Safety Science 48 (2010) 544–555

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

STAMP-based analysis on the railway accident and accident spreading: Taking the China–Jiaoji railway accident for example

Min Ouyang [a,b], Liu Hong [a,*], Ming-Hui Yu [a], Qi Fei [a]

[a] Institute of Systems Engineering, Huazhong University of Science and Technology, Wuhan 430074, PR China
[b] Department of Civil and Environmental Engineering, Rice University, 6100 Main Street, MS-318, TX 77005, United States

ARTICLE INFO

Article history:
Received 22 December 2008
Received in revised form 29 May 2009
Accepted 4 January 2010

Keywords:
STAMP-based analysis
Railway accident
Accident spreading

ABSTRACT

Each hazard analysis technique is based on a model of accident causation. Most accident models regard accidents as resulting from a chain or sequence of events, such models are fit for accidents caused by failures of physical components and for relatively simple systems, but suffer from serious deficiencies when they are applied to software-intensive, complex engineering systems. Recently, a new accident model called System-Theoretic Accident Models and Process (STAMP) for system safety has been proposed, it is based on control theory and enforces constraints on hazards and thereby prevent accidents. In this paper, taking the China–Jiaoji railway accident happened on April 28, 2008 as an example, the STAMP approach has been used to analyze the railway accident and some improvement measures have been proposed. As the occurrence of one accident can cause many other accidents happen, based on the STAMP-based analysis, the accident spreading processes have also been discussed and modeled, which will be helpful to analyze accidents spreading in a broad sense and establish effective emergent measures for accident response management.

1. Introduction

On the morning of April 28, 2008, a major railway accident happened between Wangcun and Zhoucun, near Zibo, in Shandong province, People's Republic of China. Train T195 from Beijing to Sifang railway station in Qingdao derailed at 04:38 China Standard Time (CST) on the inside (left) track around a bend and train 5034 from Yantai to Xuzhou, coming from the other direction on the outside track, collided with it at the K290 + 940 m mileage marker on the double tracked Jiaoji Railway at approximately 04:41 CST. The accident caused 72 fatalities and 416 injuries (http://en.wikipedia.org/wiki/2008_China_Railways_train_T195_accident). Many media and officials reported and investigated this accident, almost all of them thought the accident was due to human errors. Some people were arrested for their mistakes, the director general of the Jinan railway bureau and the bureau's Party chief were sacked. However, about half a year latter, on October 13, train DJ5506 from Qingdao to Xuzhou railway station in Jinan railway run at 42 km/h over the speed limit for 8750 meters and 3 min and 23 s. It is fortunate that there was no injuries happened, but we should take a deep thought on why accident analysis and response in the past seem useless. This is just as Nancy Leveson said in her paper (Leveson, 2008), "We don't seem to be making much progress lately in reducing accidents in most industries. Major accidents keep occurring that seem preventable and that have similar systemic causes. Too often, we fail to learn from the past and make inadequate changes in response to accidents." In this paper, a systematic accident model called STAMP will be used to analyze the China–Jiaoji railway accident.

Accident Models can explain why accidents occur and play fundamental role in investigating and analyzing accidents. In the past, there are several types of accident models proposed. One type of accident models is the sequential accident models, which view accident causation as the result of a chain of discrete events that occur in a temporal order. The Domino theory proposed by Heinrich in the 1940s (Ferry, 1988) belongs to this class of accident models. In this theory there are five factors in the accident sequence, namely, social environment and heredity, fault of the person, unsafe acts or conditions, accident, injury. These five factors are arranged in a domino fashion which cause the fall of the first domino result in the fall of the entire row. This kind of accident models are fit for accidents caused by failures of physical components or human errors in relatively simple systems (Qureshi, 2007). However, many accidents have more than one contributing factor. So another type of accident models—Epidemiological Accident models have been proposed, which regard events leading to accidents as analogous to the spreading of a disease. Reason has made deep studies on this

* Corresponding author. Tel.: +86 02787540210.
E-mail addresses: pandasjtu@126.com (M. Ouyang), torrent1978@gmail.com (L. Hong), yumh@sohu.com (M.-H. Yu), qfei@mail.hust.edu.cn (Q. Fei).

