Station". The four original branches belonging to Shanghai Bureau were cancelled. Shanghai Railway Bureau dispatches trains directly for the four provinces. [5]

The CTC dispatchers work in a 12 hour shift and look closely to the display without stopping. According to the investigation report, during the 7 minutes after D3115 was dispatched and before dispatching D301, the dispatcher confirmed the field status of other stations along the line, confirmed again the station status of Wenzhou South station, learned the other train operation status, and received and dispatched another 8 trains.

Besides the busy status of the CTC dispatcher, he also faced schedule pressure and performance pressure. As the high speed rail has been rapidly developed in China, people's eyes all over the world are looking at China and at how they perform in high speed rail development. Stopping trains not only would cause disruptions in schedules, but also negatively impact the whole image of the China high speed rail and the operations of the bureau.

Safety Related Responsibilities:

The operation personnel must follow the operation rules, both normal and abnormal situations. The CTC dispatcher must ensure safe dispatching of trains. The station operator must ensure safe train operation together with the train operator in abnormal or failure situations.

Flawed or Inadequate Decisions and Control Actions

The CTC dispatcher didn't track the failure status in the field and didn't track the D3115 train status in time after he dispatched the train into the blocks. Without knowing where the leading train D3115 was and what the field failure status was, the CTC dispatcher decided to dispatch the following train D301 into the blocks normally.

In the last minutes before the accident and after the station operator learned what happened to D3315, he failed to report to the CTC dispatcher and didn't warn the following train operator even in the abnormal station control state.

Inaccurate Mental Models:

At the time station operator reported to CTC dispatcher, there was an inconsistency between the station interlocking computer display and the station CTC display. The CTC dispatcher knew that there were failures in the field and commanded the abnormal station control status. But as the CTC display didn't

show the occupancy status of D3115, the dispatcher's mental model didn't consider the train stopped there, and he must have assumed even if it stopped, it would continue in OS mode as already commanded to the operator.

As the track circuit failed due to lightening, the display in the station interlocking computer gave the wrongly occupied information, even when D3115 stopped on that track circuit. The station operator's mental model must have been that it was wrongly occupied due to the track circuit failure. He didn't realize there was a train until he finally reached the D3115 operator.

Both the CTC dispatcher and the station operator must have assumed the failed system was still fail-safe. Their mental model didn't consider the TCC failure would cause the wrongly permissive status of the signaling system to the following train. They both thought the train would be stopped by the system automatically if it was getting too close to the leading train. If not, the train can go through normally and they would avoid another "holding a train in station". That probably explains why the CTC dispatcher would command D301 to run normally and the station operator didn't report the D3115 to CTC dispatcher after he learned its status.

Dysfunctional Interactions

Except mentioning there were 8 times the D3115 train operator failed in trying to reach the CTC dispatcher and the station operator failed 3 times to reach the train, the investigation report didn't explain why. The most probable reason is that the dispatching communication channel also experienced intermittent failure. The dispatching communication system used between the train operator, station operator and the CTC dispatcher is based on the GSM-R network.

From the proximate events, about 4 minutes before the accident, the CTC dispatcher asked the station operator about the status of D3115. He didn't get any result due to the communication. About 2 minutes before the accident, the station operator reached the D3115 and learned that the train failed to start, but he didn't report this situation to the CTC dispatcher. Then 33 seconds before the accident, another station operator tried to warn the following train D301 about the stopped D3115, but he couldn't finish the call before the accident happened.

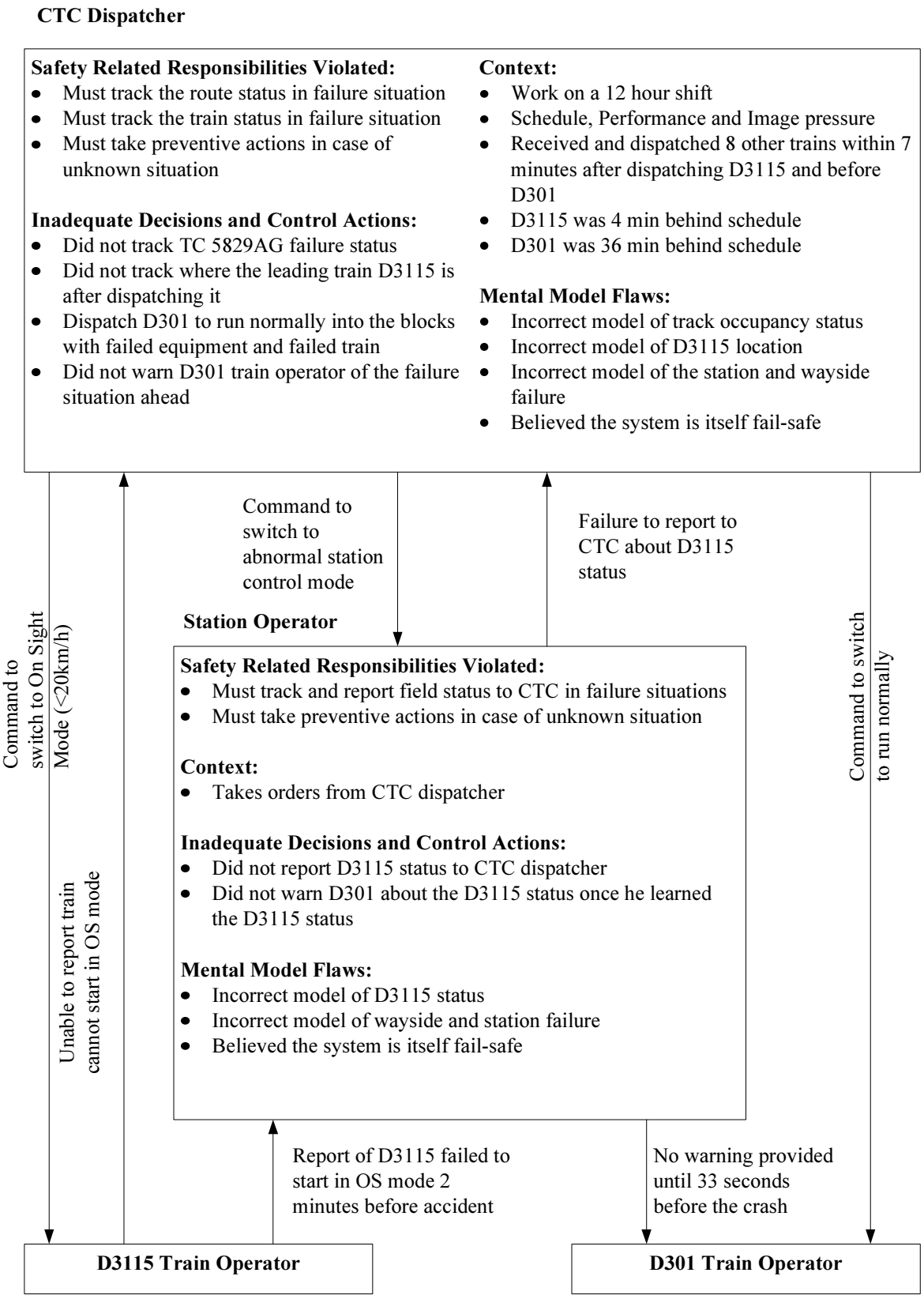


Figure 2-6. STAMP Analysis at Operational Level

2.9. The Project Development and Management Process

Context

MOR requires permission be given to railway signaling product suppliers. The permission is granted by MOR itself. At the CTCS-2 level, only CRSC, Hollysys, and China Academy of Railway Science (CARS) had permission to provide CTCS-2 wayside equipment. Only CRSC and Hollysys had permission to provide the CTCS-3 system. [4]

At the same time, the research and development of the CTCS system has to catch up with the schedule of railway speed increase and the building of new dedicated passenger lines. In the seven years before the accident happened, CRSC developed the CTCS system integration platform. The CTCS-2 and CTCS-3 system they developed had been used extensively in the Chinese High-speed Rail lines. [4]

With the tight schedules they faced, the development teams barely had the time to improve the system they designed. Problems occurred during the development and testing phase that could only be solved after the system was in service run.

Safety Related Responsibilities:

The project management must set safety standards for the design team. The project design team must follow the safety standards to develop the system hazard analysis and provide it to the management for review.

The development project team must provide a safe design of the product and deliver operational and maintenance documents to the operation and maintenance team. The project team must ensure and verify the safety of the system they are delivering to the customer.

To achieve this, not only fail safe design principles need to be followed, but also an effective safe design approach must be established with the goal of identifying scenarios and causal factors and then to eliminate or mitigate hazardous situations. Extensive integration testing, field testing and test runs must be conducted before final delivery of the product.

Flawed or Inadequate Decisions and Control Actions

The LKD2-T1 equipment was developed in a hasty way. There was no formal design and development team organized for this project, no comprehensive review for the equipment, no formal review by the PIO board, and no complete design documents.

Traditionally, the design focus has been more on hardware than software. Testing has focused more on functional requirements than safety requirements.

Process Model Flaws:

Traditionally, more focus on safety has been put on hardware design than on software design and more on hardware and software design than on documenting assumptions, system limits and operating procedures.

Due to the tight schedule, they thought problems and errors would be discovered and solved through incidents that occurred during the service run.

Dysfunctional Interactions:

The project design and development team must provide complete operation and maintenance manual to the operation team. Due to the management confusion of this project, lots of documentation was missing.

Safety Related Responsibilities Violated:

- Must establish safety standards for project design and development
- Must establish effective safety guided design process
- Must test and verify the safety of the products implemented

Context:

- Many parallel projects going on with very tight project schedule
- LKD2-T1 type TCC was developed from a new hardware platform

Inadequate Decisions and Control Actions:

- No formal project team organized for this project
- No safety standards, no formal design review
- Lack of certain failure management in software
- Not fail safe design for PIO board hardware
- Not fail safe design for TCC software
- Inadequate hazard analysis to capture the failure scenarios
- No testing requirements capable of detecting hazardous behaviors.

Process Model Flaws:

- Less focus on safe software design than hardware design.
- Traditional testing is focused more on functional requirements than safety requirements.
- Believed the errors and failures can be discovered and fixed during operation process.

Figure 2-7. STAMP analysis of the project development and management process

2.10. The Corporate Level Management

CRSC Corporate Level Management:

Context

The rapid development of high speed rail brings the CRSC group great opportunities for economic development. As mentioned earlier, only companies who have MOR permission can manufacture and supply the signaling equipment, CRSC faced only a couple of competitions for CTCS-2 system and almost no competitions for CTCS-3 system.

Safety Related Responsibilities:

As the product and service provider, CRSC corporate level management must follow MOR safety regulations and establish the safety policy for the company; must monitor the safety practices in the organization; and must ensure its products delivered to customer meet MOR safety requirements and national quality requirements.

Flawed or Inadequate Decisions and Control Actions

The decision to not organize a formal project team for product development was one of the major management deficiencies for the project.

CRSC management failed to monitor closely the quality of the research and development of CRSCD, failed to follow MOR and national regulations and rules. They handed the entire project to CRSCD for development and management with no monitoring of the status afterwards.

They did not detect the inadequate management of the LKD2-T1 project, they did not know the PIO board was not reviewed, and they proposed the usage of LKD2-T1 product when its component design was not finished.

Process Model Flaws:

The management put more focus on schedule and delivery management than on the quality management of the product development and thought the system safety would be controlled by the design and development process.

The management has this mental model that safety can be taken care of just by designing the system according to fail-safe principle, which has already been required in the CTCS and CTCS-2 specifications. In fact, the fail-safe principle alone is far from adequate to achieve system safety. The other factors including management and organization are equally important in preventing accidents by controlling hazards as evidenced by this accident.

Dysfunctional Interactions:

The project design and development team must provide complete operations and maintenance manuals to the operations team. Due to the poor management of this project, lots of documentation was missing.

Safety Related Responsibilities Violated:

- Must establish safety policy for the company
- Must monitor the safety practices inside of the company
- Must ensure safety and reliability of the products delivered to customer

Context:

- Great opportunity for economic development of the group
- Less competition for the advanced signaling projects

Inadequate Decisions and Control Actions:

- Inadequate monitoring of the safety management program of the organization
- Inadequate monitoring of the quality management program of the organization
- Inadequate management of the research and development activities of the company
- Inadequate reviewing process for design and development activities
- Did not ensure the fail safe design principle was followed by the project
- Disorganized management of the LKD2-T1 TCC R&D project
- Did not find out that the PIO board was not reviewed
- Out of control of the quality management of its subsidiary manufacturers
- Immature proposal of the LKD2-T1 TCC application when its component design was not finished

Process Model Flaws:

- Believed safety can be taken care of by designing the system safe.
- More management on schedule of product delivery than on development processes

Figure 2-8. STAMP Analysis at CRSC Corporate Management Level

Shanghai Railway Bureau Management:

Context

Not only the dispatchers and other operation personnel, but the management also has to cope with the operation and maintenance management of the busiest main lines. Together with the operations people, they faced the same schedule pressure, and they wanted to build a good image of effective high speed rail operation in China.

Safety Related Responsibilities:

As the rail operation organization, Shanghai Railway Bureau must ensure safe operation in every step of the operation and maintenance practices. It must establish clear procedures for people to follow in both

normal and abnormal situations. It must provide adequate training to the operation and maintenance personnel.

Flawed or Inadequate Decisions and Control Actions

Shanghai Railway Bureau was not strict enough in execution of the emergency operation rules, was not effective in monitoring the regulation execution in operation. Not enough training was provided to the operation and maintenance personnel.

Process Model Flaws:

The managements should have put more focus on schedule management than on the quality management of operations. They thought the frequent stopping of trains would impact their operational and management image.

Dysfunctional Interactions:

The operations side must provide detailed information on operational problems they experienced to the system design side, and the management must follow the resolution of these problems. The investigation report didn't explore this interaction, but presumably it didn't function very well.

Safety Related Responsibilities Violated:

- Must monitor the safety practices within the company
- Must establish effective operational and maintenance procedures to follow in hazardous situations
- Must provide adequate training to operation and maintenance personnel

Context:

- One of the busiest railway bureaus in China
- Facing schedule, performance and operation image pressure from the outside world

Inadequate Decisions and Control Actions:

- Inadequate monitoring of the safety rules execution
- Inadequate control in executing emergency safety rules
- Inadequate training provided to operation and maintenance personnel

Process Model Flaws:

- Believed the operation personnel follow the regulations
- Believed schedule and performance management is more needed than safety management
- Believed more frequent stopping of trains would impact their performance image

Figure 2-9. STAMP Analysis at Shanghai Railway Bureau Management Level

2.11. MOR

Context

As China faced great demand for rail transportation and fast economic development, MOR wanted to take this opportunity to improve the existing rail system greatly and develop the high speed rail rapidly.

The rapid development made everybody face great schedule pressure. When schedule concerns conflict with following a strict design process, which rule to follow?

Safety Related Responsibilities:

MOR must establish safety rules for both system design and system operations to follow; must monitor the safety execution in each side, ensure safety rules are followed and executed in each step of the control actions taken inside of the control structure. At the same time, MOR must establish practical schedule for rail signaling projects in order to ensure that the safety rules will be followed.

Flawed or Inadequate Decisions and Control Actions

In the railway projects, MOR had rushed to speed up the construction and system development, in order to catch up or be ahead of the schedule, and didn't put enough practical considerations and actions on safety. Emergency and failure management rules were not complete; the regulations and standards for the dedicated passenger line systems were not complete; and the product technical reviews lacked sound basis and foundation. There were function overlaps between different departments inside of the organization. They permitted the usage of the LKD2-T1 product without field testing and test runs, while deciding to improve the system during revenue service.

