A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident

Dajiang Suo

Computer Science and Technology Dept.
Tsinghua University, 100084, Beijing, China
sdj08@mails.tsinghua.edu.cn

Abstract: This paper seeks to analyze the "7.23" Yongwen Railway accident in China from a system theoretic perspective. In particular, the STAMP safety control structure for this accident has been constructed and divided into two respective processes including system development and operation, which are then analyzed at each level. Furthermore, to understand why and how the system evolved over time, system dynamics models are constructed to describe the changes indirectly leading to the accident. As could be seen, this analysis raises some questions which are not included in the investigation report but critical to the comprehensive understanding of the accident. Based on the analysis results, recommendations are generated aiming at preventing the same kind of accidents in the future.

1 Introduction

On July 23rd, 2011, at 20:31, a train accident took away nearly 40 people's life on the Yong-Tai-Wen High-Speed coastal railway line, Zhejiang province, Southeast of China (Figure 1). The High-Speed train D301 rear-ends the D3115 with the speed of 99 kilometers per hour. Six cars derailed and two of them went off a bridge 50 feet above the ground. It is considered to be the most serious railway accident in the development of Chinese railway history.

At first, the accident was attributed to failures of the Track Circuit and its interface with the Train Control Center (TCC), which is proved to be struck by lightening hundreds of times in the evening of July 23rd. This resulted in the data acquisition board in the TCC failing to collect the consistent information of the Track Circuit occupancy and identify the correct position of the D3115 (Figure 1). Therefore, it transmitted erroneous signal to the signal lights. Also, the investigation board in the final report [1] claimed that human operators of the Shanghai Railway Bureau also contributed to make the conditions worse, as well as the poor supervision in the Railway system and the contractor of the signal&communication system.

Nevertheless, as Leveson [3] pointed out, if the purpose of accident analyses is to find the "root cause" or someone to blame, in this case the failures in the signal device, the dispatcher and the watch keeper, we might lose the potential opportunities to maximize what can be learned from the accident. In fact, if the scheduling system had operated as expected during the emergency, the hazard appeared in the Track Circuit 5829 could have been prevented. From a system theoretic perspective, poor coordination and communication between multiple controllers (TCC, watch keeper and the dispatcher) played a critical role in leading to the hazards involved. Besides, dynamic changes lead by scheduling pressures increase the risk behaviors of personnel in the

railway system, thus making the emergency response mechanism as a whole vulnerable to potential risks.

Before analyzing the accident in great detail, several concepts need to be presented first. In general, the control system related to this accident is the Chinese Train Control System 2 (CTCS2). It is designed to meet the requirements by the Chinese High-Speed train with the speed more than 200km/h. In general, it is consisted of four parts [2]:

Centralized Traffic Control (CTC) – It receives information related to current situation of the railway line (e.g. track occupancy and status of electrical and mechanical components) and issues dispatching commands to the TCC.

Train Control Center (TCC) – It is the ground control center of train control information located at each station and has three functions. Firstly, it collects route information and device status from the signal system on the ground (e.g. Track Circuit) and receives the operation and schedule information from the CTC. By using this information, it generates train control information through logic calculation. Also, the status of the signal device on the ground and the

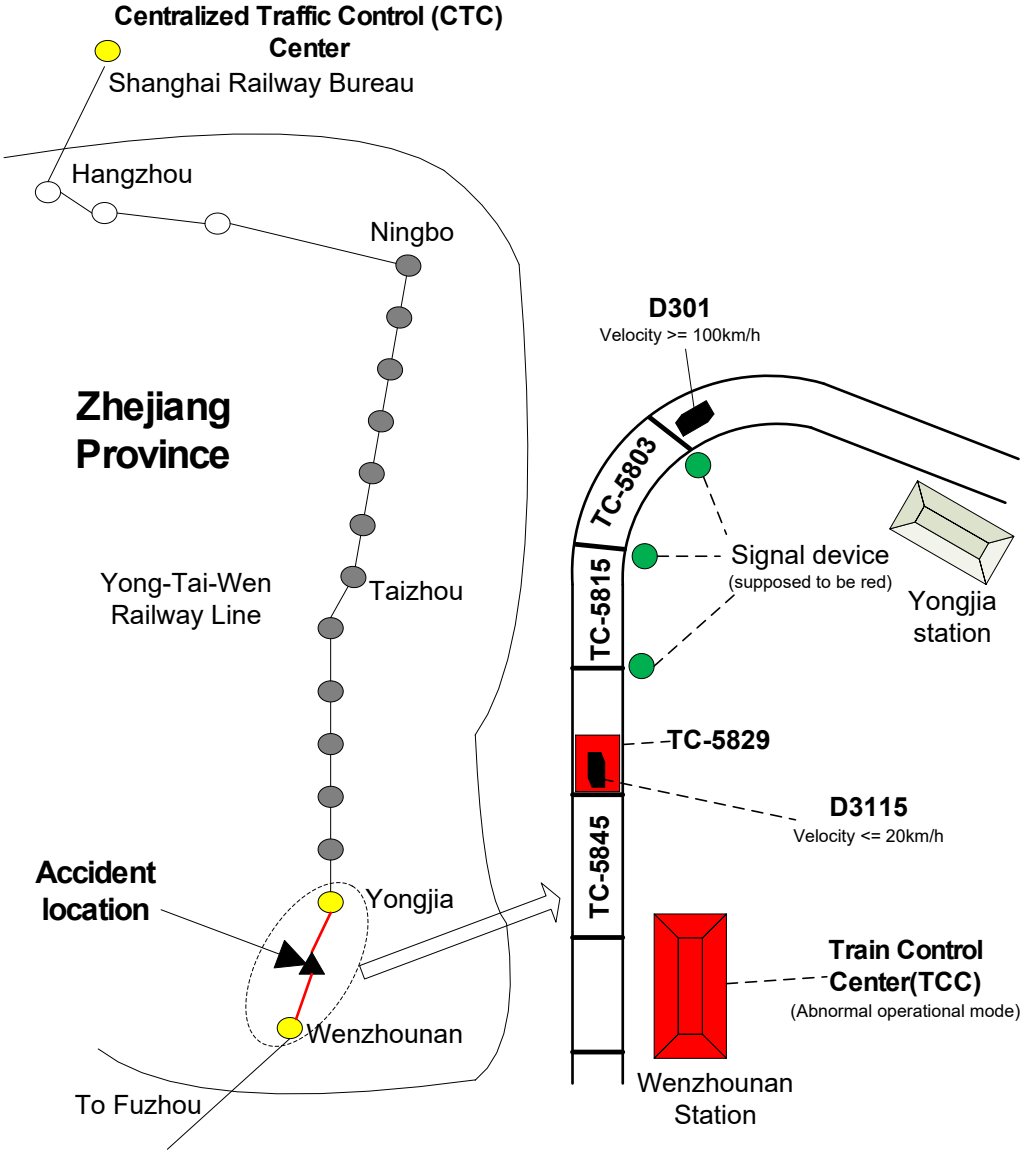


Figure 1. The location of the accident and its surrounding environment

train status would be transmitted to the CTC. In addition, it transmits these control information to on-board devices through signal device on the ground. As pointed out that “Train control center is the ground logic control center and vital signal device.” [2]

Ground signal system – It serves as the intermediary between the TCC and the on board device, which includes Track Circuit (inspecting railway track occupancy), signal device (directing the driver in abnormal operational mode and warning), Track relay (transmit signal between TCC and signal device and Track circuit) and LEU& Active Transponder (ground-to-train information transmission system). For simplicity, the ground signal system in this paper was referred to as Track Circuit used for transmitting signal and monitoring track occupancy. In fact, in the final investigation report the ground system equals to the Track Circuit.

Automatic Train protection (ATP) – It is the on-board device which could be used to realize over-speed protection. “It receives line data, speed limit ahead, operation status ahead, and route information from the ground, and then combines with train parameters to produce train operation protection control parameters” [2]. One thing should be addressed is that the ATP would stop the train immediately if it detects errors or failures in the Track Circuit. According to the investigation report, the Train D3115 failed to restart until 2 minutes before the accident because the ATP detected erroneous signal from the Track Circuit.