0925-7535/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2010.01.002

type of accident models (Reason, 1990, 1997). But epidemiological models simply regard organization mistakes as management errors and do not consider the effect of organization culture while they emphasize on linear causality relationships and did not consider the non-linear relationships, including the feedback. However, the types of systems we are attempting to build and the context in which they are built has been changing. Systems become more complex and system components interact with each other in more complicated manners. So some more effective models are needed and then the systemic accident models have been proposed (Hollnagel, 2004). Systemic accident models view accidents as emergent phenomena, which arises due to complicated interactions between system components that may lead to degradation of system performance, or result in an accident (Qureshi, 2007).

Railway accidents cause a great number of casualties every year in our world. Causal analysis of railway accidents has attracted a lot of interest by many researchers. Santos-Reyes et al., by use of a systemic method, have respectively analyzed two accidents—the Paddington railway collision, occurred on 5 October 1999 (Santos-Reyes and Beard, 2006) and the Edge Hill railway accident, occurred on Sunday 9 May 1999 in Liverpool, England (Santos-Reyes and Beard, 2008). They have identified many 'learning points', which are relevant for preventing similar accidents on the railways. Fukuda, from the standpoint of effective and efficient safety management of railway transport, has described the definition of accidents, method of accident analysis, possibility of accident analysis, problems, etc. in railways (Fukuda, 2002). Niwa thought that a new accident analysis method should be proposed to analyze railway accidents because traditional analysis methods are difficult to find causes of the recent compound accidents with technologies developing day by day (Niwa, 2009).

A new type of systemic accident models called Systems-Theoretic Accident Model and Processes (STAMP) recently has been proposed by Levenson (2004). This model considers technical (including hardware and software), human and organizational factors in complex socio-technical systems. In the STAMP approach, accidents in complex systems do not simply occur due to independent component failures, rather they occur when external disturbances or dysfunctional interactions among system components are not adequately handled by the control system. Accidents therefore are not caused by a series of events but from inappropriate or inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system. This STAMP accident model has been used to analyze many major accidents, such as a public water supply contamination accident happed in a small town of Walkerton, Ontario, Canada (Leveson, 2002), a Friendly Fire Accident (Leveson et al., 2002). In this paper, we will use the STAMP approach to analyze the railways accident, the China–Jiaoji railway accident is used as an example. As the occurrence of one accident can cause many other accidents happen, based on STAMP analysis, the accident spreading process will be also discussed, which will be helpful to analyze accidents spreading in a broad sense and establish effective emergent measures for accident response management. The rest of this paper is organized as follows: Section 2 introduces the STAMP-based accident analysis approach briefly, the railway control structure to ensure train safety has been proposed. In Section 3, the first accident in China–Jiaoji railway accident has been analyzed and some improvement measures have been proposed to prevent future ones. The second accident and improvement measures have been discussed in Section 4. Then, the accident spreading processes have been briefly discussed in Section 5. Finally, what we get in our paper is summarized in Section 6, and the future directions are proposed.

2. STAMP-based accident analysis

Each hazard analysis technique is based on a model of accident causation. The STAMP model of accident causation can be used to perform STAMP-Based Hazard Analysis (STPA). In STAMP model, the most basic concept is not an event, but a constraint. The cause of an accident, instead of being understood in terms of a series of events, is viewed as the result of a lack of constraints imposed on the systems design and on operations (Levenson, 2004). In the STPA process, hazards are thought to be eliminated or controlled through system design. Fig. 1 presents a basic process control loop in STPA (Herring et al., 2007). Based on systems control theory, the following requirements must be satisfied for the system controller to achieve its objective (Levenson, 2004; Kohda, 2008): (1) the controller must have a goal to achieve; (2) the controller must be able to affect the state of controlled process; (3) the controller must be (or have) a model of the controlled process; (4) the controller must be able to estimate the state of the controlled process. As can be seen in the Fig. 1, the controlled process is subject to process inputs and disturbances. The process output may become input into another linked process control loop.

Based on the basic process loop, a system accident can occur due to its dysfunction, which may be caused not only by its component failure, but also by an incorrect system model or incorrect control rules. STAMP provides a useful classification of control flaw leading to hazard (Levenson, 2004). This classification can be seen in the Fig. 2.