Process Model Flaws:

MOR believed the safety rules have been followed by all parties and the strict policy against violating safety rules would push people to follow the rules. MOR also believed everything is possible through enough effort.

Safety Related Responsibilities Violated:

- Must establish adequate safety regulations for system development and operation.
- Must take effective actions in ensuring safety rules are followed
- Must establish practical schedule for railway project development

Context:

- Want to be in lead position in high speed rail development in the world
- Want to build local competency and enter markets abroad

Inadequate Decisions and Control Actions:

- Railway project schedules are not realistic to ensure safety and quality.
- Incomplete regulations and specifications for high speed rail integration
- Inadequate safety regulations
- Ineffective organization management
- Permitted the LKD1-T2 TCC equipment to be used without field testing and test run
- Certification of the LKD1-T2 TCC equipment after considering it "basically" satisfies MOR requirements
- Permitted to improve the system during the usage of LKD1-T2 TCC equipment in service operation
- Did not establish special rules to identify and discover failures after giving permission to improve the system during service operation.
- Inadequate technical review procedures
- Inadequate monitoring of the safety rules execution in railway bureaus

Process Model Flaws:

- Believed safety rules were being followed through emphasizing safe design process
- Believed safety rules were being followed through strict rules in punishment for violating safety in operations
- Believed everything is possible through enough efforts

Figure 2-10. STAMP Analysis at MOR Level

2.12. Coordination and Communication

To establish an effective safety control structure, effective coordination and communication between parties not in direct hierarchical control levels is important.

In this railway project control structure, the project development and management team must provide complete operation and maintenance manuals to the operation and maintenance teams. The operation team must provide detailed information about operational problems they experience to the system design

team, for them to improve the system design or operational procedures. The maintenance team must also provide detailed information about maintenance problems to the system design team.

Both the CRSC and the Shanghai Railway Bureau management have to ensure communication and coordination between the development team and the operation team is effective, the communication channels are established, and they are readily accessible. They must take action to ensure that problems are reported immediately and they must follow the resolution of these problems.

2.13. Dynamics of the Accident and the Safety Culture

As everybody in the China Rail "world" may have already known, safety has always been the number one priority of MOR, both in the system design and the system operation sides of the structure. You can see signs of "Safety is always the number one consideration", and signs about "safe operations" all over the train depots, operation and maintenance places. Fail safe design cannot be emphasized enough. MOR also has strict rules towards those violating safety rules.

But, safety is not a slogan. It's not something that can be controlled by fail safe design alone. And, it's not something can be controlled by pressure and punishment. Safety has to be managed very carefully, within each step of the control actions, within each of the communications and coordination between controllers, and inside of the whole control structure.

According to Rasmussen, most major accidents result from a migration of the system toward reduced safety margins over time. In this accident, pressure from both development schedule and operation schedule was one cause of this degradation in safety. The following system dynamics model shows how the safety margin was reduced due to the schedule pressures faced by the development organization and the performance pressure faced by the operation.

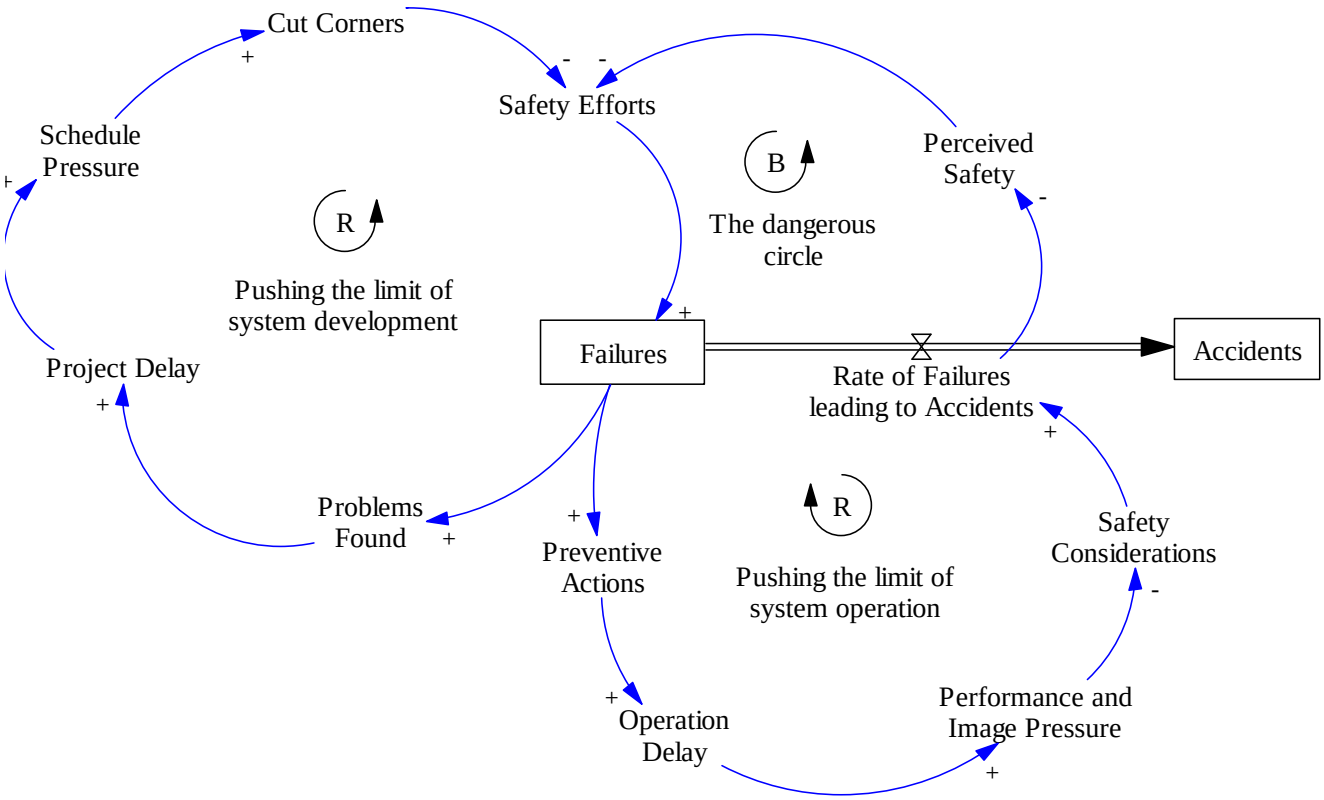


Figure 2-11. The Dynamics of Schedule Pressure Leading up to the Accident (Reference to [1])

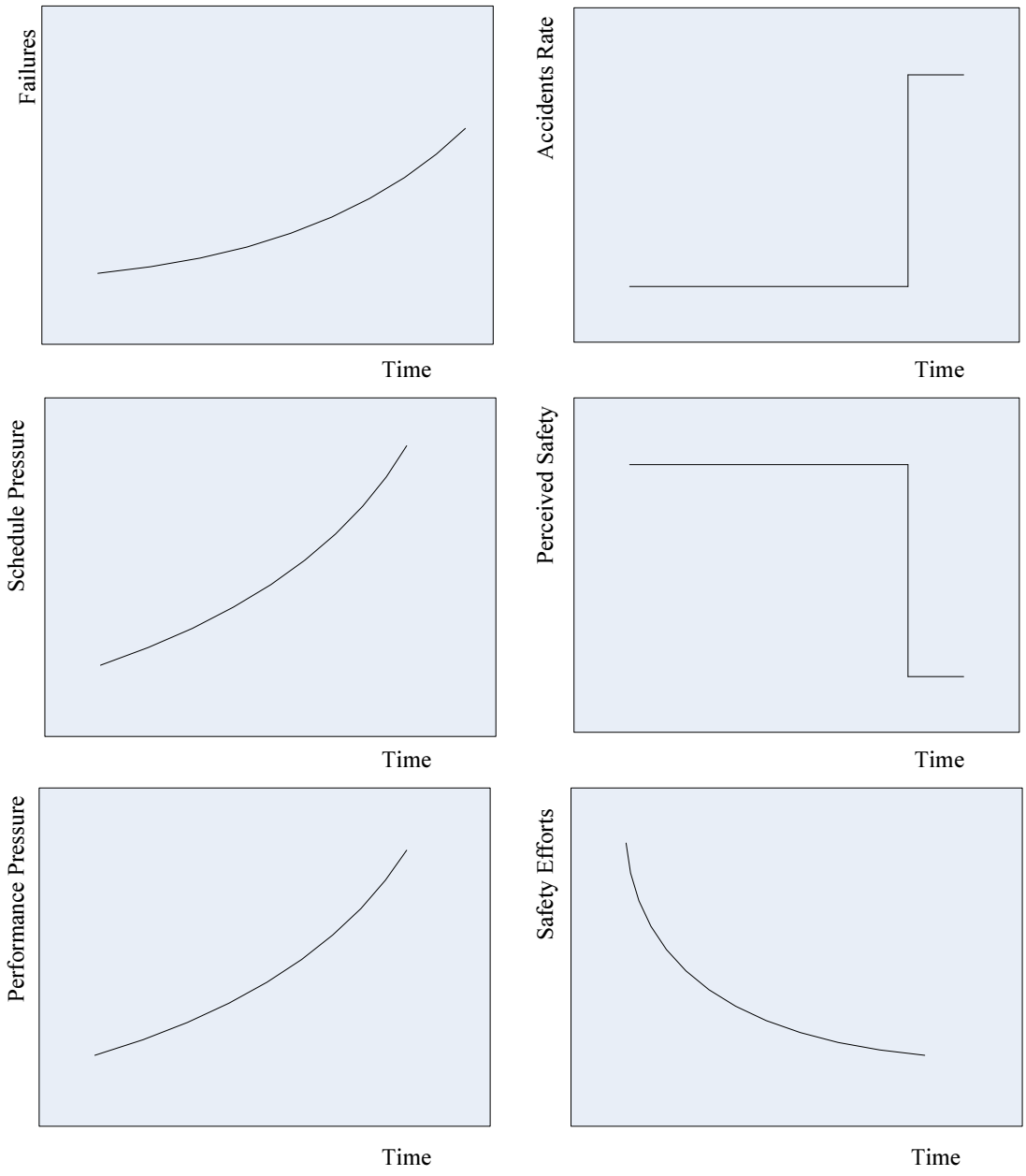


Figure 2-12. Reference modes for the accident dynamics model

In the reinforcing (R) loop of pushing the limit of system development, as more failures occur, more problems need to be fixed. This leads to increased pressure in project schedules. In order to meet schedules, the development team has to cut corners, reduce safety efforts, which in turn will lead to more failures.

In the reinforcing (R) loop of pushing the limit of system operation, as more failures occur, more preventive actions need to be taken. This means more operation delays, which leads to an increase in performance and image pressure. In order to reduce this pressure, the operation team has to reduce

safety considerations. Together with the previous reinforcing loop, these accelerated safety risks will eventually increase the accident rate.

As accidents usually do not occur for a while, in the loop called “the dangerous circle”, there is a false confidence in the perceived safety, which leads to reduced safety efforts. This is a dangerous circle because as the confidence getting higher and higher, people will tend to decrease more and more their safety efforts, which will eventually lead to big accidents.

A safety culture is a culture that exhibits high management commitment to safety and high level of awareness of safety controls in each level of the safety control structure. It promotes learning from mistakes, not from blame and punishments.

The above analysis shows how safety was sacrificed in face of tight schedules of development and schedules of train run. Some other policies need to be examined as well to find out whether they promote safety culture or not.

Consider the MOR regulations on rewards and punishments for safe train operations as an example. Another system dynamics diagram shown below, which is apparently a “Policy Resistance” case, we can see how a policy can work against its intended results. At the same time the diagram shows how to analyze whether a policy is promoting or damaging a safety culture.