Besides, several important concepts of operations of the railway line should also be defined clearly:

Red light strip (shown in Figure 1) – In the displays of the TCC, it often represents the occupancy of the Track Circuit by the train. But sometimes the abnormality in the Track Circuit may lead to red light strip. Therefore, the appearance of the “Red light strip” indicates that a particular track section is occupied by a train or its related track Circuit is failed.

Occlusive section – to protect the High-Speed train from rear-end, the approach called occlusive section driving has been taken on the High-Speed railway line. The railway line is divided into many occlusive sections on each of which only one train could run, thus keeping a safe distance between two trains.

Decentralized autonomous control mode (DACM) – in this mode, the dispatcher controls the operation of the train directly. He issue control command through CTC, which will transmit the signal to TCC through Track Circuit. After receiving command from the Track Circuit, the ATP on the train will calculate control parameters to decide the speed of the train.

Unconventional station control mode (USCM) – During emergency situations (e.g. Red strip failures or abnormal conditions in TCC and CTC), the Train control system will change from DACM to this mode and the Watch keeper in each train stations will be responsible for scheduling the train including the entering and leaving the station and deciding the speed of the train.

On-sight mode – In this mode, the driver controls the train by himself. Normally, this train runs with the speed less than 20 kilometers per hour. Before the accident, the train D3115 had difficulties in transiting to this mode three times, which caused the train stopped more than 8 minutes.

As mentioned before, human operators also played critical role in the normal operation of the train. It is the watch keeper in the Wenzhou station who did not perform procedures after the failure of TCC according to regulations in the Unconventional station control mode. Moreover, the dispatcher in Shanghai Railway Bureau failed to identify that D3115 was in Track Circuit 5829 because of erroneous signal from Track circuit, so he did not notify D301 to decelerate.

2 The Related Basic Events

Both D3115 and D301 were behind schedule and reached Yongjia railway station at 19:51 and 20:12, respectively. The Railway station changed its operational mode from automatic control to abnormal control (man-control) because of a failure in the track circuit. A “Red-Light strip”, which represents the occupancy of the railway section, appeared in the monitor of the CTC, but actually there was no train in that section. At 20:14, D3115 left Yongjia station and reached 5829AG at 20:21. Due to the failure of Track circuit, it stopped automatically for nearly eight minutes and failed to restart until 20:29. After that it kept running at the speed almost 20 kilometers per hour according to the railway regulation under abnormal conditions. At the same time, D301 also left from Yongjia station to Wenzhounan station at 20:24 and was supposed to decelerate when it received signals from the Track circuit or encountered the red light of the signal device. Unfortunately, failures in the TCC made erroneous signal sent to D301 and the signal light, indicating that there was no train in section 5829 and the signal lights in section 5815 and 5803 turned green. As a consequence, D301 did not stop or decelerate at Section 5815 and 5803 (As shown in Figure 1).

Although the failure in the signal system lead to the erroneous signal transmitting to the driver in man-control mode, the watch keeper in the railway station and the dispatcher should have found the abnormal situation and respond to it immediately. However, no one realized the hazards from 20:24, when D301 left Yongjia station to 20:31, when it crashed into D3115. The investigation board first attributed the accident to the defects of the design in the Signal&Communication system. But in the final report of the 7.23 high-speed train accident by the investigation board, the deputy leader of the investigation board says the main reason for the High-Speed train accident is inadequate management in the railway system.

A more detailed description of the whole process including behaviors of the watch keeper, the dispatcher and divers of D301 and D3115 could be seen in Figure 2.

Time	Watch Keeper	Dispatcher in Shanghai	D301	D3115
19:39:00	Notified the dispacher of the "read strip" failure			
19:51:00				Reached Yongjia Station 4 Min behind schedule
19:54:00		Realized that the display in CTC differed from the state of TCC in Wenzhou Station, he issuing the order to change from automatic control to manual control		
20:09:00		Notified D3115 of the "read strip" failure in 5829AG		

20:12:00			36 min behind schedule in Yongjia	
20:14:58				Left Yongjia Station
20:17:00		Ordered D3115 to transferred to On Sight mode (V<20km/h) if there is a red light in the interval		
20:21:22				Reached 5829AG and stopped automatically for the TC Failure
20:21:46				a. Failed to restart three times for the TC Failure
20:22:22	Failed to call D3115 three times			b. Failed to call dispatcher in Shanghai three times/b
20:24:25	Failed to call D3115 three times	Ordered D301 to leave	Left for Wenzhou	a/b
20:26:12	Told dispatcher in Shanghai that D3115 reached Third section(near 5829AG) but could not be contacted	Asked Watch keeper in Wenzhou nan about the state of D3115		a/b
20:27:57	Got report from D3115 that he could not contact with dispatcher and failed to restart. Replied to D3115 "roger that"			a/b and contacted with watch keeper in Wenzhou Station
20:28:43 - 20:28:51				Failed to contact with dispatcher in Shanghai
20:28:51 - 20:29:02				Failed to contact with dispatcher in Shanghai
20:29:26				Transferred to on-sight mode successfully and restart
20:30:05				Rear-ended by D301 with the speed of 99km/h

Figure 2. Related events leading to the accident

3 The System Theoretic View of The Accident

As mentioned in last section, both the failures of the signal devices and risk behaviors in the scheduling system contributed to this accident. However, from the point of view of events, it is still not clear how and why all these mechanism failed to prevent the train from rear-end accident. Questions like “why the over-speed protection, the communication between human controllers, and the monitor by the dispatcher, failed without exception” could not be answered. A system perspective give us a broader view of how this accident happened not only because of component failures, but also lead by the poor supervision and management by the in the railway system.

Leveson [3] proposed a new accident model called Systems-Theoretic Accident Modeling and Processes (STAMP) to analyze the safety of a social-technical system. It is based on system theory and considers system safety as a control problem rather than treating accidents as a serious of related event and often focuses on the “root cause” [4]. As modern systems become complex, understanding system safety and preventing potential risks requires more efforts than just identifying component failures. In fact, in the Yong-Tai-Wen high-speed railway, both the system management during the stage of system design and development and supervisions and enforcement of safety regulations contributed to the accident other than failures in the TCC and the Track Circuit.

To analyze safety from a social-technical perspective, a model with multiple control levels [3] has been proposed including both system development and operation and the interaction between them. Each level takes information from its lower one and enforces safety constraints on it. Table 1 describes the mapping from the generic safety control structure to the real components in the development of Zhejiang high-speed railway in China, while Table 2 focuses on the operational phase.

Table 1. Generic components in the high-speed railway development

Components in hierarchical safety control structure(Development)	**The corresponding components in Chinese railway system**
Governments regulation agencies	Chinese Ministry of Railways
Governments regulation agencies	Zhejiang Government
Maintenance and Evolution	Shanghai Railway Bureau
Company Management	CoastalRailway Zhejiang Co. LTD
Project Management	China Railway Signal & Communication Corporation (CRSC)
Design and Implementation	Beijing National Railway Research&Design Institute of Signal&Comm Co. LTD
Safety Assurance	System Integration Group

Table 2. Generic components in the high-speed railway operation

Components in hierarchical safety control structure(Operation)	**The corresponding components in Chinese railway system**
Governments regulation agencies	Chinese Ministry of Railways
Safety Assurance and Supervision	Shanghai Railway Bureau
Maintenance	Electrical&Signal Office
Operation	Transportation Office
Operation & Maintenance	Wenzhou Station

3.1 Hierarchical safety control structures

The safety control structure includes both the construction of the high-speed railway line within Zhejiang Province and the operation of the Yong-Tai-Wen railway line, which is shown in Figure 3. It includes the High-Speed Train (D301 and D3115), the whole CTCS2 system, the Shanghai Railway Bureau and the Ministry of Railways on the right. The development structure (on the left) only incorporates those involved in the development of the signal&communication system because failures of signal devices are believed to be one of the main reasons for the accident. As mentioned before, there are two operational modes in this system (DACM and USCM). In the former, the CTC issues scheduling commands which transmit through TCC and the LEU and finally reach the ATP, which monitor the status information from the Track Circuit. If there is a Red light strip, the TCC will transmit to the USCM in which the train will be controlled by the coordination between the driver and the watch keepers in the station.