To analyze causal factors of a system accident, the procedure of STAMP-based accident analysis can be described as follow (Leveson, 2002): (1) To identify the hazard involved in the loss. (2) The hierarchical safety control structure related to the hazard is constructed and the constraints necessary to control the hazard are identified for each controller. (3) Starting from the technical process and using the proximate events and general application knowledge, any failures and dysfunctional interactions (including communication problems) involved in the loss are identified. (4) For each constraint, a determination is made about why it was violated: either the constraint was never identified and enforced or the enforcement was inadequate. In addition, Any human decisions should be understood in terms of (at least): the information available to the decision maker as well as any required information that was not available, the behavior-shaping mechanisms (the context and pressures on the decision making process), the value structures underlying the decision, and any flaws in the mental models of those making the decisions (Leveson, 2002).

In this paper, we will apply the STAMP approach to analyze the railway accident. Fig. 3 shows the hierarchical control structure to ensure the safe operation of trains in China, starting form the

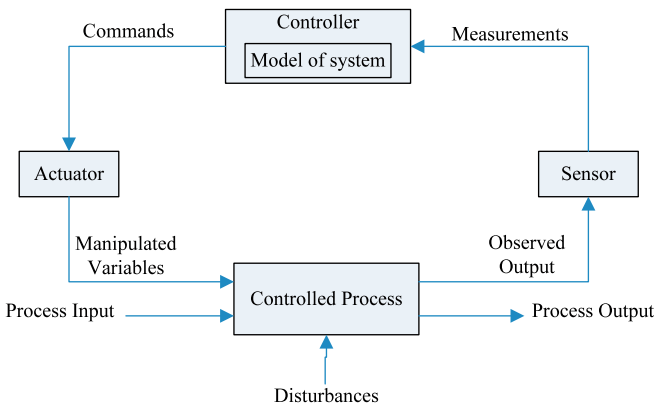


Fig. 1. A basic process control loop in STPA (Niwa, 2009).

Inadequate Enforcement of Constraints (Control Actions)
1.1 Unidentified hazards
1.2 Inappropriate, ineffective, or missing control actions for identified hazards
1.2.1 Design of control algorithm (process) does not enforce constraints
- Flaw(s) in creation process
- Process changes without appropriate change in control algorithm (asynchronous evolution)
- Incorrect modification or adaptation

1.2.2 Process models inconsistent, incomplete, or incorrect (lack of linkup)
- Flaw(s) in creation process
- Flaws(s) in updating process (asynchronous evolution)
- Time lags and measurement inaccuracies not accounted for

1.2.3 Inadequate coordination among controllers and decision makers (boundary and overlap areas)
Inadequate Execution of Control Action
2.1 Communication flaw
2.2 Inadequate actuator operation
2.3 Time lag
Inadequate or missing feedback
3.1 Not provided in system design
3.2 Communication flaw
3.3 Time lag
3.4 Inadequate sensor operation (incorrect or no information provided)

Fig. 2. A classification of control flaws leading to hazard.