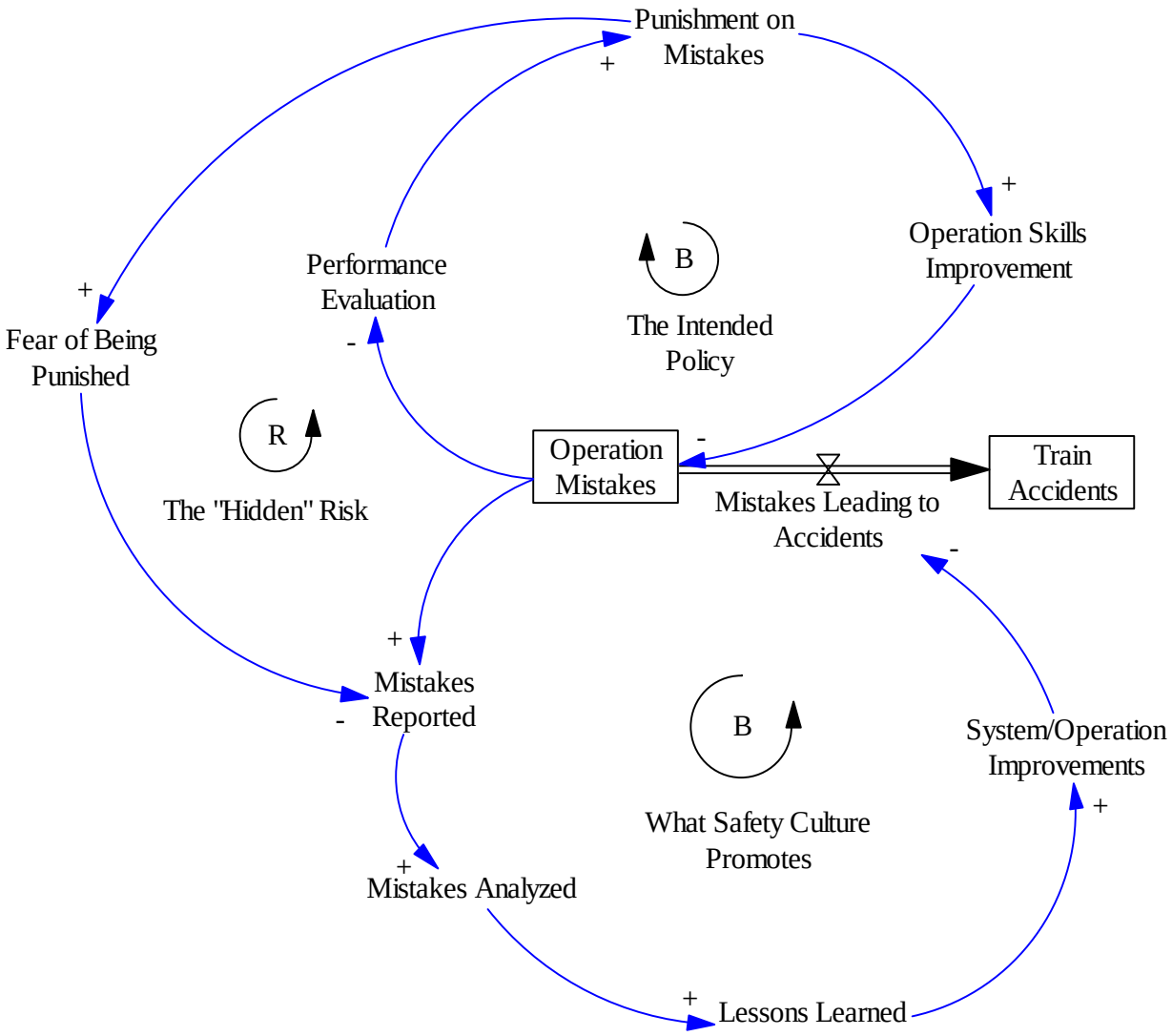


Figure 2-13. Policy Resistance Analysis of the Punishment Policy

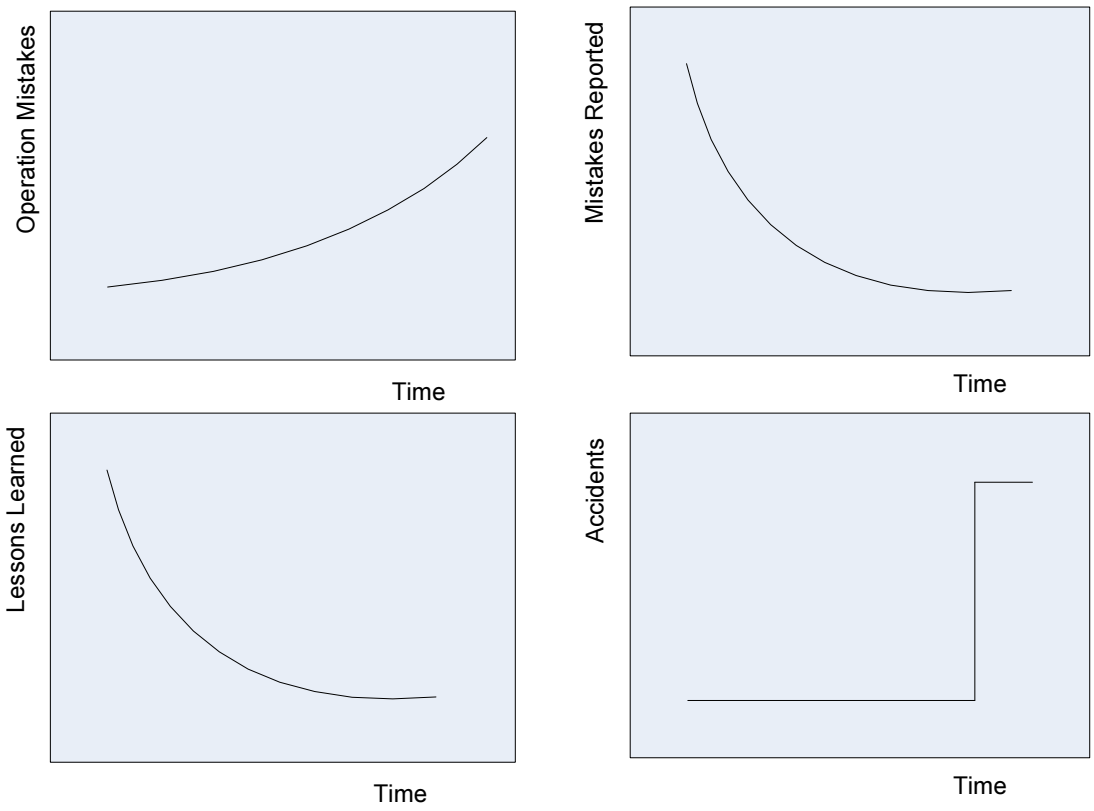


Figure 2-14. The Reference Modes of the Policy Resistance model

Very often before some kind of accidents, there are pre-cursors, or small incidents, that may be discovered by operation mistakes. Due to the linkage between operation mistakes and performance, and due to the strict punishment rules, people are afraid of reporting mistakes. They are reluctant to let others know that they did something that caused unintended results. In the reinforcing "The hidden risk" loop, the more punishment for mistakes, the fewer mistakes that are reported.

But the system design is not a closed loop by itself; it needs feedback from operations to be improved. The more problems discovered during operation, the more problems will be analyzed and fixed. A safety culture promotes learning from mistakes, as indicated in the Balancing (B) loop of "What a Safety Culture Promotes". Reporting more mistakes will lead to more improvements in both system design and operational improvements, through modifying system design and/or establishing more operational procedures. This in turn, will lead to the elimination or control of system hazards.

The policy maker may think once the performance evaluation is linked to the mistakes people make, together with strict punishment for big mistakes, people will be forced to follow rules and improve their performances. This is the balancing loop (B) of the model.

But, they may not realize that, due to the fear of punishment, people may be afraid of reporting operation mistakes, as indicated in the reinforcing (R) loop in the model. As less and less mistakes are reported, there will be less and less lessons learned from operations. This in turn, can eventually lead to big accidents.

2.14. Recommendations

The recommendations here are based on the analysis done previously, summarized from the safety constraints, inadequate control actions and inaccurate mental models of those elements inside of the control structure.

Physical Equipment and Design:

1. Investigate more about lightening protection in extreme situations.
2. Re-visit the design of the whole system and develop detailed hazard analysis using STPA (example provided in Chapter 3 of this thesis) to identify all potential accident scenarios.
3. Fully test the system against all failure situations and environmental situations including temperature, humidity, lightning, etc.
4. Add failure management to the TCC software to handle the equipment failures and provide alarms to the station operators.
5. Add failure management to the CTC software to respond to failure in tracking trains and provide alarms to the dispatchers.

CRSCD Project Development and Management:

1. Set up a formal project development team with roles and responsibilities assigned.
2. Perform adequate hazard analysis and risk analysis for each project.
3. Establish effective safety guided system design procedures and design safety into system.
4. Document operational assumptions, safety constraints and operational limits in the system design documents.
5. Identify inadequate safety control between onboard, wayside and station equipment.
6. Establish technical review procedures.
7. Establish integration tests, field tests and test run procedures.
8. Provide comprehensive operational and maintenance manuals.
9. Gather feedback from operations and maintain hazard logs.
10. Investigate more into the interface specification between wayside and onboard equipments. Make sure the specification is correct for the following system design.

CRSC Corporate Management:

1. Establish a safety policy for the entire organization.

2. Establish a corporate level safety control structure, assigning responsibility to enforce the safety controls.

3. Specify criteria in measuring and evaluating the decisions in implementing safety control.

4. Establish a corporate process safety organization to provide safety oversight.

5. Establish and manage the communication and coordination channels with the end users of the system.

Shanghai Railway Bureau Management and Operation:

1. Establish a safety policy for the railway bureau.

2. Establish a corporate level safety control structure, assigning responsibility to enforce the safety controls.

3. Establish emergency and hazardous situation operation procedures.

4. Specify criteria in measuring and evaluating the decisions in implementing safety control.

5. Establish a corporate process safety organization to provide safety oversight.

6. Ensure everyone has appropriate training in safety and specific hazards associated with operations.

7. Provide operation feedback to system design to improve the system.

8. Ensure there is always an available communication channel within the dispatching systems.

9. Establish and manage the communication and coordination channels with the system developers.

MOR:

1. Setup a safety authority department supervising and monitoring the safety of both system design and system operations.

2. Implement a more effective safety control structure, with safety responsibility clearly identified. The recommended safety control structure is in Figure 2-16.

3. Set up a complete set of specifications for the high speed rail control systems.

4. Set up and regularly update safety regulations and rules for the entire railway system.

5. Set up an effective control structure with clear safety responsibilities assigned to each controller.

6. Specify criteria in monitoring the execution of the safety rules.

7. Establish a safety organization to provide safety oversight.

8. Implement and sustain a strong safety culture.
9. Set up practical and feasible schedules for high speed rail development.
10. Investigate more into the safety culture of the Railway industry and examine whether the policies are promoting a good safety culture or not.

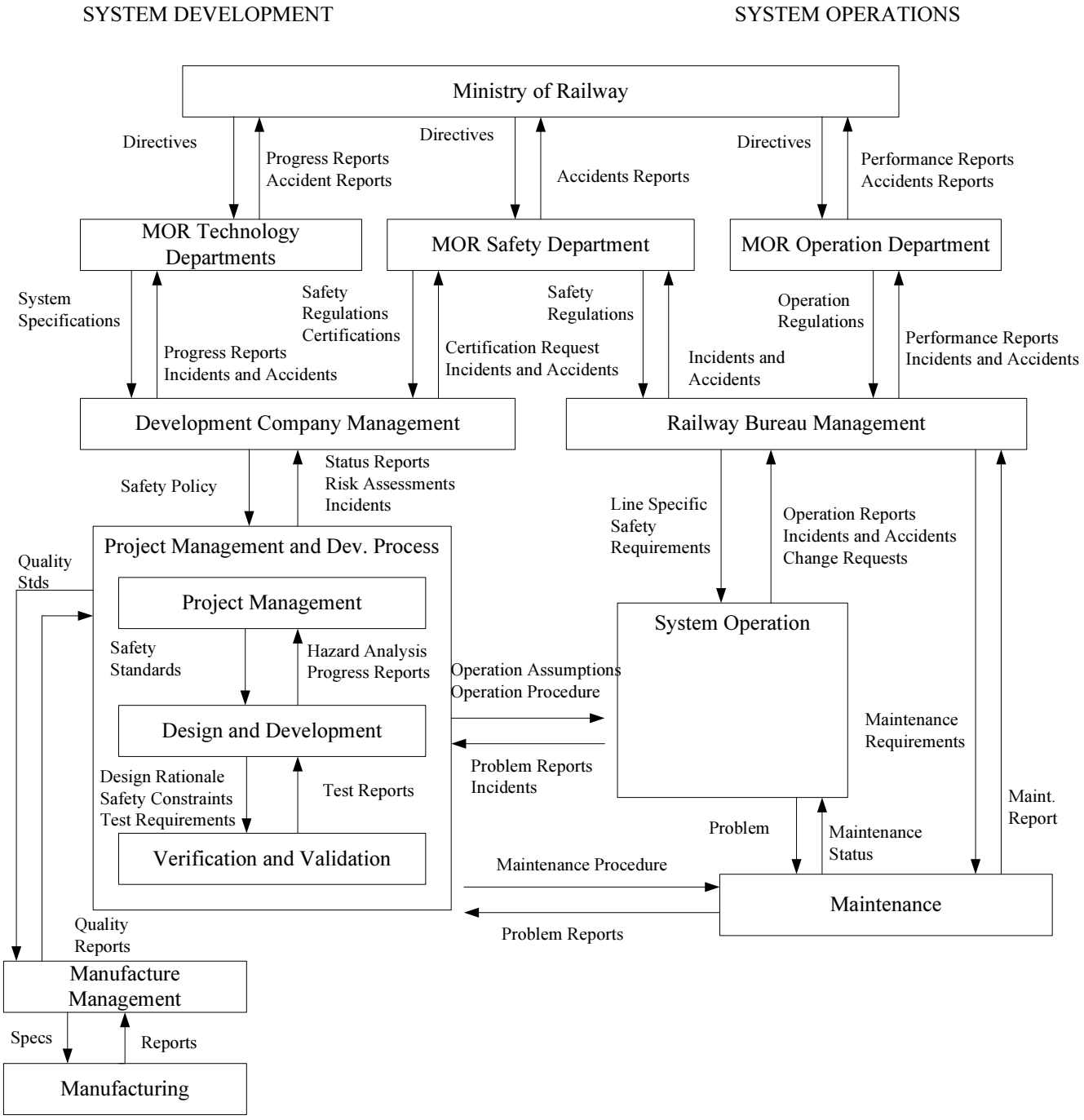


Figure 2-16. Recommended Safety Control Structure for MOR

3. Safety Guided Design Approach to the CBTC system

In the second part of this thesis, STPA hazard analysis is applied to the Communication Based Train Control (CBTC) system design. IEEE Standard 1474 is the standard for the CBTC system, including Performance and Functional Requirements (1474.1), User-Interface Requirements (1474.2), and IEEE Recommended Practice for CBTC System Design and Functional Allocations (1474.3). Based on these standards, a high level hazard analysis using STPA is done, then the high level system safety constraints are developed.

3.1. The CBTC System

The CBTC standards defined in IEEE1474.1 are intended to be applicable to the full range of transit applications, including light rail, heavy rail, and commuter rail transit systems. IEEE1474.1 has the following definitions about the characteristics of the CBTC system:

"The primary characteristics of a CBTC system include the following:

a) High-resolution train location determination, independent of track circuits

b) Continuous, high capacity, bidirectional train-to-wayside data communications

c) Train-borne and wayside processors performing vital functions "

In conventional train control systems, the train is detected through track circuit occupancy, the route and speed information is provided to train operators through wayside and cab signals. While these conventional systems are effective in train protection, they are not efficient in terms of system performance. The CBTC system aims to achieve shorter headway between trains and provide safe train protection at the same time.

According to IEEE1474.1, The CBTC System can provide Automatic Train Protection (ATP), Automatic Train Supervision (ATS), and Automatic Train Operation (ATO) functions.

The ATP function is to provide fail safe protection of trains against collision, over-speed and other hazards through train detection and train separation functions.

The ATO function is to provide speed regulation, station stopping, door control and other functions normally performed by the train operator.

The ATS function is to monitor trains, adjust performance level to maintain schedule, it typically provides manual and automatic routing functions.

The configuration of the CBTC system can include all these subsystem; or include ATP only; or ATP with certain functions of ATO/ATS.

The IEEE1474.3 has allocated the CBTC functions into the following major subsystems:

1. CBTC ATS equipment
2. CBTC Wayside equipment
3. CBTC Car-borne equipment
4. CBTC Data Communications equipment

The ATS equipment performs the ATS functions. The Wayside equipment performs wayside ATP functions. The car-borne equipment performs the car-borne ATP and ATO functions. The system is also supposed to interface with an external Interlocking system and other external wayside equipment.

For simplicity, the following analysis does not consider the ATO functions, only the manual mode of operation is considered.