On the left of Figure 3 is the safety control structure of system development. The Coastal (Yong-Tai-Wen) Railway is its subsidiary company of Zhejiang Railway which is a state-owned liabilities limited company. It cooperates with the Ministry of Railways on behalf of the government of Zhejiang Province to holds and runs related national assets of jointly built railways. To make the discussion simple and easy to understand, Zhejiang Railway and the Coastal (Yong-Tai-Wen) Railway are referred to as Coastal Railway as a whole. It is responsible for the contract of investment and construction of the Yong-Tai-Wen coastal railway line in Zhejiang Province. The China Railway Signal&Communication Corporation (CRSC) is the contractor of the signal and communication system of the Yong-Tai-Wen railway line and responsible for the system integration of signal device. It also provides Track circuit to the CTCS system. Beijing National Railway Research&Design Institute of Signal&Communication Co., Ltd. (CRSCD), a subordinate enterprise of CRSC, designed and developed the TCC system – LKD2-T1.

Based on STAMP, the accidents are led by the violations of the safety constraints and the control flaws in a particular system. Moreover, if human controllers are involved, the context in which control decisions are made must be taken into account. At first, the hazards and system constraints related to this accident could be identified. It should be noted that the safety constraints listed here only incorporate those involving the automatic and human controller in the operational

part of the system.

System Hazards:

Two trains on the same section of track traveling at different speeds

Safety constrains:

(1) When a track section is occupied by a train, the TCC transmits control parameters representing track occupancy to other trains and issues warning signals (red) to the signal device in front of this section. (2) The failures in the Train Control System must be identified and provided as feedback to the dispatcher of CTC in time. (3) The dispatcher of CTC and the watch keeper should identify the potential danger in the railway line and command the train to slow down or stop in emergency situations.

3.2 The physical process of the accident

The physical process of the train system is shown in Figure 4. The physical process being controlled is the operation of the high-speed train which has two controllers – (Automatic Train Protection) ATP and the driver. Like the train control system, the train also have two operational modes – the

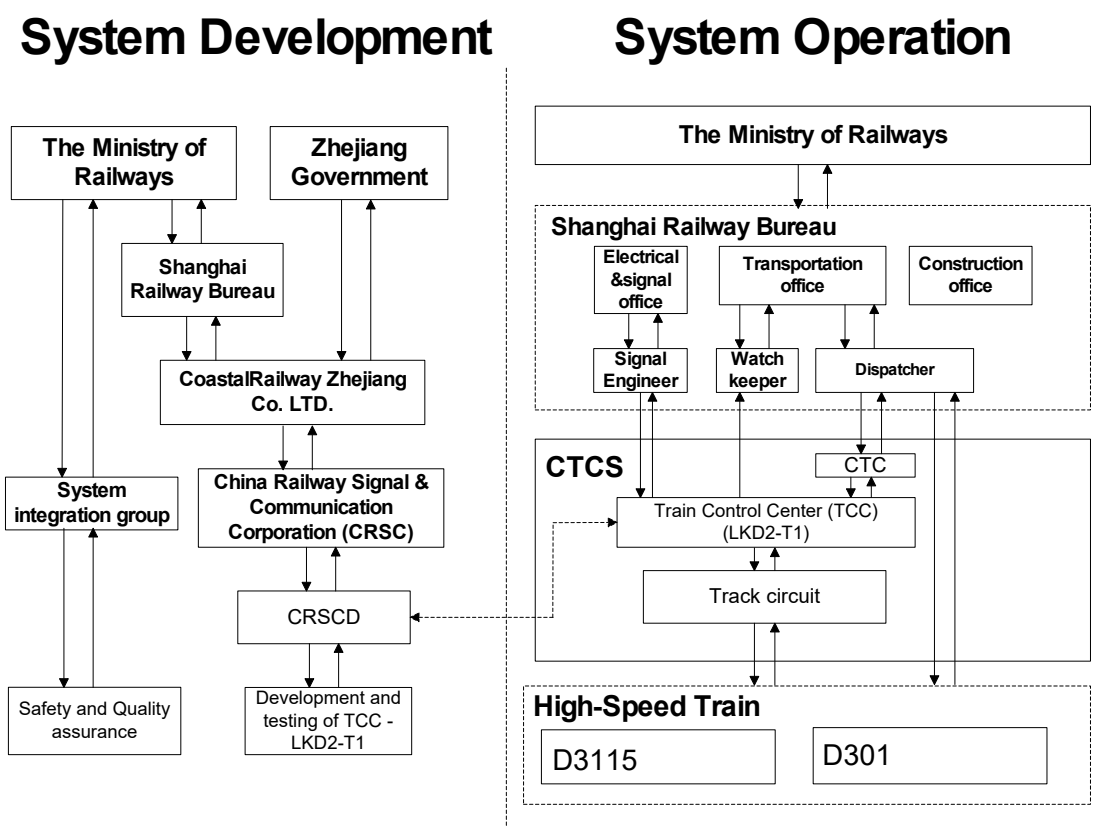


Figure 3. Safety control structure of the High-Speed train accident

automatic monitoring mode and the on-sight mode. In the former the ATP could using the data provided by the Track circuit and perform calculation to generate the control command automatically while in the latter the driver must manually operate the train according to the status of the signal light controlled by the TCC. Normally, the maximum speed for the on-sight mode is 20 kilometers per hour. In addition, if failures in the Track circuit lead to the erroneous

transmission of data to the ATP, it will stop the train immediately and transit to on-sight mode. In fact as shown in Figure 2, about 1 minute before the accident, the D3115 train was in on-sight mode running at a speed lower than 20 km/h and D301 was in monitoring mode with a high speed (99km/h). The ATP did not decelerate or stop D301 as designed when two trains were in the same section because the failed TCC transmit erroneous signal to it. To make things worse, the driver of the D301 did not realize that D3115 was in front not far away until it was too late. In the end, the D301 crashed into D3115 with a speed more than 90 kilometers per hour although the driver of the D301 performed the emergency brake. Obviously, 1 kilometer is not enough for the driver of D301 to stop the train safely.

Automatic Train Protection (ATP in D301 and D3115)

Safety Requirements and constraints violated:

Over-Speed protection;

Warn the driver when there is a failure in the automatic control system.

Inadequate control actions:

Provided erroneous signal to the ATP;