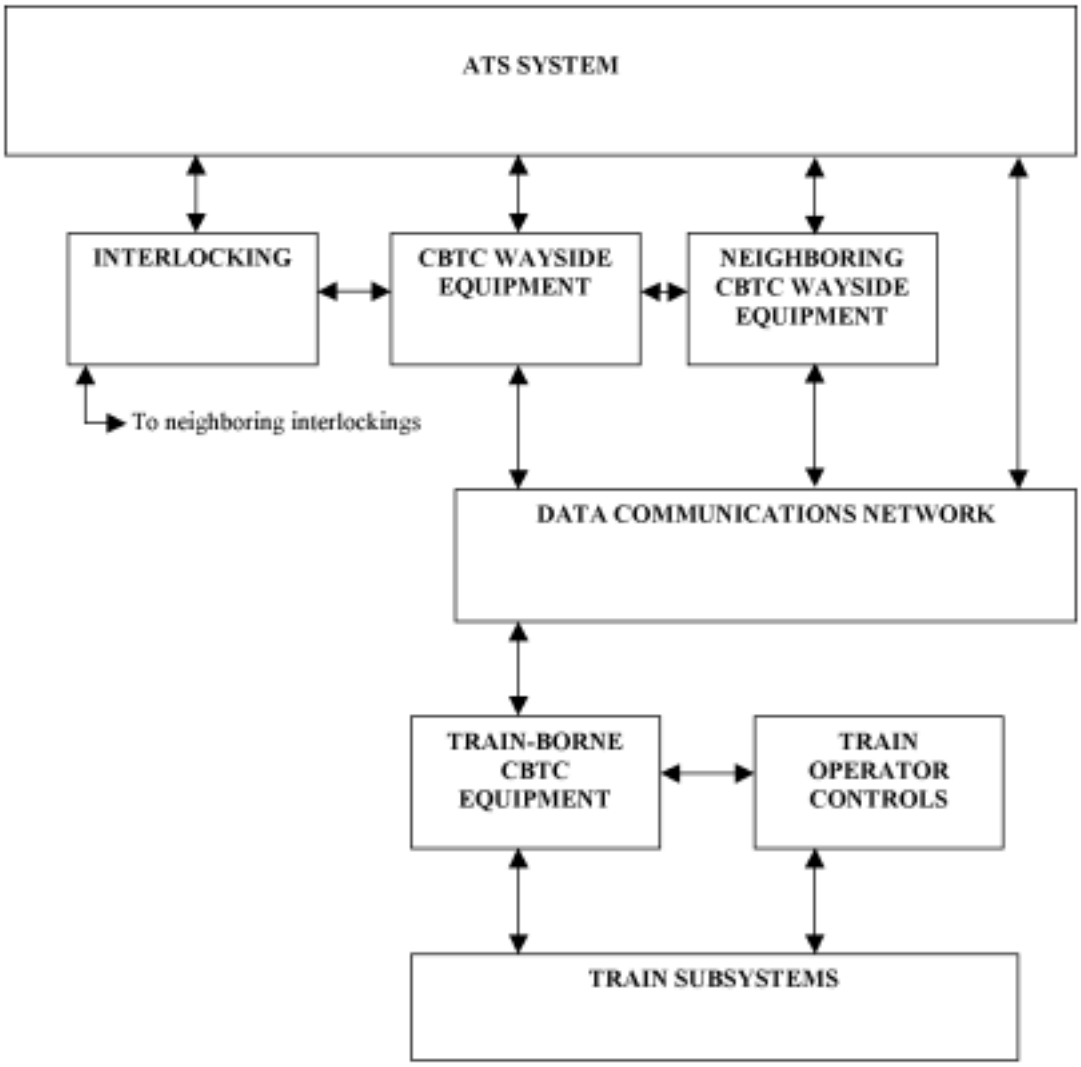


Figure 3-1. Example Functional Block Diagram for a Typical CBTC System [8]

3.2. The Safety Guided System Design Process using STPA

The primary goal of STPA is to include the new causal factors identified in STAMP that are not handled by the older techniques. More specifically, the hazard analysis technique should include design errors, including software flaws; component interaction accidents; cognitively complex human decision-making errors; and social, organizational, and management factors contributing to accidents. In short, the goal is to identify accident scenarios that encompass the entire accident process, not just the electro-mechanical components [1].

One key to having a cost-effective safety effort is to embed it into a system engineering process from the very beginning and to design safety into the system as the design decisions are made. STPA can be used not just as a hazard analysis technique on an existing system; it can also be used in a proactive way to help guide the design and system development. This integrated design and analysis process is called safety-guided design.

There are two main steps in performing the STPA process: [1]

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:

    a. A control action required for safety is not provided or not followed;

    b. An unsafe control action is provided;

    c. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequences;

    d. A control action required for safety is stopped too soon or applied too long.

2. Determine how each potentially hazardous control action identified in step 1 could occur.

    a. Augment the control structure with a process model for each control component.

    b. For each unsafe control action, examine the parts of the control loop to see if they could cause it. (Refer to Figure 3-2).

    c. Consider how the designed controls could degrade over time and build in protection.

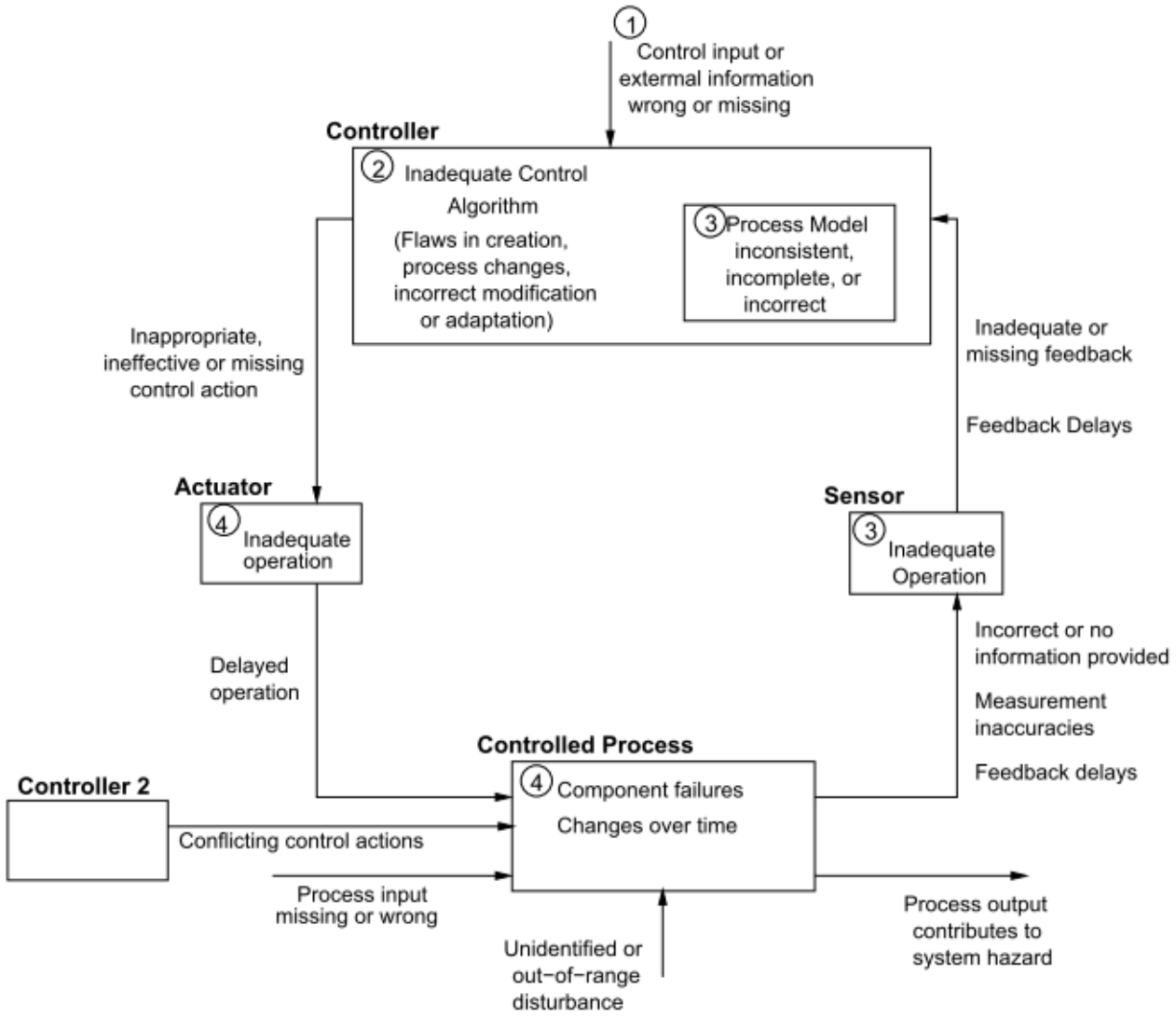


Figure 3-2. Causal Factors to be Considered for Scenario Analysis [1]

Specifications act as the glue to integrate the activities of engineering and operating complex systems. An intent specification is used to help people deal with complexity. The primary difference between the intent specification and a standard specification resides in its structure, the structure is so constructed that the contents provide not only “what” and “how” information, but also the important “why” information. The structure of an intent specification is based on the hierarchy concept of systems theory, in which complex systems are modeled in a hierarchy of levels, each level imposing constraints to the level below, and each level providing the “why” information to the level above. [1]

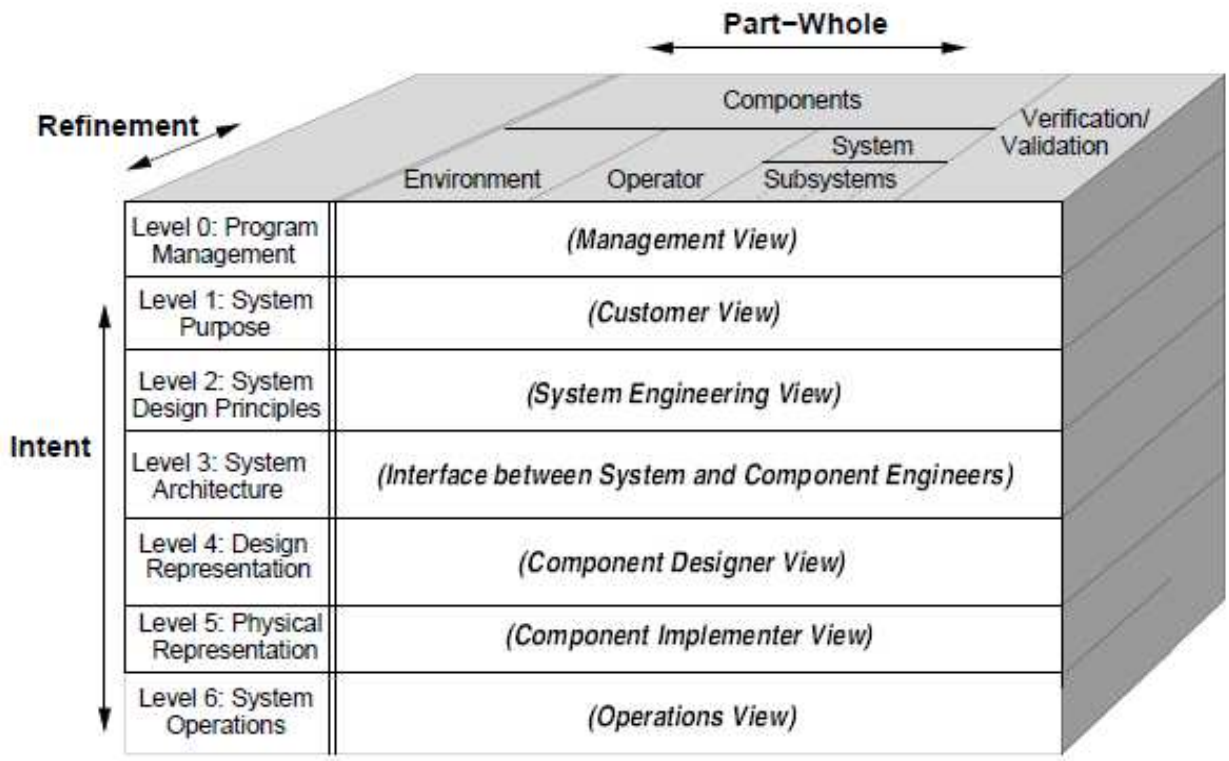


Figure 3-3. The Structure of an Intent Specification [1]

The following sections start a safety-guided design approach for the CBTC system, based on the intent specification structure (Level 1 only), using the STPA hazard analysis technique.

In Level 1 of this intent specification, system level goals and environmental assumptions are documented, accidents and hazards are identified, and a preliminary hazard analysis is performed. High-level system safety constraints and safety constraints for the system elements (ATS, WC-APT, TC-ATP) are developed from the hazard analysis.

3.3. Level 1: System-Level Goals, Requirements, and Constraints Generation

3.3.1. System Goals

G1. Allow trains to operate safely at much closer headways.

G2. Provide automatic safe train separation and over speed protection.

G3. Provide automatic passenger protection.

3.3.2. Accident Definition

A1. Train to train collision.

A2. Train to structure collision.

A3. Train derailment.

A4. Train to highway vehicles collision.

A5. Train collision to work crews and work trains.

A6. Passenger injury associated with train doors.

3.3.3. Hazard Identification

The CBTC system determines for the train the most restrictive point of the fixed and mobile obstacles ahead, which is the movement authority limit. A target point is more restrictive than the limit of movement protection by a defined safety margin, and the safety margin is determined by the applicable safe braking model. The CBTC system will calculate the ATP profile (the profile of safe speed) based on the target point and other speed limit data (track speed limit, train speed limit, temporary speed limit).

Under CBTC control modes, accidents A1, A2, A4 are all related to the protection that the train will never over pass its target point. The target point, together with the safe braking model, determines the speed limit for the train. These accidents happen when a train runs at a higher speed than the one could protect it from the fixed or mobile obstacles. Accident A3 relates to the train over speed as well, especially the speed limits for the track sections. Accident A5 specially relates to the train over speed inside the work zone, which often protects by the temporary speed limit. So the high level hazard considered here for these accidents is the train over speed hazard. This high level hazard can be further refined in considering different types of obstacles and different types of speed limits.

Another hazard related to accident A3 is the violation of route interlocking protection principles. The route should be locked before the train enters the interlocking and when the train is inside of the interlocking. The switches should also be locked when the track section containing the switch is occupied by a train. The conventional interlocking protection is provided by the interlocking system. This protection system is not developed here, but in order to achieve more close headway between trains, the interactions between wayside controller, train-borne controller and interlocking system are considered for the hazard analysis.

The high level hazard considered for accident A6 is related to door opening. This hazard can be further refined to train starts with door open, door opens when train is running, door cannot be opened in emergency situations, etc.

The high level hazards considered here are:

H1. Train over speed [A1], [A2], [A3], [A4], [A5]

H2. Violation of interlocking protection principle [A3]

H3. Door opening caused hazard [A6]

3.3.4. Environmental Assumptions

EA1. The track is designed for a maximum speed of TBD km/h.

EA2. The maximum physical speed for the rolling stock is TBD km/h.

EA3. High-integrity communications exist for the train control system.

EA4. Transponders are installed for absolute train position reference.

EA5. All trains have identification numbers for tracking purpose.

3.3.5. System Control Structure

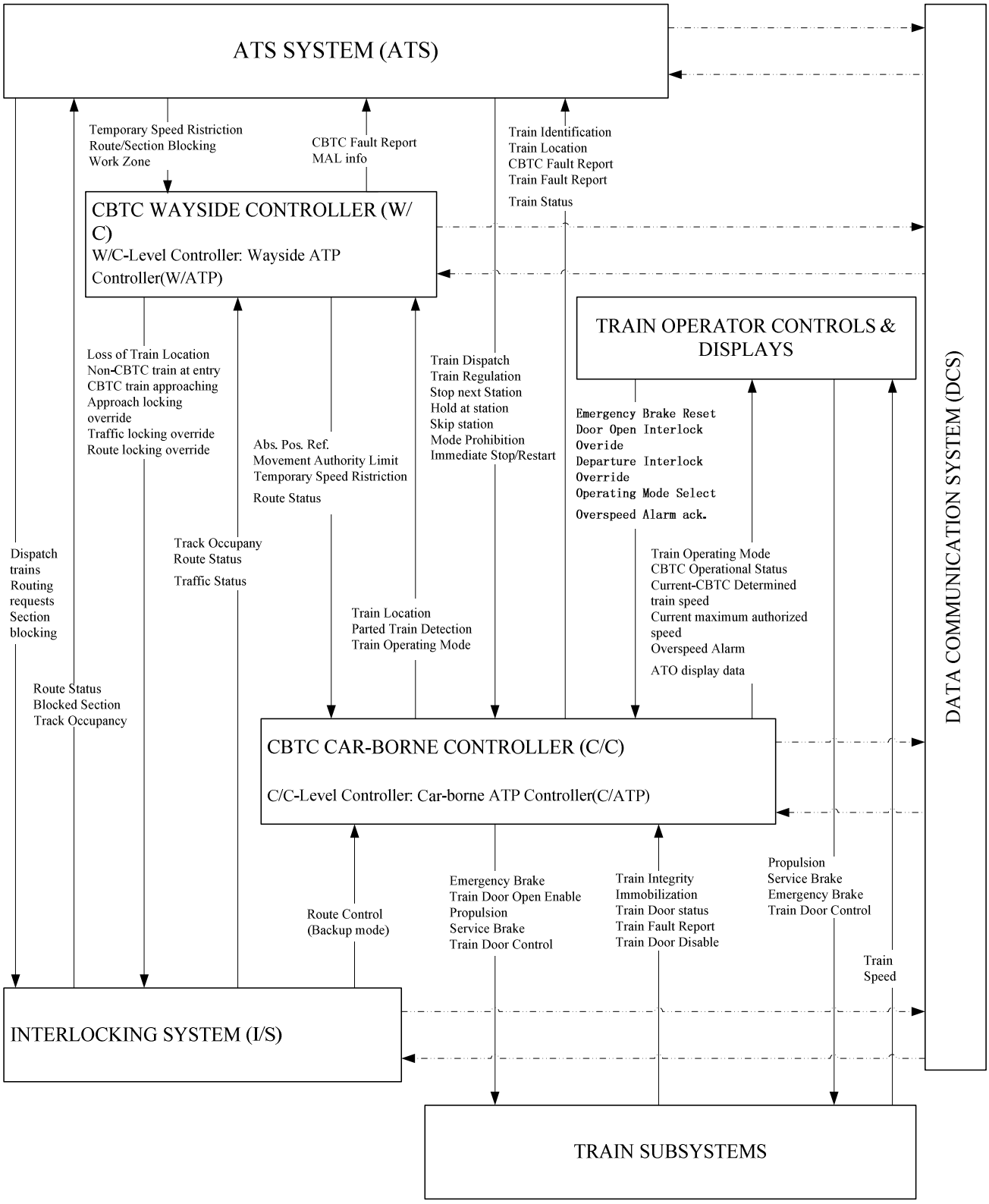
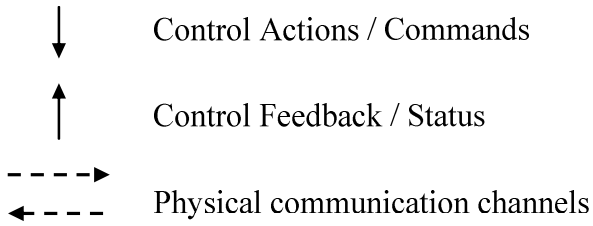


Figure 3-4. CBTC System Control Structure

Legend:



Functional Elements and Allocation:

1. ATS System (ATS)

   Functions Performed: Train identification; Train tracking; Train routing; Train regulation; and Station Stop. In the analysis here, only the function of setting temporary speed restriction is considered.

2. CBTC Wayside Controller (WC-ATP)

   Functions Performed: Limit of safe route determination; Limit of movement protection; External interlocking commands; Highway grade crossing warning device control; and Fixed ATP data management.

3. CBTC Train-borne Controller (TC-ATP)

   Functions Performed: Train Location determination; ATP profile determination; Authorized speed determination; Actual train speed/train travel direction determination; Supervise/enforce authorized speed and travel direction; Door control interlocks; Car-borne ATP user interface, and Fixed ATP data management.

4. Interlocking System (IS)

   Functions Performed: Performs routing for the train.

5. Train Operator Controls

   Functions Performed: Mode Selection and Manual Control of the train.

6. Train Subsystems

   Functions Performed: Train Control according to the commands it receives.

3.3.6. High Level Hazard Analysis

This section uses the STPA process to analyze each of the high level hazards. The two steps of STPA include identifying the potential for inadequate control of the system that could lead to a hazardous state and determining how each potentially hazardous control action could occur.

A controller can provide unsafe control in the following four ways:

1. A control action is not provided, missing or not followed;
2. A control action is provided but is wrongly provided;
3. A control action is provided at the wrong timing, earlier or later than the required timing, or out of sequence with other control actions.
4. For a control action which is a continuous signal, the control action is stopped too early or applied too long. [1]

For each hazard analysis, first tables are created listing all the unsafe control actions provided by controllers from the four ways we identified above. Then causal factors are considered in the three general categories: (1) the controller operation, (2) the behavior of actuators and controlled processes, and (3) communication and coordination among controllers and decision makers.

3.3.6.1. H1. Train Over-speed

Step 1 in STPA is to identify the potentially hazardous control actions. Based on the system control structure, tables 3-1, 3-2, 3-3, 3-4 analyze the possible unsafe control actions for all controllers related to train speed control.

Table 3-1. Unsafe Control Actions for ATS

Control Action	Not Providing Caused Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon or Applied Too Long
Temporary Speed Restriction	TSR not provided		TSR provided too late	

Table 3-2. Unsafe Control Actions for Wayside Controller (WC)

Control Action	**Not Providing Caused Hazard**	**Providing Causes Hazard**	**Wrong Timing/Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Absolute Position Reference	No position reference provided to the train	Wrong position reference provided to the train	Train read position data earlier or later than its actual position	No or wrong position reference provided to the train
Movement Authority Limit	No MAL provided to the train when the train is under CBTC control	Wrong MAL provided to the train	MAL calculated for the current train position provided too late	

Table 3-3. Unsafe Control Actions for Train-borne Controller (TC)

Control Action	**Not Providing Caused Hazard**	**Providing Causes Hazard**	**Wrong Timing/Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Emergency Brake	Emergency Brake should be executed but not		Emergency Brake provided too late	Emergency Brake stopped too soon.
Maximum allowed speed		Wrong maximum allowed speed provided	Maximum allowed speed updated too late	
Current train speed		Wrong current speed provided	Current speed updated too late	

Table 3-4. Unsafe Control Actions for Train Operator (TO)

Control Action	**Not Providing Caused Hazard**	**Providing Causes Hazard**	**Wrong Timing/Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Propulsion		Propulsion given when the train is not supposed to speed up		Propulsion applied too long
Brake	Brake not given when the train needs to slow down			Brake applied too short
Emergency Brake	Emergency Brake should be executed but not		Emergency Brake provided too late	

Step 2 of STPA is first to augment the control structure with process models and then to determine how hazardous control actions could occur. Figure 3-5 is the process model for train speed control. In this process model, ATS controls the setting of temporary speed restrictions (TSR) and the Wayside Controller determines the movement authority limit for the Train-borne Controller. The Train-borne Controller can then calculate the maximum authorized CBTC speed according to this movement authority limit, TSR, and fixed speed limits (train maximum speed limit and track maximum speed limit) which is set by its ATP data.

Based on the process models developed, the next step is to identify the causal factors for the hazards. For train speed control, there are three kinds of speed limits: one is the speed limit calculated by Train-borne Controller according to its target stopping point, one is the fixed speed limits set inside of the TC ATP parameters, such as track maximum speed and train maximum speed, and the other is the temporary speed restriction set in ATS. For clarity, in this STPA causal factor analysis, the temporary speed restriction controlled by ATS is separated from the other speed limit controls. Figure 3-6 is the causal factor analysis for train over speed due to incorrect TSR settings, and Figure 3-7 is the causal factor analysis for train over speed due to all other reasons.