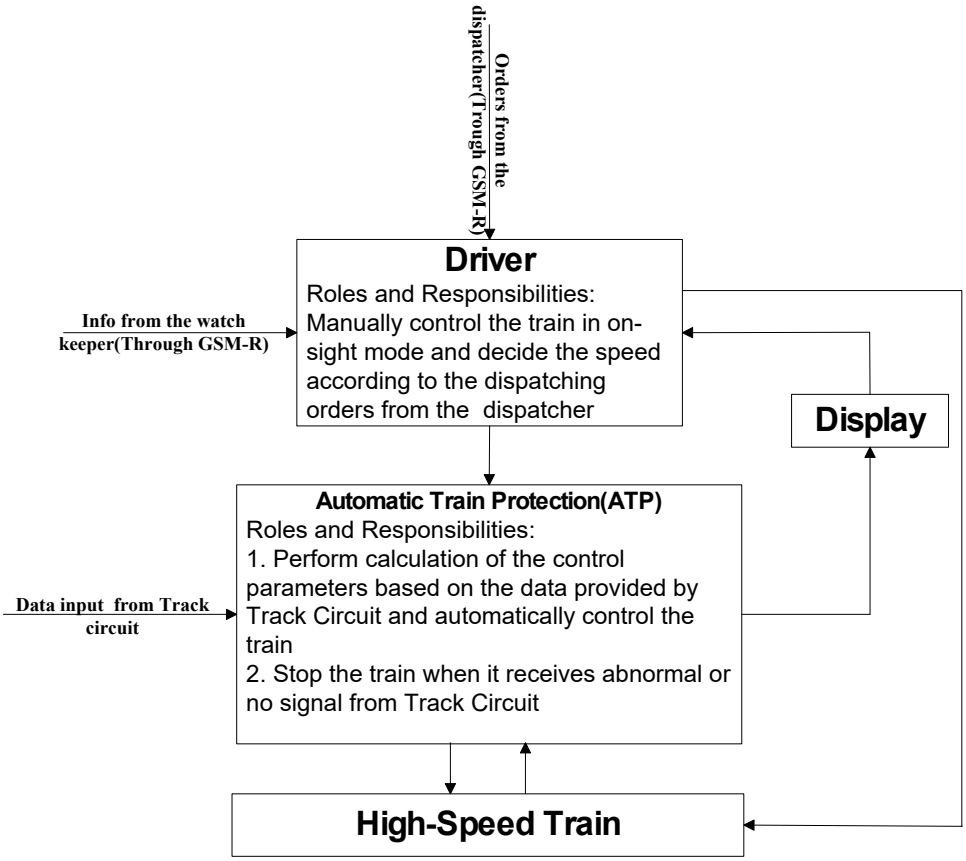


Figure 4. On-Train control system

Turned the signal light green when D3115 was in the corresponding section;

Do not perform automatic emergency brake when the distances between two trains are less than 2 kilometers.

Incorrect process model:

The ATP in D301 has an incorrect model of the position of D3115 due to the erroneous input from

the Track circuit. The TCC provide unsafe signal transmitting through Track circuit to the ATP in D301, which made the ATP failed to stop or decelerate D301 even if there were two trains existing in the same Occlusive section.

Control Inputs or external Information wrong:

Erroneous Control Inputs from TCC and the failures in Track Circuit.

The Driver of D301

Safety Requirements and constraints violated:

Perform emergency brake when there is a train in front.

Inadequate control actions:

According to the investigation report, the driver of D301 performed the brake as soon as he saw D3115. Unfortunately, it is too late for him to stop the train.

Incorrect process model:

He did not aware of the state of D3115 and slowed down the train because no one told him to do so. Also, the display in the ATP and the signal light (erroneously turned green) make him thought that there was no train in the front section. So it is necessary to ask why the dispatcher and the watch keeper did not inform him about the situations.

External Information wrong:

The signal light is supposed to turn red if there is a train on the next section, like the TC-5829. However, but is keeps green because of the erroneous signal sent by the TCC.

Context:

According to the investigation report, the driver failing to respond to emergencies was attributed to the dispatcher and the watch keeper who was supposed to notify the driver about the potential risks in Track Circuit 5829AG. Besides, bad weather might lead to the low visibility, which might be one reason why the driver of D301 did not find D3115 promptly.

3.3 The Train control system

The whole ground Train control system is shown in Figure 5, which includes the physical controller – TCC located in Wenzhou station and the human controllers involved. As regulated in [10], the watch keeper should have asked the driver of D301 to stop the train as soon as hazards were found in the railway line. This mechanism, called “junction control for operation and maintenance of rolling stocks and locomotives” [10], is designed to notify the driver of the potential risks and ensure the safety of the train. In addition, it is the dispatch that has the responsibility to monitor the speed and position of the train. Therefore, questions like “Did the watch keeper or the dispatcher know the exact position of the D3115?” or “Did the errors in the signal lights are realized by any of the staff members?” should be addressed in order to understand their behaviors during the emergency. Unfortunately, this information is not included in the investigation report. Although the failures in the Train control system might lead to the erroneous signal being given to them, the related hazards could be identified by communications between them through the GSM-R (Communication system used in the railway system).

TCC (LDT1-T)

Safety Requirements and constraints violated:

Collect data from track circuit to decide the track occupation;

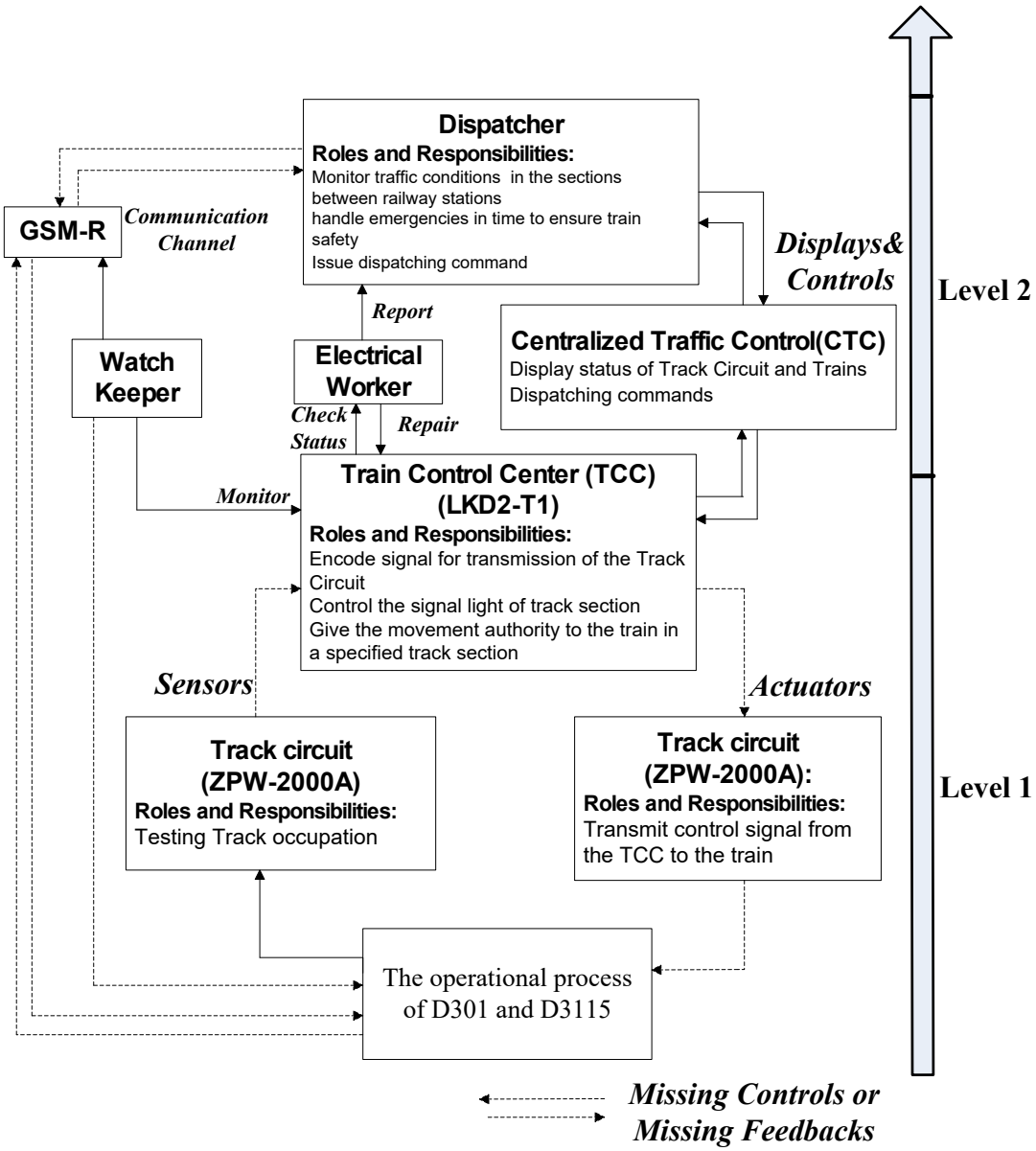


Figure 5. Train control system on the ground

Send encoded signal to the ATP through Track Circuit to control the operation of the train;

Control the signal device to display green, yellow or red light, so the driver could be aware of the situations of the occlusive section in front.