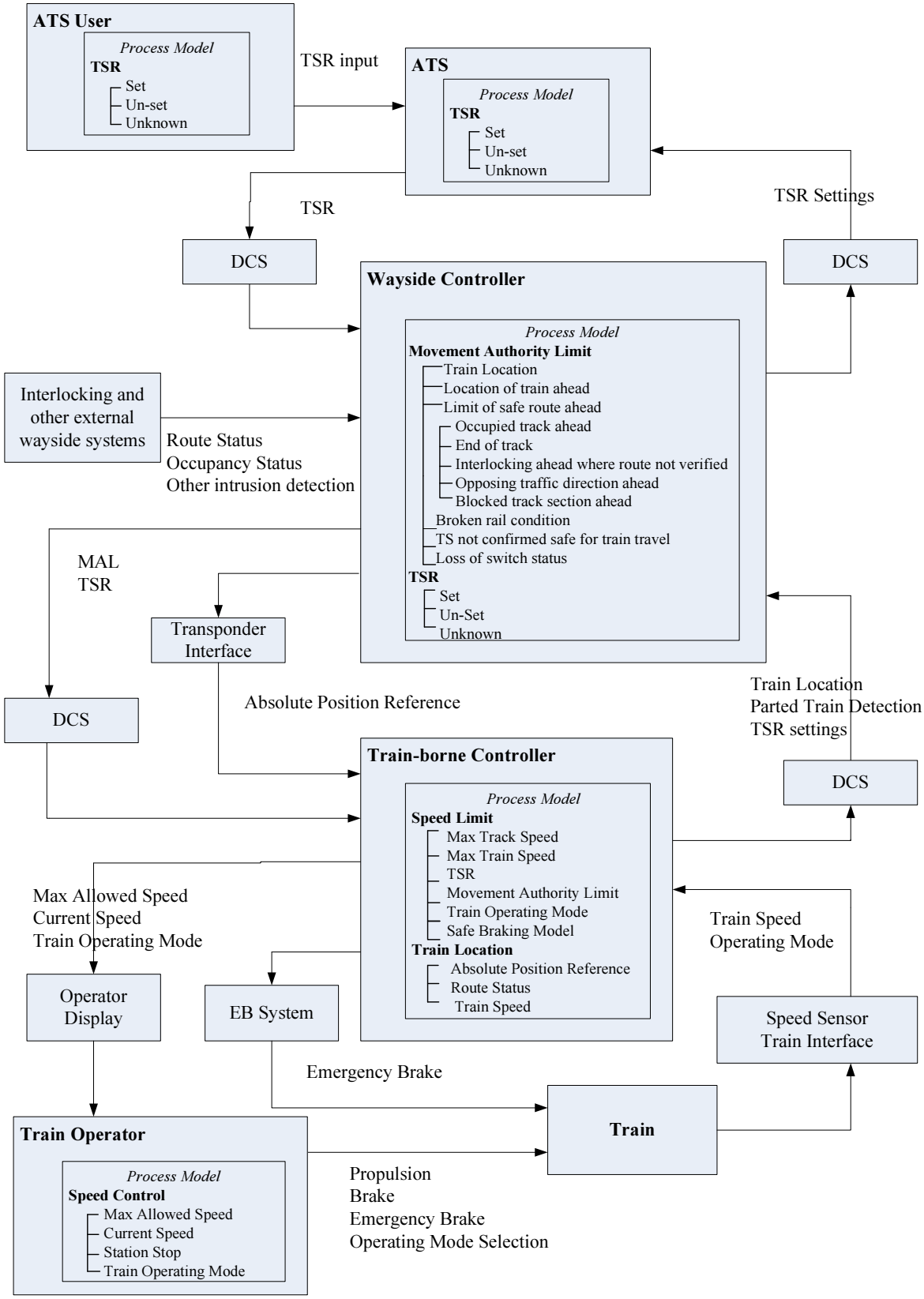


Figure 3-5. Process Model for Train Speed Control

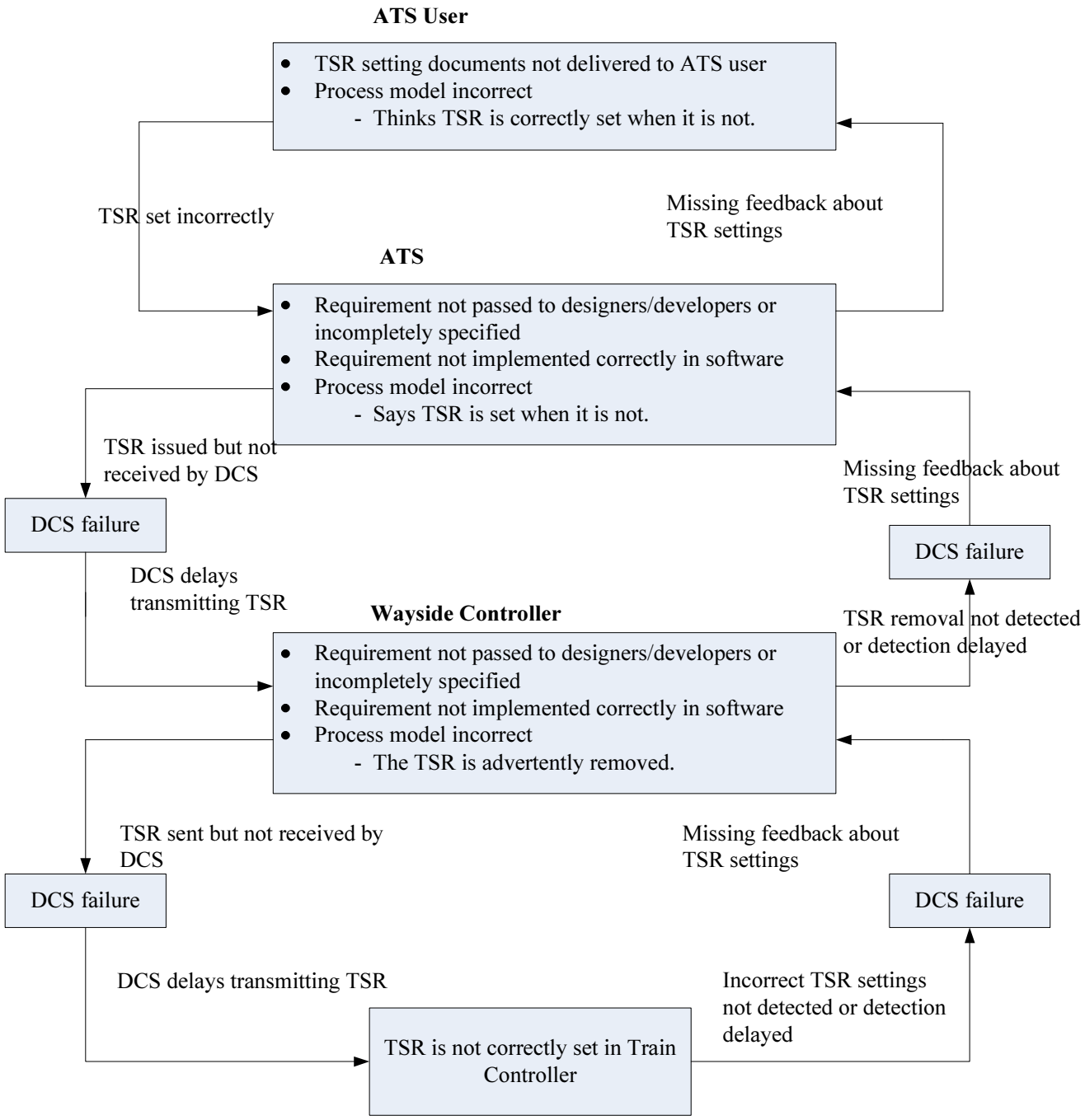


Figure 3-6. Causal Factor Analysis for TSR Settings in Train Speed Control

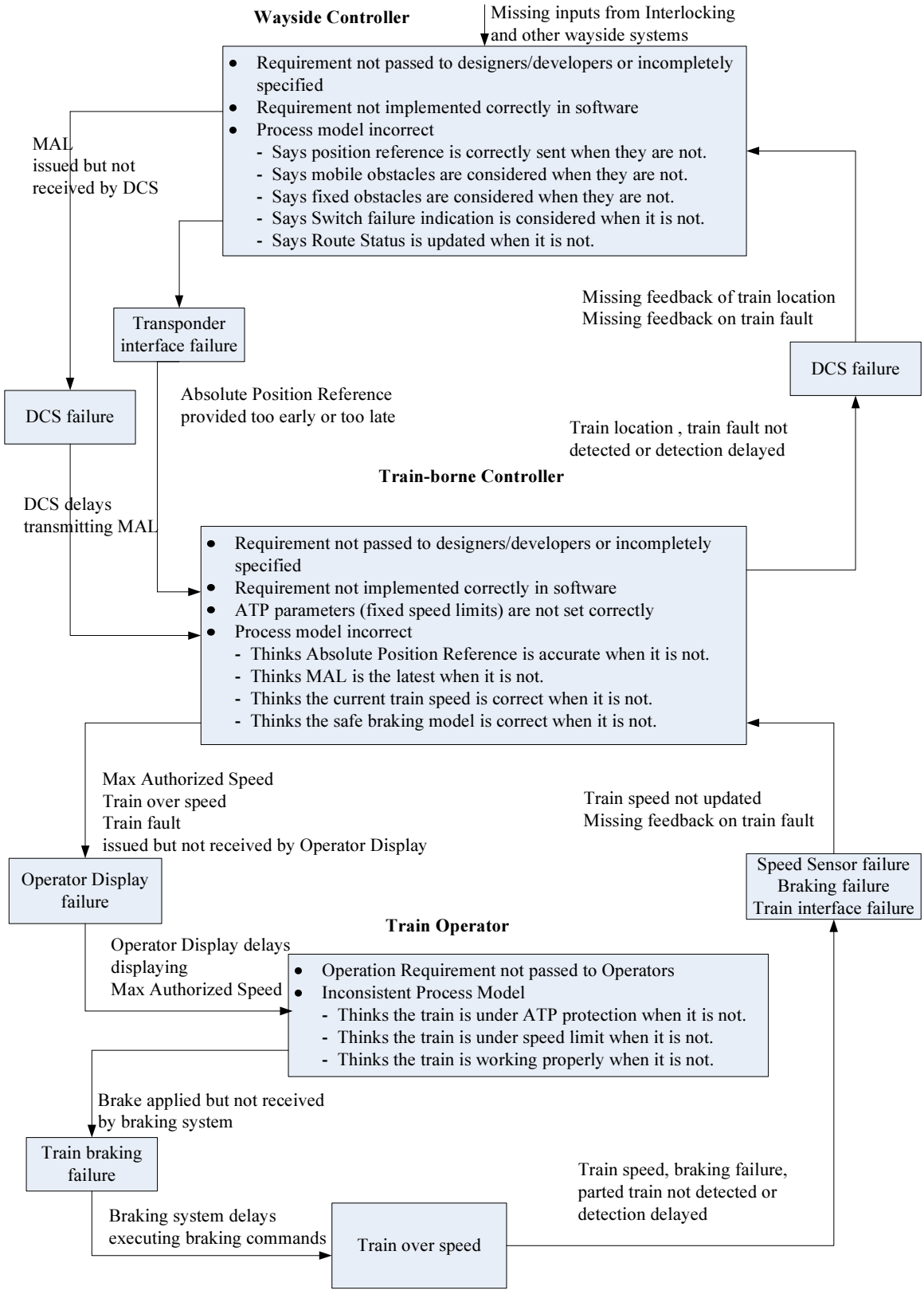


Figure 3-7. Causal Factor Analysis for Train Speed Control (without TSR) of H1

3.3.6.2. H2. Violation of Interlocking Protection Principle

By taking advantage of the CBTC train location determination, the CBTC system can permit early release of approach locking, traffic locking and route locking. The approach locking override allows an almost immediate requesting of a different route, following a cancelled signal. The traffic locking override permits head-to-head moves by two CBTC-equipped trains within traffic sections. The route locking override allows an earlier release of the route than by the conventional train occupancy detection.

The conventional interlocking protection provided by the interlocking system is not considered here, but these modified interlocking functions are initiated and controlled by the CBTC system. The hazards associated with these interactions are examined here. Table 3-5 identifies the unsafe control actions for the Wayside Controller, which issues these commands to modify the traditional interlocking functions. Figure 3-8 is the process model for the modified interlocking functions control. Figure 3-9 is the causal factor analysis for the hazard of violating interlocking protection principle.

Table 3-5. Inadequate Control Actions for Wayside Controller (WC)

Control Action	**Not Providing Caused Hazard**	**Providing Causes Hazard**	**Wrong Timing/Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Approach locking override		Approach locking override provided when criteria is not met		
Traffic locking override		Traffic locking override provided when criteria is not met.		
Route locking override		Route released when criteria is not met		

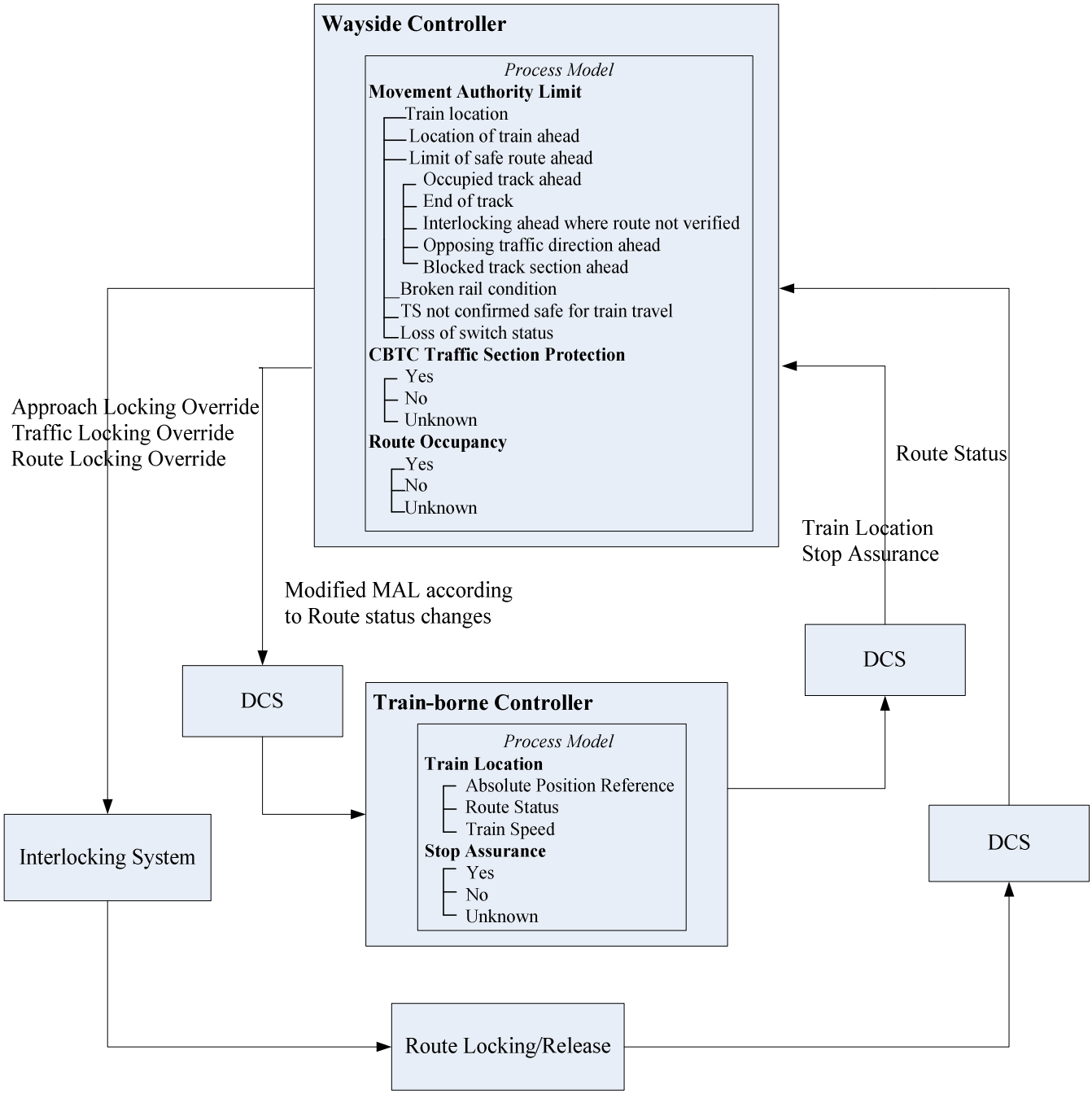


Figure 3-8. Process Model for Modifying Interlocking Functions Control

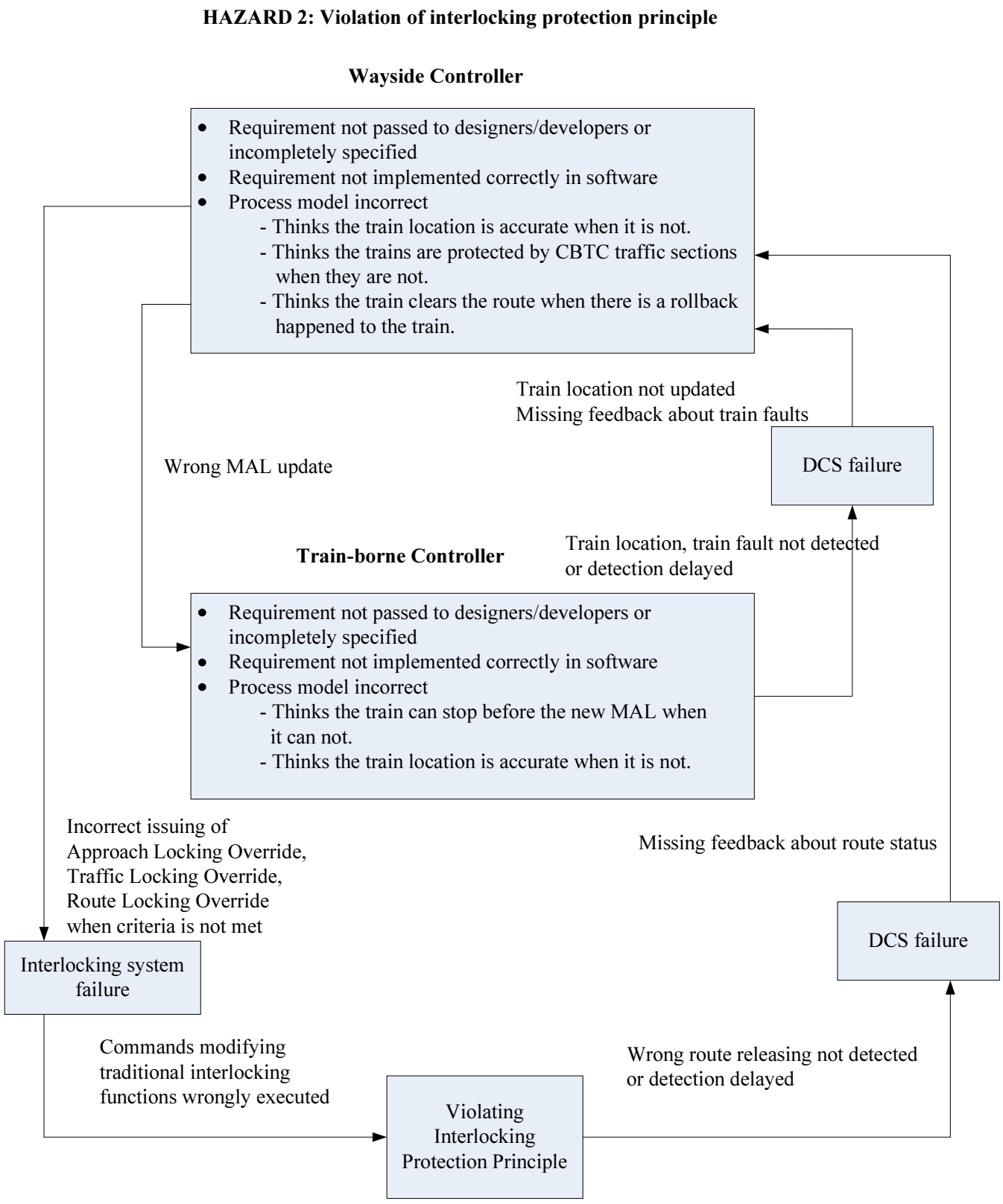


Figure 3- 9. Causal Factor Analysis of H2

3.3.6.3. H3. Door opens with train in motion or not aligned at platform

In manual control mode, the Train-borne controller provides the train door open enable signal only when the train is properly aligned at platform, the train is detected at zero speed, and the train is constrained against motion. Train doors can only be opened when the train door open enable signal is high, and the operator will open and close train doors by pushing buttons.

The high level hazard considered here is that train door opens when the train is in motion or when the train is not properly aligned at platform. Table 3-6 identifies the unsafe control action for the Train-borne Controller and table 3-7 identifies the unsafe control actions for the Train Operator. Figure 3-10 is the process model for the train door control in manual mode while figure 3-11 is the causal factor analysis for this hazard.

Table 3-6. Unsafe Control Actions for Train-borne Controller (TC)

Control Action	**Not Providing Caused Hazard**	**Providing Causes Hazard**	**Wrong Timing/Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Door Open Enable		Door Open Enable provided when criteria is not met		Door Open Enable Applied too long.

Table 3-7. Unsafe Control Actions for Train Operator (TO)

Control Action	**Not Providing Caused Hazard**	**Providing Causes Hazard**	**Wrong Timing/Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Door Open		Door Open provided when criteria is not met		
Door Close	Door Close not provided when train moves			

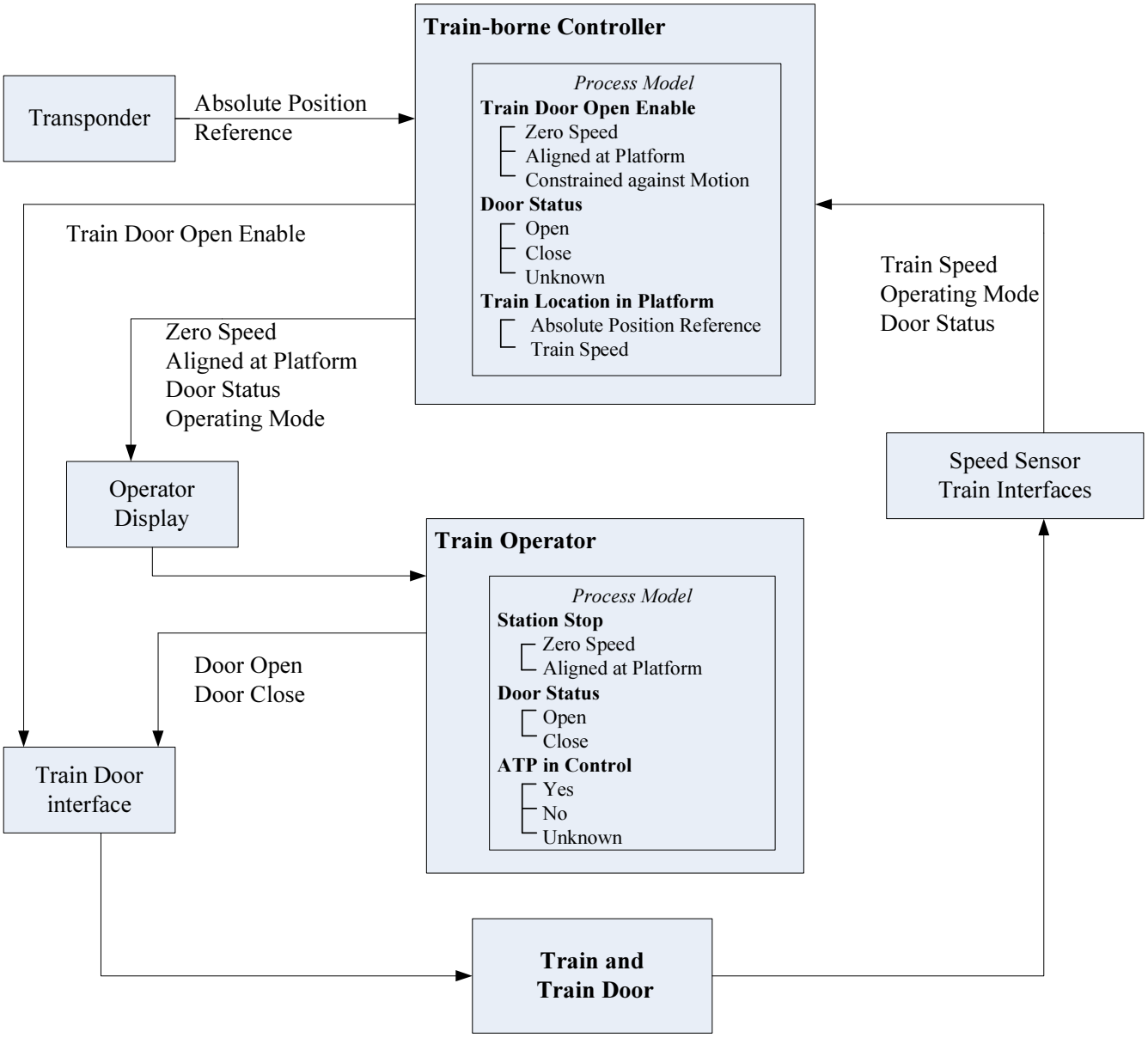


Figure 3-10. Process Model for Train Door Control

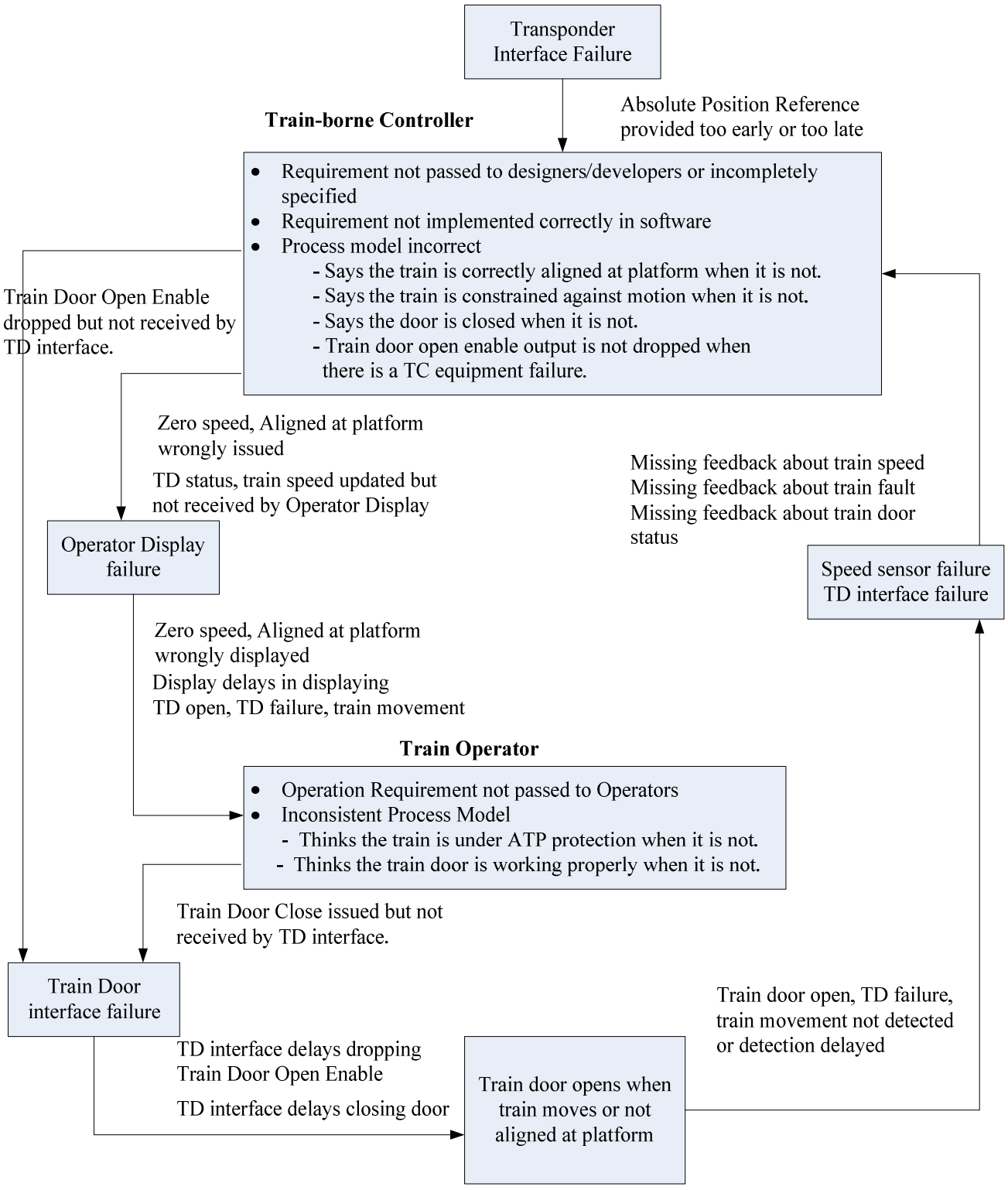


Figure 3-11. Causal Factor Analysis of H3

3.3.7. Hazard List and Hazard Log

3.3.7.1. H1. Train over-speed

System Element: ATS, WC-ATP, TC-ATP

Causal Factors:

ATS-CF1.1. The communication path between the ATS and the WC is broken.

ATS-CF1.2. The ATS believes the Track/Section Blocking settings are received by the WC when it is not.

ATS-CF1.3. The Track/Section Blocking settings are inadvertently removed by the ATS user.

ATS-CF2.1. The Track/Section Blocking is wrongly set by the ATS user.

ATS-CF3.1. The ATS believes the TSR settings are received by the WC when it is not.

ATS-CF3.2. The TSR settings are inadvertently removed by the WC.

ATS-CF4.1. The TSR is wrongly set by the ATS user.

WC-CF1.1. The communication path between the WC transponder and the TC reader is broken.

WC-CF2.1. The WC transponder is moved or replaced without updating its location data.

WC-CF3.1. The WC transponder transmits its location too early for the TC to read it.

WC-CF3.2. The WC transponder transmits its location too late for the TC to read it.

WC-CF4.1. The WC transponder transmitting window is too small for the TC to read it.

WC-CF4.2. The WC transponder transmitting window is too big caused the TC reads it too early or too late than its actual location.

WC-CF5.1. The communication path between the WC and the TC is broken.

WC-CF6.1. The WC does not receive the route status and switch position updates from the interlocking.

WC-CF6.2. The WC does not calculate the movement authority limit according to the most restrictive limit of safe route ahead.

WC-CF6.3. The WC does not identify the unknown mobile obstacles before the train.

WC-CF6.4. The WC does not identify the fixed obstacles in its track map.

WC-CF6.5. The TC does not update its location data.

WC-CF6.6. The TC sends the wrong location data.

WC-CF6.7. There is an unacceptable delay in TC sending its location data.

WC-CF6.8. The TC does not send its parted train information to the WC when the train is detected parted.

WC-CF7.1. There is an unacceptable delay in WC sending the movement authority limit.

WC-CF8.1. The WC does not receive the route status and switch position updates from the interlocking.

WC-CF9.1. There is an unacceptable delay in WC sending the route status to the TC.

TC-CF1.1. The TC uses the old movement authority limit to determine the target point.

TC-CF1.2. The TC uses the wrong safe braking model parameters of the train.

TC-CF1.3. The TC uses the wrong track map.

TC-CF2.1. There is an unacceptable delay in displaying the maximum allowed speed.

TC-CF3.1. The speed measurement of the train is not accurate.

TC-CF4.1. There is an unacceptable delay in displaying the current train speed.

TC-CF5.1. The link between TC and train braking system is broken.

TC-CF6.1. There is an unacceptable delay in TC issuing the command and the train executing the command.

TC-CF7.1. The Emergency Brake is incorrectly reset by the operator.

Safety Constraints:

The communication path between the WC and the ATS must not become broken or obstructed. (←ATS-CF1.1, →ATS-SC1)

The ATS must ask for confirmation if the Track/Section Blocking settings are received by the WC. (←ATS-CF1.2, →ATS-SC2)

The ATS must be able to prevent inadvertent removal of the Track/Section Blocking by the ATS user. (←ATS-CF1.3, → ATS-SC3)

The ATS must ask for confirmation of the correct settings of Track/Section Blocking from the ATS user. (←ATS-CF2.1, → ATS-SC4)

The ATS must ask for confirmation if the TSR settings are received by the WC. (←ATS-CF3.1, → ATS-SC5)

The ATS must be able to prevent inadvertent removal of the TSR settings by the ATS user. (←ATS-CF3.2, →ATS-SC6)

The ATS must ask for confirmation of the correct settings of TSR from the ATS user. (←ATS-CF4.1, →ATS-SC7)

The communication path between the WC transponder and the TC reader must not become broken or obstructed. (← WC-CF1.1, → WC-SC1)

The context of the WC transponder must be consistent with its location. (←WC-CF2.1, →WC-SC2)

The WC transponders must not transmit its signal too early for the train to read it before it arrives at the location. (←WC-CF3.1, →WC-SC3)

The WC transponders must not transmit its signal too late for the train to read it after it arrives at the location. (←WC-CF3.2, →WC-SC4)

The WC transponder transmitting window must not be too small that the TC cannot read the location data. (←WC-CF4.1, → WC-SC5)

The WC transponder transmitting window must not be too big that the TC read its location data too early or too late. (←WC-CF4.2, → WC-SC6)

The communication path between the WC and the TC must not become broken or obstructed. (←WC-CF5.1, →WC-SC7)

The communication path between the WC and the interlocking must not become broken or obstructed. (←WC-CF6.1, → WC-SC8)

The WC must calculate the movement authority limit according to the most restrictive of mobile and fixed obstacles ahead. (←WC-CF6.2, →WC-SC9)

The WC must be able to locate non-CBTC equipped trains, or trains with failed CBTC equipments, and other working trains according to requirements. (←WC-CF6.3, →WC-SC10)

The WC must use the most up to date track map. (←WC-CF6.4, →WC-SC11)

The WC must verify the time of the location data to ensure its validity in using it. (←WC-CF6.5, →WC-SC12)

The TC must send its updated location data to the WC every TBD seconds. (←WC-CF6.5, →TC-SC1)

The TC location data uncertainty must be within TBD meters. (←WC-CF6.6, →TC-SC2)

The TC location data transmission delay must be within TBD seconds. (←WC-CF6.7, →TC-SC3)

The TC must be able to detect parted train information and send it to the WC. (←WC-CF6.8, →TC-SC4)

The WC movement authority limit transmission delay must be within TBD seconds. (←WC-CF7.1, →WC-SC13)

The WC must verify the time of the route status and switch position to ensure their validity in using them. (←WC-CF8.1, →WC-SC14)

The WC must send the route status and switch position information to the TC within TBD seconds. (←WC-CF9.1, →WC-SC15)

The TC must verify the time of the movement authority limit to ensure the most up to date one is used to calculate the target point. (←TC-CF1.1, →TC-SC5)

The TC must ensure the correct safe braking model parameters are used for the maximum allowed speed calculation. (←TC-CF1.2, →TC-SC6)

The TC must ensure the correct track map is used for the maximum allowed speed calculation. (←TC-CF1.3, →TC-SC7)

The time delay in displaying the maximum allowed speed must be within TBD seconds. (←TC-CF2.1, →TC-SC8)

The TC speed measurement accuracy must be within TBD meters. (←TC-CF3.1, TC-SC9)

The time delay in displaying the current train speed must be within TBD seconds. (←TC-CF4.1, TC-SC10)

The link between TC and the train braking system must not be broken. (←TC-CF5.1, TC-SC11)

The delay between TC issuing the Emergency Brake command and the train executing the command must be within TBD seconds. (←TC-CF6.1, TC-SC12)

The TC must be able to prevent the Emergency Brake reset by operator when the conditions are not met. (←TC-CF7.1, TC-SC13)

3.3.7.2. H2. Violation of Interlocking Protection Principle

System Element: WC-ATP, Interlocking System, TC-ATP

Causal Factors:

WC-CF11.1. The WC thinks the train can stop before the cancelled signal when actually it cannot.

WC-CF12.1. There is an unidentified train in the traffic section which the WC failed to detect.

WC-CF12.2 There is a track circuit failure and there is non-communicating train over it.

WC-CF13.1. The WC process model determines the train has cleared the interlocking but there is a rollback happened to the train.

Safety Constraints:

The WC must not send the Approach Locking Override to the interlocking without getting confirmation from the TC that the train can stop. (←WC-CF11.1, →WC-SC16)

The WC must be able to locate non-CBTC equipped trains, or trains with failed CBTC equipments, and other working trains according to requirements. (←WC-CF12.1, →WC-SC10)

The WC must not send out the Traffic Locking Override to the interlocking if there is a track circuit failure and there is a suspected train over it. (←WC-CF12.2, →WC-SC17)

The WC must consider the worst case of the train roll back distance in deciding if the train has cleared the route or not. (←WC-CF13.1, →WC-SC18)

The TC must set a maximum allowed roll back distance for the WC to consider in deciding the train has cleared the route. (←WC-CF13.1, →TC-SC14)

The WC must not send out the Route Locking Override to the interlocking if there is a track circuit failure and there is a suspected train over it. (←WC-CF12.2, →WC-SC19)

3.3.7.3. H3. Door opens with train in motion or not aligned at platform

System Element: TC-ATP

Causal Factors:

TC-CF8.1. TC wrongly determines that the train is aligned at platform.

TC-CF8.2. TC wrongly determines that the train is at zero speed.

TC-CF9.1. TC does not stop output the Door Open Enable signal after the door is closed or after the train starts to move.

TC-CF9.2 There is a failure with TC and it doesn't drop the Door Open Enable signal to low.