Inadequate control actions:

Do not update the data of the status of Track Circuit

Send erroneous signal to the ATP of D301, which lead to the hazardous conditions: The ATP was supposed to stop D301 when it receives signal from TCC, however, due to the hardware failure in the PIO circuit (responsible for data acquisition from Track Circuit) in TCC, it received erroneous data of the Track Circuit 5829AG. To make things worse, the software of TCC did not capture this exception. As a consequence, it sent no-occupation code to D301 indicating that there is no train in section 5829 and turns the signal lights of section 5829 and the next two sections green

Inadequate control algorithm: the algorithm do not conform to fail-safe principle: According to the fail-safe principle, even if the data receiving from the track circuit was wrong, the TCC should send command to stop train D301 and turn the signal lights red to ensure the safe operation.

Incorrect process model: Inadequate model of the Track Circuit interface

Control Inputs or external Information wrong:

Erroneous Control Inputs from the interface of Track Circuit.

Dispatcher (Shanghai Railway Bureau)

Safety Requirements and constraints violated:

Monitor traffic conditions in the sections between railway stations and issue dispatching command in Decentralized autonomous control mode.

Notify the driver about potential risks in emergencies to ensure the train safety

Inadequate control actions:

Did not effectively monitor the operational status (speed and position) of both train D3115 and D301

Dysfunctional interactions:

According to the investigation report, the watch keeper did not know the status of TCC and Track Circuit after the report of failures of them, which is lead by the poor communications between the electrical worker in Wenzhou station and him. Also, he failed to contact with the driver of D3115 to know the emergency situations of D3115 in Track 5829AG. As a result, he did not notify D301 of the risk in the third interval. It was not clear that the poor communication was due to the failures in the GSM-R system or any other factors.

Incorrect process model:

Incorrect model of train D3115 and D301: the dispatcher did not aware of the current situations in the third interval, which lead to hazards for train D3115 and D301. Specifically, train D3115 stopped at the third section due to the failure in Track Circuit 5829AG while D301 was running at a high speed (>100km/h) in the following two sections;

Incorrect model of the TCC in Wenzhou Station: he did not know that the PIO circuit was damaged by the lightening at that time of the accident and the software sent erroneous signal to both the train D301 and the signal lights in the first and second track sections.

Control Inputs or external Information wrong:

Erroneous inputs from CTC.

Watch keeper (Wenzhou Station)

Safety Requirements and constraints violated:

Supervise the operation of D301 in unconventional station control mode and cooperate with drivers to ensure the safety of the train during emergencies.

Inadequate control actions:

The Watch Keeper did not effectively perform junction control of D301 during emergencies. In fact, it is one of the reasons that the driver of D301 was not aware of the potential risks in track 5829AG where D3115 stopped three times due to failures in Track Circuit.

Incorrect process model:

Incorrect model of train D301: Although he got the report from the driver of D3115 that D3115 stopped at the third interval and could not restart because of failures in the Track Circuit, he did not notified D301 to decelerate or stop before it entered track 5829. Obviously, neither did he be aware of the status of D301 which is running with a speed more than 100 kilometers per hour, nor realized the potential risk in the track 5829AG.

Context in which decisions are made:

The scheduling pressure might increased the overall performance goal of the whole Shanghai Railway system while at the same time less attention resources were spent on the safety of the train. In fact, several late arrivals of the train in the Jing-hu high-speed railway line made the public and the media doubted the transportation ability of the Chinese high-speed railway. So as a member of the railway scheduling system, the watch keeper would put higher priorities on performance goal and might take risks (failed to perform cooperative control) to keep the on-time arrival rate at a relatively high level.

Poor communication and coordination between the three controllers

As could be seen in Figure 5, there are three controllers involved in this accident (one automatic controller – TCC, and two human controllers – dispatcher and the watch keeper). From a control perspective, hazard appearing in Track circuit 5829 could be attributed to the conditions that the human controller failed to provide control commands to slow down or stop the train D301 while the automatic controller had abnormally issued command to stop the train D3115 in Track circuit 5829AG because of hardware failures. In other words, if the automatic controller had provided no commands to stop the train D3115 in 5829AG or the watch keeper and dispatcher had predicted the existence of hazards in this situation and took actions to stop the train D301, the accident could be prevented.

3.4 Shanghai Railway Bureau

Shanghai Railway Bureau

Safety Requirements and constraints:

Administer the Yong-Tai-Wen railway line: It is the responsibility of the Shanghai Railway Bureau to coordinate different departments in it to ensure the normal operation of the high-speed railway line within Zhejiang Province;

Supervise implementations of the safety regulations defined by the Minister of Railways;

Train the staff in the Shanghai Railway system (e.g. dispatcher and watch keeper) to improve their awareness of safety and the ability to response to emergencies.

Inadequate control actions:

Ineffectively supervise the staff to carry out safety regulations of the high-speed railway line: as described above, none of the dispatcher, the watch keeper and the electrical worker took actions according to regulations when there were emergencies in the third interval of Wenzhou station. They made mistakes either because they did not realized the hazard or did not know how to cope with them. To be more specific, if the Shanghai Railway Bureau monitored the behaviors of the watch keeper effectively and trained them to be more alert in the unconventional station control mode, they would strictly implement the cooperate control of the train D301 and remind the diver to decelerate the speed. Also, the dispatcher might remind the driver of D301 of the risks lead by failures of TCC and Track Circuit if he had took enough emergency training.

Incorrect process model:

According to reports on the website of the Shanghai Railway Bureau, before the start of the Yong-Tai-Wen railway line on September 28th, 2009, it established a special panel responsible for organizing staff including electrical workers to perform test of the new devices for this new railway line and carry out several emergency practices. Also, they performed training for staff in

transportation office including dispatchers and watch keepers starting in February, 2009. All of these efforts made them satisfied with the safety conditions of this line while in fact there were potential risks because of the design flaw in electrical devices and the poor safety awareness of workers in the Shanghai railway system.

Context in which decisions are made:

Scheduling Pressures might make local authorities believe that improving the on-time performance is their first concern. To prevent late arrival of the high-speed train, they would take the risk to violate safety regulations as long as performance goal be achieved.

3.5 The Ministry of Railways

The Ministry of the Railway:

Safety Requirements and constraints:

Establish criteria to manage the work of system integration in the Yong-Tai-Wen railway

Establish mechanism to response to emergencies and accidents

Perform inspections and surveillance of the work of Shanghai Railway

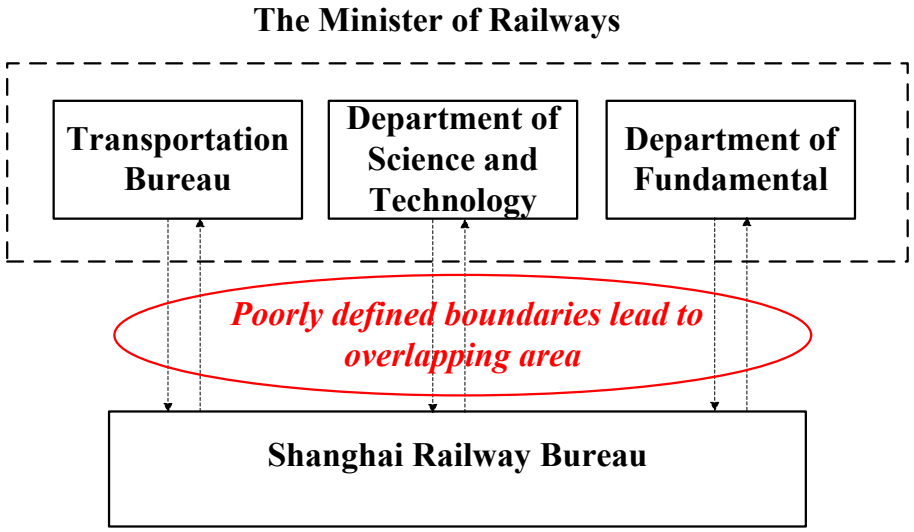


Figure 6. The Ministry of Railways

Inadequate control actions:

According to the accident report, the MOR just focused on the project schedule and underestimated the design flaw in the signal product and its impact on system safety. Moreover, it did not establish standards to ensure the safety of the project and mechanisms to respond to emergency. However, as early as September 2009, the shanghai Railway Bureau organized several emergency drills to prepare for the safe operation of the Yong-Tai-Wen high-speed railway.

Ineffective supervise and inspect of the safe operation of the Shanghai Railway Bureau.

As in many other cases, the MOR did not have a specialized department which is responsible for safety issues. Both the newly established system integration group and the three departments have safety supervision as part of their responsibilities. Unfortunately, neither of them performed detailed risks and hazards analysis to ensure the safety of the signal system.

Dysfunctional interactions:

Responsibilities were overlapped among various departments of the MOR (Figure 6). According to the accidents report, MOR established specific project group for the high-speed railway.

However, it did not have standard procedure to follow. As a consequence, several departments including Transportation Bureau, Department of Science and Technology and Department of Fundamental violated safety regulations in terms of inviting tenders for the signal device、technological examination and device status. They performed technical pre-examination of the TLKD2-T1 based on subjective judgment and approved the use of TLKD2-T1 without on-site testing.

3.6 CRSC

CRSC:

Safety Requirements and constraints:

Quality/safety control process must be established to monitor the whole development process of signal devices and ensure that the quality of products meet national standard

Inadequate control actions:

The CRSC did not establish safety program to ensure the quality of products of its sub-company. More over, it failed to take the responsibilities of oversight and underestimated the potential risks of TLKD2-T1. As a result, it permitted the use of TLKD2-T1 without comprehensive Verification and validation (V&V).

As the signal system integrator of the Yong-Tai-Wen Railway line, it failed to take the responsibility of supervision of its sub-company. In fact, no safety regulations of production was established，which in a certain sense led to its poor awareness of the quality of the TCC-TLKD2-T1.

Dysfunctional interactions:

Like the situation in the Ministry of Railways, safety program did not be established among the sub-companies of the CRSC. To make things worse, both the CRSC and the CRSCD did not take the responsibilities to supervise the development of TLKD2-T1.

Mental model Flaw:

The leader of the CRSC believed that the signal products is of high quality and could be used normally in the high-speed railway line.

3.7 CRSCD

Safety Requirements and constraints:

Must ensure that the quality of the TCC meet national safety standards and perform comprehensive V&V process

Inadequate control actions:

Before develop TLKD2-T1 TCC, CRSCD did not effectively evaluate the quality and safety of TLKD2-T. Specifically, the leaders in CRSCD made the decision to update TLKD2-T based on the oral report from Automatic Control Research Institute. More over, it did not find any design flaw and potential risks of TLKD2-T1.

Mental model Flaw:

The CRSCD thought the quality of TLKD2-T1 could be maintained just because personnel of Automatic Control Research Institute make promises.

Feedback: Leaders in CRSCD did not have direct channel to acquire the state of products of its sub-departments. For them, the only source of information is the oral report, which made them believe that TLKD2-T1 could meet the safety requirement of the project.

4 Creating System Dynamic models Based On STAMP Safety Control Structure

It is not enough to identify the poor coordination between multiple controllers in each level of safety control structure and the weaknesses of it at the time of the accident. Changes in the safety control structure also have the potential of leading to unpredicted consequences in terms of system failures and accidents. For policy makers and managers to make reasonable decisions to prevent accidents in the future, it is also important to understand why and how this system evolved toward a state vulnerable to hazards [3,8]. system dynamics modeling [5] is used to describe the changes during the development and operational process of the Yong-Tai-Wen high-speed railway line.

Dulac [8] propose a framework which create system dynamic model based on the safety control structure of a system. To be more specific, the system development and operation are treated independently and several critical causal loops and variables which have great impact on risk are identified. Likewise, in this paper, two related models are constructed. The first model identifies the economic and social factors that speeded up the growth rate of the high-speed railway and later caused the design flaws in the electrical devices, while the second model is focus on how the system evolved to a hazard state and why all the protective mechanism did not take effects in preventing the accident. To make the model easy to understand, we only construct simple high-level models and omit some secondary factors in this accident given that the purpose of this section is to show how to construct system dynamics of this accident based on STAMP safety control structure described above. Therefore, a more comprehensive model could be build when more information becomes available.

4.1 System development

To facilitate system dynamic analysis, all the organizations from system development in Figure 3 are organized into several groups (Figure 7), each of which has a specific responsibility during the process of system development. For instance, the Minister of Railways and Zhejiang Government were served as government agencies that made regulations and provided funds to its sub-organizations (e.g. CoastalRailway Zhejiang) and Shanghai Railway Bureau was responsible for the maintenance and evolution of the railway line within Zhejiang province. A special department, called system integration group was established to supervise the implementation of regulations, however, it failed to play a role in urging the various groups to follow the safety standards (represented by the red fork in Figure 7).

The influence of performance, resources and safety pressure and reporting channels between generic dynamic components are of great importance to the assemble of various components into a integrated system and modeled as dynamic connectors [8]. Only high-level models are developed to perform the mapping from STAMP to system dynamic and the methodology used is not exactly the same as the one described in [8]. To be more specific, the reporting and reinforcing channels have the potential to create the causal loop structures. For instance, in Figure 7, the problem or incidents reporting channels have indirectly relationship with the scheduling pressure (upper left corner of Figure 7). Based on the national development plan of the railway lines defined by the Ministry of railway, the Zhejiang government set the goal for the development of Zhejiang

high-speed railway which aims at becoming the first province in china to accomplish railway modernization. As a result, the constructions of the 12 railway-related projects were scheduled to be completed by 2014. So the time budget for the construction was very limited and the related pressures lead to reductions of safety priority. Poor safety regulation and supervision made the design flaws in the signal products undetected, which is one of the reasons contributed to the accident. In fact after the accident, the funds for the