Safety Constraints:

The TC must be able to determine the train is properly aligned at platform with a tolerance of TBD meters. (←TC-CF8.1, →TC-SC15)

The TC must be able to determine the train is at zero speed with a tolerance of TBD km/h. (←TC-CF8.2, →TC-SC16)

The TC must stop output Door Open Enable signal after the train door closes and after the train starts. (←TC-CF9.1, →TC-SC17)

In case of TC failure, the TC must be able to drop the Door Open Enable signal to low. (←TC-CF9.2, →TC-SC18)

3.3.8. High-Level Safety Constraints

CBTC system must protect the train from running over-speed inside of the CBTC territory. (←H.1)

CBTC system must not cause hazard to passengers associated with train door control. (←H.3)

3.3.9. High-Level Requirements

To refine the goals into testable and achievable high level requirements:

HLR.1. CBTC system shall allow safe train operation with the minimum mainline headway of TBD seconds between trains. (←G1, G2)

HLR.2. CBTC system shall provide train location determination within the uncertainty of TBD meters. (←G1, G2)

HLR.3. CBTC system shall provide automatic train separation and over speed protection for any trains running inside the CBTC territory under the maximum civil and train speed allowed. (←G2)

HLR.4. CBTC system shall provide automatic passenger protection for any trains running inside the CBTC territory under the maximum civil and train speed allowed. (←G3)

3.4. Level 1.1: ATS Goals, Requirements, and Constraints

3.4.1. ATS Goals

ATS-G1. Protect work crews and working trains. (←H1)

3.4.2. ATS Safety Constraints

ATS-SC1. The communication path between the WC and the ATS must not become broken or obstructed. (←H1)

ATS-SC2. The ATS must ask for confirmation if the Track/Section Blocking settings are received by the WC. (←H1)

ATS-SC3. The ATS must be able to prevent inadvertent removal of the Track/Section Blocking by the ATS user. (←H1)

ATS-SC4. The ATS must ask for confirmation of the correct settings of Track/Section Blocking from the ATS user. (←H1)

ATS-SC5. The ATS must ask for confirmation if the TSR settings are received by the WC. (←H1)

ATS-SC6. The ATS must be able to prevent inadvertent removal of the TSR settings by the ATS user. (←H1)

ATS-SC7. The ATS must ask for confirmation of the correct settings of TSR from the ATS user. (←H1)

3.5. Level 1.2: Wayside Controller (WC-ATP) Goals, Requirements, and Constraints

3.5.1. Wayside Controller (WC-ATP) Goals

WC-G1. Provide vital train separation protection. (← H1)

WC-G2. Achieve closer headways between trains. (←H1, ←H2)

3.5.2. Wayside Controller (W/C-ATP) Safety Constraints

WC-SC1. The communication path between the WC transponder and the TC reader must not become broken or obstructed. (←H1)

WC-SC2. The context of the WC transponder must be consistent with its location. (←H1)

WC-SC3. The WC transponders must not transmit its signal too early for the train to read it before it arrives at the location. (←H1)

WC-SC4. The WC transponders must not transmit its signal too late for the train to read it after it arrives at the location. (←H1)

WC-SC5. The WC transponder transmitting window must not be too small that the TC cannot read the location data. (←H1)

WC-SC6. The WC transponder transmitting window must not be too big that the TC read its location data too early or too late. (←H1)

WC-SC7. The communication path between the WC and the TC must not become broken or obstructed. (←H1)

WC-SC8. The communication path between the WC and the interlocking must not become broken or obstructed. (←H1)

WC-SC9. The WC must calculate the movement authority limit according to the most restrictive of mobile and fixed obstacles ahead. (←H1)

WC-SC10. The WC must be able to locate non-CBTC equipped trains, or trains with failed CBTC equipments, and other working trains according to requirements. (←H1)

WC-SC11. The WC must use the most up to date track map. (←H1)

WC-SC12. The WC must verify the time of the location data to ensure its validity in using it. (←H1)

WC-SC13. The WC movement authority limit transmission delay must be within TBD seconds. (←H1)

WC-SC14. The WC must verify the time of the route status and switch position to ensure their validity in using them. (←H1)

WC-SC15. The WC must send the route status and switch position information to the TC within TBD seconds. (←H1)

WC-SC16. The WC must not send the Approach Locking Override to the interlocking without getting confirmation from the TC that the train can stop. (←H2)

WC-SC17. The WC must not send out the Traffic Locking Override to the interlocking if there is a track circuit failure and there is a suspected train over it. (←H2)

WC-SC18. The WC must consider the worst case of the train roll back distance in deciding if the train has cleared the route or not. (←H2)

WC-SC19. The WC must not send out the Route Locking Override to the interlocking if there is a track circuit failure and there is a suspected train over it. (←H2)

3.6. Level 1.3: Train-borne Controller (TC) Goals, Requirements, and Constraints

3.6.1. Train-borne Controller (TC-ATP) Goals

TC-G1. Protect trains from running over speed. (←H1)

TC-G2. Achieve closer headways between trains. (←H1, H2)

TC-G3. Protect passengers from door related hazards. (←H3)

3.6.2. Train-borne Controller (TC-ATP) Safety Constraints

TC-SC1. The TC must send its updated location data to the WC every TBD seconds. (←H1)

TC-SC2. The TC location data uncertainty must be within TBD meters. (←H1)

TC-SC3. The TC location data transmission delay must be within TBD seconds. (←H1)

TC-SC4. The TC must be able to detect parted train information and send it to the WC. (←H1)

TC-SC5. The TC must verify the time of the movement authority limit to ensure the most up to date one is used to calculate the target point. (←H1)

TC-SC6. The TC must ensure the correct safe braking model parameters are used for the maximum allowed speed calculation. (←H1)

TC-SC7. The TC must ensure the correct track map is used for the maximum allowed speed calculation. (←H1)

TC-SC8. The time delay in displaying the maximum allowed speed must be within TBD seconds. (←H1)

TC-SC9. The TC speed measurement accuracy must be within TBD meters. (←H1)

TC-SC10. The time delay in displaying the current train speed must be within TBD seconds. (←H1)

TC-SC11. The link between TC and the train braking system must not be broken. (←H1)

TC-SC12. The delay between TC issuing the Emergency Brake command and the train executing the command must be within TBD seconds. (←H1)

TC-SC13. The TC must be able to prevent the Emergency Brake reset by operator when the conditions are not met. (←H1)

TC-SC14. The TC must set a maximum allowed roll back distance for the WC to consider in deciding the train has cleared the route. (←H1, H2)

3.7. Comparison with the IEEE 1474 PHA requirements

Per requirement in IEEE Std 1474.1-2004, "The PHA (Preliminary Hazard Analysis) shall consider the following for identification and evaluation of hazards, as a minimum:

1. Hazardous components (e.g. fuels, propellants, lasers, toxic substances, hazardous construction materials, pressure systems, and other energy sources).

2. Safety-related interface considerations among various elements of the system (e.g. material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls) ……

3. Environmental constraints, including the operating environments (e.g. drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects).

4. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g. human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors, such as equipment layout, lighting requirements, potential exposures to toxic materials; effects of noise or radiation on human performance)……

5. Facilities, real property installed equipment, support equipment (e.g. provisions for storage, assembly, checkout, proof/testing of hazardous systems/assemblies that may involve toxic,

flammable, explosive, corrosive, or cryogenic materials/wastes; radiation or noise emitters; electrical power sources), and training (e.g. training and certification pertaining to safety operations and maintenance).

6. Safety-related equipment, safeguard, and possible alternate approaches (e.g. interlocks, system redundancy; fail-safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).

7. Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed. ” [8]

Comparing with these isolated requirements, STPA is a more systematic approach to the hazard analysis. It does not start from hazardous components, equipments, malfunctions; rather it starts from the accidents and the hazardous states. It is a top down approach to encompass all the causal factors that could lead to the hazardous states. It does not consider any components, equipments or function failures independently, rather it considers the system as a whole with a focus on inadequate control actions at each level of the control structure.

While all kinds of hazardous components or environments can be included in the hazard definition, system safety defines hazards as within the system being designed but not in its environment alone. An accident is considered to be caused by a hazardous state or condition of the system combined with its environment. The STPA hazard analysis starts from accidents, using a top down approach, to identify hazards, inadequate control actions, causal factors and reaches the safety constraints.

In the new systems theory view of safety, high reliability is neither necessary nor sufficient for safety. Bottom-up reliability engineering analysis techniques, such as FMEA, are not appropriate for safety analysis. Even top-down techniques, such as fault trees, if they focus on component failure, are not adequate [Leveson, Safer World] Instead of relying on system redundancy, the STPA process aims to eliminate or control the system hazards through eliminating the unsafe control actions, which is reached by examining the control loop and the process models. System redundancy will only add more interactions into the system but will not eliminate the unsafe control actions by itself. The system as a whole has to be examined.

4. Conclusion and Future Work

In analyzing accidents, STAMP provides more insights into investigating the whole socio-technical system through examining the control structure. In the 7.23 train accident analyzed in Chapter 2, the STAMP model helps identify more inadequate controls inside of the control structure, from the physical process to management, to the overall communication and coordination and to the safety culture of the China Railway system.

Together from the CAST and STPA analysis, we are able to identify more inadequate controls and needed improvements in the following areas:

1. Physical Process Analysis: Not only the fail-safe design should be applied, the overall physical system control needs to be examined. As one example, data communication failure was only mentioned as a result of lightening and GSM-R dispatching communication interruption was not mentioned at all in the accident investigation report. After the CAST analysis, we understand how these inadequate controls have contributed to the accident. While in STPA analysis, one of the safety constraints we developed is "the communication path between the controller (ATS, WC, etc.) and the controlled process (WC, TC, etc.) must not become broken or obstructed." We have to enforce these safety constraints in our system design to eliminate the safety hazards. Fail-safe design is just not enough.

2. System Interactions Analysis: Using STAMP, in the dysfunctional interactions analysis in the physical process, we discovered that within the 7 minutes the leading train stopping on the track, the onboard ATP was just waiting for a code from the track circuit to start the train in OS mode. We think this interface needs to be further investigated: If conditions are not met to run the train in full ATP control, what is the benefit of not letting it start in OS mode in which the operator is supposed to have full safety control over the train? We think this interface is not safe for this kind of hazardous situation and should be re-designed. Again, this suggests the need to use STPA in hazard analysis to encompass all kinds of accident scenarios.

3. Mental Model and Process Model Analysis: Using the mental model analysis in STAMP, we understand how the inconsistent mental models within the CTC dispatcher and the station operator prevented them from taking more restrictive actions in controlling the following train. This not only contributed to our understanding of the accident, it also provides important insights in designing the system. In STPA analysis, we try to identify all the inconsistent process models in the systems which can cause bad implementation of the system, or inconsistent mental models which cause people make bad decisions, and design the system to eliminate these inconsistencies.

4. Management and Organizational Analysis: From the CAST analysis, we discovered the conflicts between safety and schedule pressure and performance pressure, which caused the degradation in safety efforts. We recommended establishing a safety organization in the highest level of the control structure. This safety organization must be free from project development pressure and the train operation pressure, so it can oversee and control safety more effectively.

5. Overall Communication and Coordination Analysis: From the CAST analysis, we were able to identify the missing communications between the system design team and the system operation team. The operation assumptions should be delivered to the operations team, so the operators can

make informed decisions. And operational failures should be provided back to the design team for the system to be improved.

6. Safety Culture: To create a strong safety culture in China Railway system, we recommend examining each aspect of the existing safety practices and looking at them dynamically. One example was given on analyzing the safety policy of punishment: From the systems dynamics model analysis, we concluded that contradictory to the management expectations, there exists "policy resistance" that may damage the effectiveness of the policy.

Using the control structure has contributed to all of the above analysis. It not only helps in analyzing the physical system, it also helps in analyzing the management system. By creating the control structure, we can understand very clearly how the system elements interact with each other, how the controller controls the process one level below, and how the controlled process provides feedback to the controller. The safety constraints can thus be developed from these control actions and the process models we analyzed. As we can see from the examples, the control structure is much more useful in understanding the system than the block diagrams.

In summary, the STAMP accident analysis provides us insights on how the inadequate control can happen within the safety control structure, how the safety constraints are violated and how the inconsistent process model can impact the behavior of the controllers. Rather than focusing on finding the root causes of the accidents, the CAST model focuses on building a strong safety control program.

By focusing on first identifying the inadequate control and bad implementations and then identifying the causal factors, STPA can actually be very comprehensive in encompassing all kinds of accident scenarios. The safety constraints can then be implemented in the system design.

The work here only provides a preliminary hazard analysis with a focus on the ATP part of the system. Further work can be done to include more subsystems, to design for human controllers, and to refine the hazards and hazards analysis by continuing to the lower levels of the intent specification.

5. Appendix

5.1. A. Comparison with the MIT STAMP/STPA workshop presentation

Here is the comparison between what I have done and the presentation from the workshop:

1. *Control Structure*: According to the general socio-technical control structure developed by Leveson, we both developed the control structure including System Development and System Operation; but the organizations inside of the system design are different. I limited the organizations to the signaling and train control development companies, because this was a signaling and train control accident, and the system was developed by the signaling and train control companies. In Suo's presentation, Shanghai Railway Bureau (responsible for the system operation) and Coastal Railway Zhejiang Co. (responsible for the construction of the Yong-Tai-Wen railway) were also included in the system design part of the control structure.

2. *Physical Process Analysis*: In this thesis, physical process includes all the physical processes involved in the accident: the CTC dispatching center, the TCC station equipment, the wayside equipment and the onboard train control equipment. In Suo's presentation, physical process (Level 1) only included the high speed train, onboard ATP and the driver.

3. *Operation Process Analysis:* In this thesis, operation process includes all involved in the operation of the system: the CTC dispatcher, the station operator and the train operator. In Suo's presentation, operation process (Level 2) included the CTC dispatcher, the TCC, Watch keeper, and track circuits.

4. *Management Level Analysis:* In this thesis, management level analysis includes the project development and management of CRSCD, corporate level management of CRSC, Shanghai Railway Bureau and MOR. In Suo's presentation, Management Level Analysis (Level 3) included MOR and Shanghai Railway Bureau only.

5. *Dynamics of the Accident:* In this thesis, I focused on the dynamics directly related to the decrease in safety efforts that eventually led to the accident, which are the system development schedule and the schedule and image pressure of the system operation. In Suo's presentation, he put more emphasis on the dynamics of Zhejiang high-speed railway construction and the province's economic development.

6. *Safety Culture:* A system dynamic model in analyzing whether policies promote or damage a safety culture is presented in this thesis. This point is not mentioned in Suo's presentation.

7. *Recommendations:* In this thesis, more specific recommendations are provided for each level of the control structure based on the previous analysis. In Suo's presentation, more general recommendations were provided.

References

[1]. Leveson, N., Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2012.

[2]. Investigation Report of “7.23 Yong-Wen Severe Railway Transportation Accident”, 2011-12-25.

[3]. MOR, CTCS-2 Train Control Center Technical Specification, 2007. [4]. CaiXin New Age, vol.34, 2011, 2011-08-29, http://magazine.caixin.com/2011-08-27/100295430_all.html#page2.

[5]. China News Week, “Review of the 7.23 high speed train crashes”, 2011-07-29, http://focus.news.163.com/11/0729/09/7A4BVKOA00011SM9_3.html.

[6]. LiJia, Introduction to the Yong-Tai-Wen Railway Communication and Signaling System Integration.

[7]. Fleming C., et al, Safety Assurance in Next Gen (Technical Report for NASA Contract NNL10AA13C0, 11/30/2011.

[8]. IEEE Std 1474.1-2004, IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements.

[9]. IEEE Std 1474.2-2003, IEEE Standard for User Interface Requirements in Communications-Based Train Control (CBTC) Systems.

[10]. IEEE Std 1474.3-2008, IEEE Recommended Practice for Communications-Based Train Control (CBTC) System Design and Functional Allocations.

[11]. Owens, B., et al, Safety-Driven Model Based System Engineering Methodology Part II: Application of the Methodology to an Outer Planet Exploration Model, December 16, 2007.

[12]. Spencer, M., et al, Technical Memo: An Analysis of In-Trail Procedure Safety Requirements, December 29, 2011.

[13]. John D. Sterman, Business Dynamics, Systems Thinking and Modeling for a Complex World, Irwin McGraw-Hill, 2000.

[14]. Dajiang Suo, A System Theoretic Analysis of the “7.23” Yong-Tai-Wen Railway Accident, STAMP/STPA Workshop, April 2012

[15]. MOR, CTCS General Technical Specifications, 2004.

[16]. Xu Xiaoming, CTCS-2 Train Control Center, China Railway Press, 2007.

[17]. IEC62278:2002, Railway applications: Specification and demonstration of reliability, availability, maintainability and safety (RAMS).

[18] IEC62279:2002, Railway applications: Communications, signaling and processing systems – Software for railway control and protection systems.

[19] IEC62280:2002, Railway applications: Communication, signaling and processing systems – Safety related electronic systems for signaling.