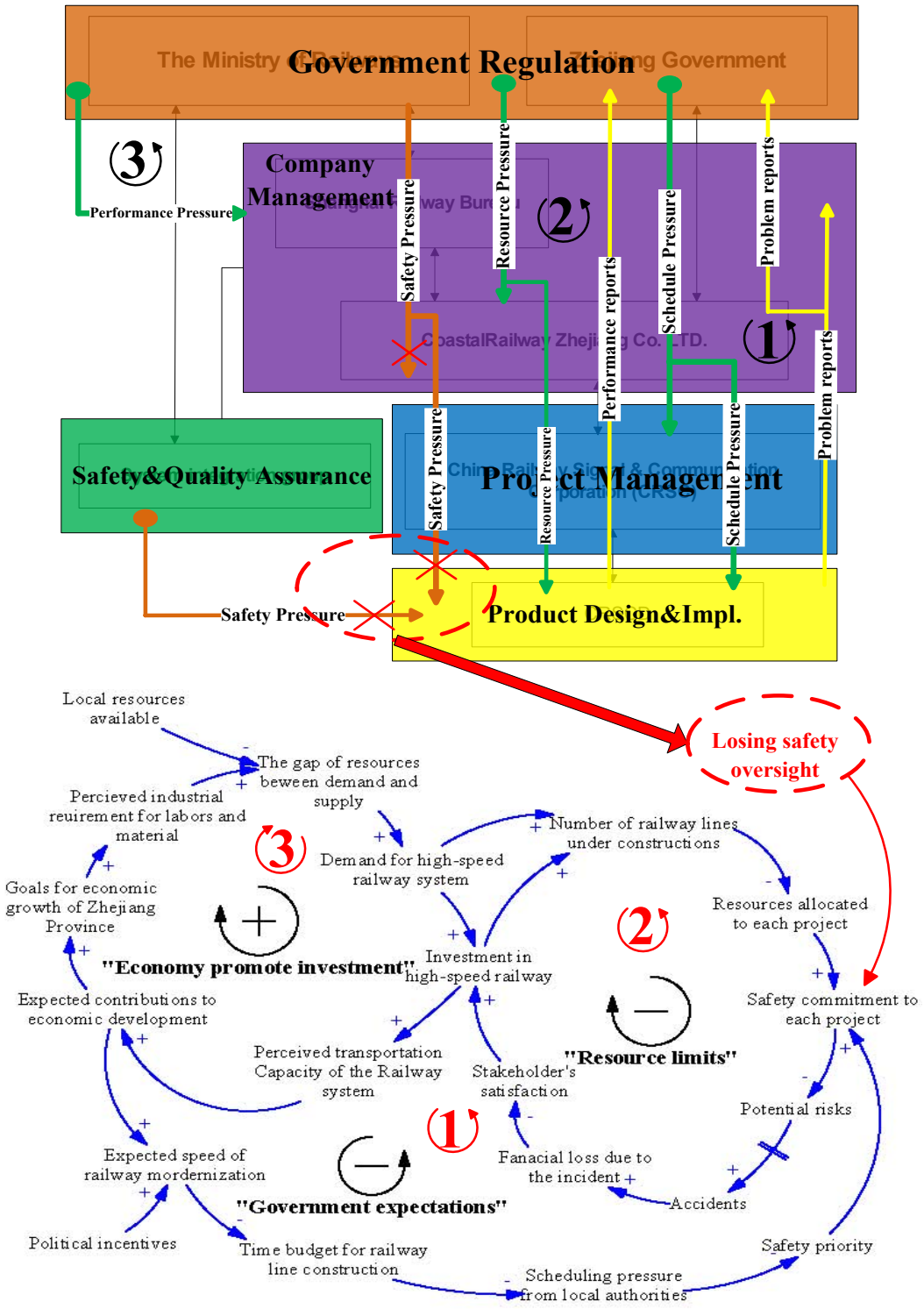


Figure 7. System dynamics of Zhejiang high-speed railway development

high-speed railway projects were cut by the minister of Railways and all the projects were stop temporarily for a complete safety inspection and this situation was reflected in the balancing loop "government expectations" (bottom of Figure 7).

The other two causal loops (no. 2 and no. 3) in Figure.7, including one reinforcing loop which promote investment to the railway in Zhejiang Province and one balancing loop which would change resource allocation on each project due to decrease in stakeholders' satisfaction with the project, could also be build as no.1 causal loop. As noted above, we do not distinguish different generic dynamic components but only consider the influence of these channels in STAMP on system safety and have it reflected in the dynamic risk management model. One thing should be addressed is that the project as a whole tend to decrease safety priority and commitment to safety due to other pressures. To make things worse, the channels for reinforcing safety oversight and transmitting safety pressures are missing for lack of safety resources and complacencies (red ellipse in Figure 7). It is pointed out in the investigation report that leaders in the CRSC believed that there are no problems with the signal&communication products because of the oral reports they received from the sub-organization. Consequently, they design flaw in the TCC was not discovered during the testing process. If safety oversight had been reinforced externally, or the project contractor, in this case the CRSC, had received more safety pressures from the management company, the safety commitment could have been maintained.

The second causal loop "resource limits" depicts total resources available to each projects and its impact on the safety situation of each project. Like the one described in [9], as the numbers of projects grew, the gap between the required capital resources and the funds provided by the stakeholders led to compromises in quality of design and the execution of safety regulations. The increasing potential of risks caused by Poor supervisions and coordination becomes inevitable. As a result, the rise in the accident rate made stakeholders unsatisfied with the project and the investment become less. In fact, the situation described above is the same with what happened after the 7.23 accident.

The third loop describing the economy of Zhejiang province which experienced dramatic changes around 2009 partly because of the impacts of the global financial crisis. The export demand for textiles and mechanical processing products had decreased drastically, which was a disaster for the many small and medium-sized enterprise which had relied heavily on exportations. The troubled economies of Zhejiang sought for incentives of economic development. To maintain the economic growth rate, the government pushed these enterprises to make the economic transition, which required for easier access to labors and material, especially in Zhejiang province where resources are rare and hard to get. Besides, the high-speed railway itself seems to be a promising way to promote the development of economy in terms of freight transportation and traveling. All of these economic factors promote the investment in high-speed railway. Of course the perceived capacity of the railway increases enormously, which lead to the overconfidence in the benefits and profits the high-speed projects would make. The local government and the enterprises believed that the high-speed railway projects would make great contributions to social and economical development and the investment in it should be increased.

4.2 System operation

The method we used is the same as the one described above, except that the stock and flow structure have been introduced to model delays in the problem reporting channels (top of Figure.

8), which made the authority failed to realize the poor safety conditions and take actions accordingly until accidents happened. These effects are represented by “problem fixation” loops in Figure 8. Specifically, they are divided into two parts - management and supervision from the

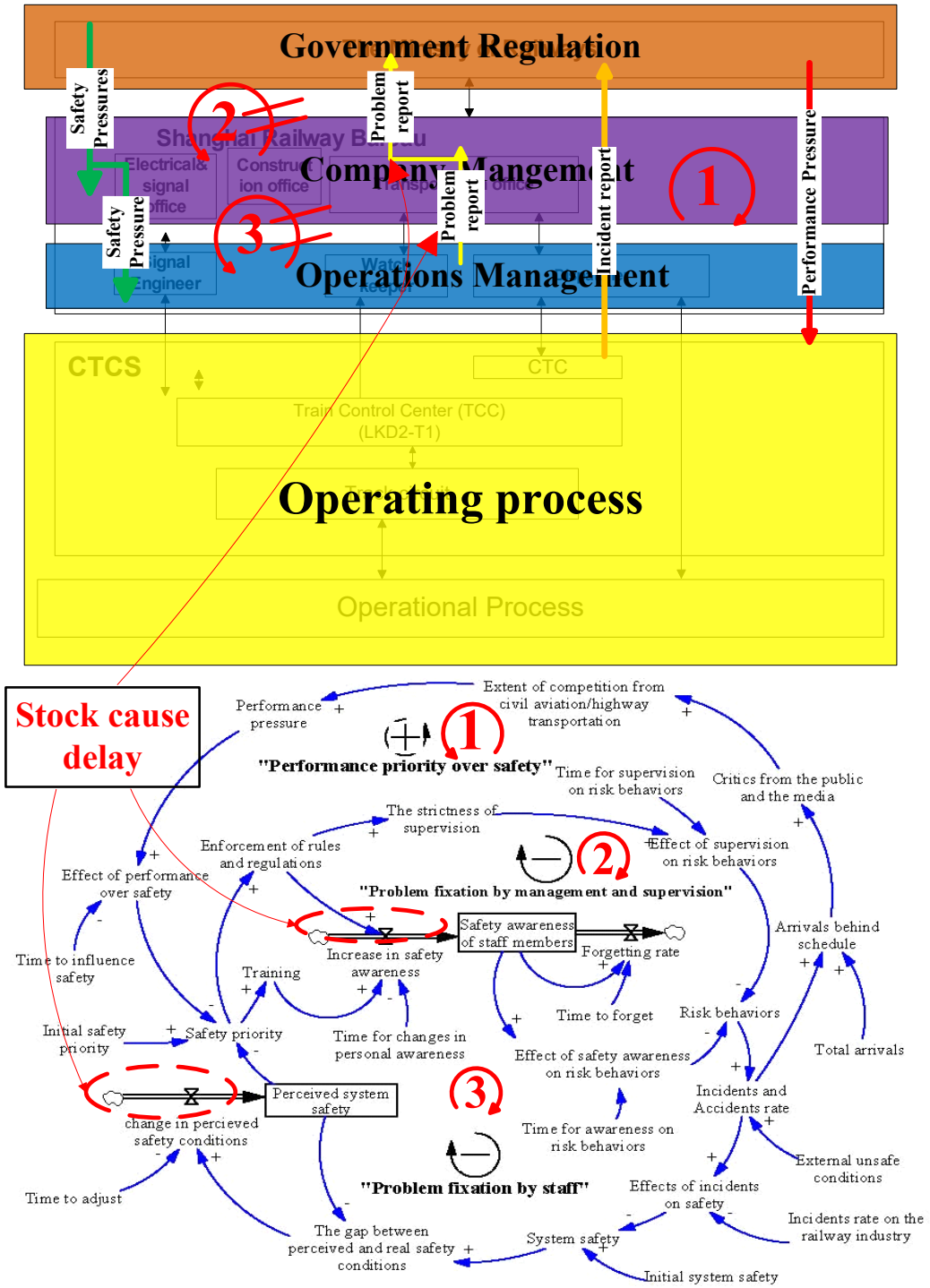


Figure 8. System dynamics of Zhejiang high-speed railway operation

authority (no. 2 loop in Figure. 8) and efforts taken by the personnel (no. 3 loop in Figure. 8). Also, it takes some time to improve the safety awareness of them by training, which will decrease if the authority takes no actions to maintain its balanced level. Another factor should be mentioned is that the reduction in incidents would also generate complacency, which could lead to a lower

safety priority. And this might in turn cause more risk behaviors and incidents. From a point of view of causal loop, this equals to a balancing loop. For simplicity, this effect was assumed to be included in the “problem fixation” loop reflected on the organizational management and supervision and the change in the personal safety awareness.

In addition, the performance pressure and the incident report channel at the top of Figure. 8 could also lead to causal effects on the safety. At the very beginning of the high-speed railway projects, one of its ultimate goals, which aim at competing with the civil aviation industry and highway transportation, was set by the Ministry of Railways. The Ministry of Railway wanted to make the high-speed railway in china a promising way to substitute for other means of transpirations. So there existed performance pressures from the start of the operation of the high-speed railway. Moreover, the local government had expected the railway to transport labors and raw materials with low cost and high efficiency in order to fulfill the ever increasing requirement for resources from industries, which also increased the performance pressures. To maintain the on-time arrival rate, it inevitably drew some of the attentions of the authority from safety. Poor supervisions and coordination led to the growth in risk behaviors and the incidents and accidents rate would therefore increase. The effect of incidents lies in two aspects. On one hand, more trains might arrive late due to failures in the power supply and errors of the scheduling system. The pressures from the mass media would intensify the competitions among various transportation systems, which in turn increase the performance pressure. On the other hand, frequent incidents would reduce the confidence of the safety structure and the risk tolerance. As a consequence, the authority might perform strict supervision on the scheduling process and the safety training of its staff. Therefore risk behaviors such as failing to perform coordinate control of the train by the watch keeper and remind the driver to slow down in case of emergency would be reduced. In general, the causal loop “Performance priority over safety” (Figure. 8) describes this effect.

Sterman [5] pointed out that stock caused delay, which results in outputs lagging behind outputs. In this model, it is reflected in the time for the authority of the railway system to perceive the system safety based on the reports and records. Comparatively, the performance pressure influenced the safety priority in a more direct and immediate way. The late arrivals of the trains would make the public unsatisfied with the high-speed railway, followed by more critics from the mass media. To maintain the superior position of it as the dominant way of transportations, the railway system would take effect to improve the performance in terms of the on-time arrival rate and therefore focus on the non-safety affairs.

5 Conclusion

Different cultures may exist in the society depending on its related nations, people lived there and the way they think and process information. Likewise, the “safety culture”, the general attitudes and approaches to safety and risk management in an organization or an industry [6], could evolve according to the development of economy in a nation. Considering that accidents occurred in a social context, it is of great importance to understand what organizational factors make the system vulnerable to risks other than technical problem. In this regard, the system theoretic approach provides us an approach to see safety in a wider perspective.

Even if there were many news reports attributing this tragedy to technical problems, from a system theoretic perspective, it could be seen that failures in the hardware and software alone does

not necessary lead to this accident. It is them together with the errors of human controllers that lead to risks [7]. The reasons lie in the whole process of project development and operation. To prevent the occurring of the same kinds of accidents in the future, some recommendations are provides below based on the analysis of the whole safety control structure. Especially the interactions between each component should be attached great significance. Specifically, the channels between them must keep working in order to meet the requirements of transmitting feedback information and enforcing safety constraints. Also, as could be seen in the system dynamics of both development and operation, the safety priority and commitment should not be affected by other factors such as scheduling and performance pressures. In this regard, as pointed out in [6], it is necessary for the safety-related departments to be independent of other sub-organizations. Recommendations specific to each components are listed below:

1. The inability of the Ministry of Railways to perform hazard analysis and safety assessment beforehand played an important role in the accident. In particular, although it establish a department responsible for safety issues in high-speed railway projects, poor coordination among various sub-organizations made it ineffective in identifying and controlling the potential hazards. From a control perspective, overlaps existed among multiple controllers. In this case, none of the project integration group and other departments involved in establishing safety assessment procedures took the responsibility to strictly supervise system development, especially the products of signal and communication. Thus, a reasonable efforts might be establishing an independent safety-related department (In fact there is one but failed to take the responsibility) so that overlap in responsibilities could be prevented. Moreover, safety regulations should be strictly enforced. Specifically, hazard analyses are necessary before and after the construction of the project and safety department have the right halt the development process of the project if there witnessed evidences confirming the existence of potential hazards which might lead to accidents.
2. The local government of Zhejiang province also contributes indirectly to leading the railway system into a hazardous state. Too many parallel projects caused by economical incentives results in deficiency of resources in terms of funding, manpower and facilities, so that safety efforts tend to be ignored during the development of railway line. Therefore, a scientific balance should be made between the safety and pace of development.
3. For the Shanghai Railway Bureau and the CRSC, safety must be independent of other issues such as on-time arrival rate and scheduling pressure. The competition among the transportation industries made the authority of the Shanghai railway Bureau give high priority to performance so that more risky behaviors were taken by the staff members. Consequently, high risk potential was not perceived by the authority until it was too late because it took time for the real system safety state to be perceived. In this regard, Workers could be trained and educated regularly to maintain their safety Awareness. But it might be more vital for the Shanghai Railway Bureau to keep the channels of feedbacks and oversight unblocked. In other words, leaders and management staff should hear from their subordinate regularly rather than depending on complacency.
4. Safety program must be established during the V&V process among its sub-companies and itself. In particular, comprehensive quality test and hazard analysis should be performed before its products came into use. Although the official approve of the use of LKD2-T1 in the high-speed railway line indirectly contributed to the product failure, the poor supervision of

its sub-companies underlie this flaw.

5. Besides recommendations above, it might be more meaningful to understand the roles that cultures and social context played in the whole railway system. A common consensus in the safety engineering is that it takes time and efforts to change safety culture of an organization. Actions should be taken to enhance the safety awareness of the leaders, management staff and workers in railway lines. Traditionally, in transportation system including railroads and aviations, safety efforts were embedded in project management and often influenced by performance and scheduling pressure. Therefore, it is necessary for the whole industry and government agencies involved to change their common attitude towards safety, which should be independent from other system elements.

6 Reference

1. Investigation report of the "7.23" Yongwen Railway accident, Available at http://www.chinasafety.gov.cn/newpage/Contents/Channel_5498/2011/1228/160577/content_160577.htm#_Toc312855797.
2. The Ministry of Railways, Technical Specification of the Chinese Train Control Center, 2010.
3. N. Leveson, "Engineering a Safer World: Systems Thinking Applied to Safety," MIT Press, 2011.
4. N. Leveson, "A New Accident Model for Engineering Safer Systems," Safety Science, Vol.42, No.4, pp. 237-270, April 2004.
5. J. Sterman, "Business Dynamics: Systems Thinking and Modeling for a Complex World," Boston, MA, Irwin McGraw-Hill, 2000.
6. N. Leveson, Joel Cutcher-Gershenfeld, "What System Safety Engineering Can Learn from the Columbia Accident," International Conference of the System Safety Society.
7. N. Leveson, "Safeware: System Safety and Computers," Addison-Wesley Publishers, 1995.
8. N. Dulac, "A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems," Ph.D. dissertation, Dept. of Aero. Astro. Eng, MIT.
Cambridge, MA, 2007.
9. A. Abdymomunov, "Application of System Safety Framework in Hybrid Social-Technical Environment of Eurasia," M.S. thesis, Engineering Systems Division, MIT, Cambridge, MA, 2011.
10. The Ministry of Railways, The Railway industry Standard of China: TB/3059—2009, 2009.