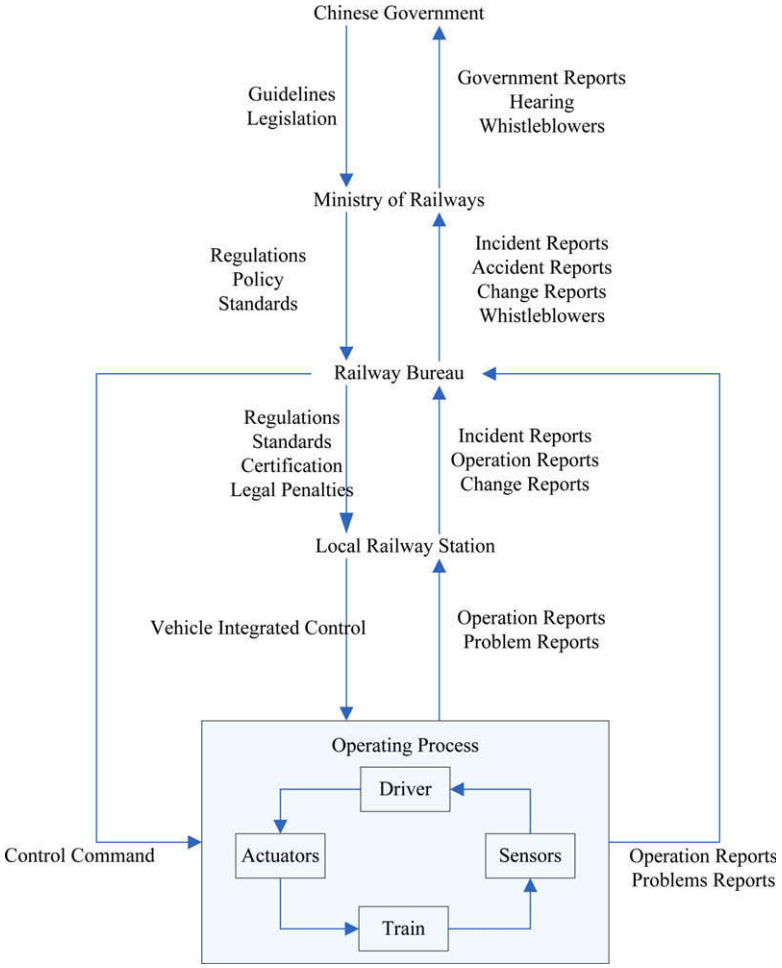


Fig. 3. The hierarchical control structure to ensure the safe operation of trains in china.

Chinese government providing guidelines and legislations down to the train involved in the accident. At the lowest level in the control structure is the driver who not only directly controls the train, but also has the responsibility to provide the operation reports and problem reports to local railway stations and the corresponding railway bureaux. The local railway stations are responsible for implementing the "Vehicle Integrated Control" with the driver to confirm the safe operation requirements, while it must report the

problems and incidents to the corresponding railway bureau. The railway bureaux have the responsibility for making regulations, standards, certifications and legal penalties for its dominated railways administrations while they must report the incidents and accidents to the ministry, and in some special cases they must send directly the temporary control commands to the drivers. The ministry of railways is responsible for making the uniform rules and regulations and standards for the Chinese railways with the supervision of their execution.

Under this control structure, the China–Jiaoji railway accident on April 28, 2008 will be taken as an example to analyze the casual factors and thereby provide some improvement measures. When one train is running on railways, it is confronted with many kinds of dangers, such as derailment, collision, falling from a bridge. In fact, there were two accidents happened in the China–Jiaoji railway accident: the derailment of train T195 and the collision between train T195 and train 5034. The latter accident could be thought as the spreading of the former accident. Based on the STAMP approach, these two accidents will be analyzed respectively in following two sections.

3. STAMP-based analysis on the first accident—derailment of train T195

3.1. Accident process

The accident occurred on the morning of April 28, 2008, between Wangcun and Zhoucun, near Zibo, in Shandong province, People's Republic of China. Train T195 from Beijing to Sifang railway station in Qingdao derailed at 04:38 China Standard Time (CST) on the inside (left) track around a bend (http://en.wikipedia.org/wiki/2008_China_Railways_train_T195_accident). The accident occurred as follow:

- March 2008 – Jinan railway bureau issued traffic control command number 4240, limiting the speed of Jiaoji railway K290 + 784 to K293 + 780 temporarily to 80 km/h.
- April 23 – Jinan railway bureau issued traffic control file number 154, changing the working diagram from April 28, changing the speed limit K290 + 784 to K293 + 780 from temporary to long-term limit. This file was only published on Jinan railway bureau's website and delivered by a relatively slow post mail, and Beijing railway bureau was in the cc. list.
- April 26 – The scheduler in Jinan railway bureau issued traffic control command number 4158, canceling temporary traffic control commands that were previously issued. As the scheduler thought the context of file 154 had been carried out and the speed limit in that section had amended to long-term limit, the command 4240 was also cancelled. However, this command arrived at the Beijing railways bureau earlier than file 154, so that the speed limit for train T195 in that section of railway was restored to 140 km/h.
- The driver of train 2245 reported to the duty man in Zhoucun railway station about the conflict between the command and the file.
- April 28 ~02:30 – Lu Min, the director in duty of Jinan west train schedule duty room, reported to the scheduler in duty, the train 2557's driver noticed the speed limit sign was 80 km/h while the LKJ transport monitor on train displayed as 120 km/h when he was passing down Zhoucun–Wangcun in K293 + 780 M to K290 + 784 M.
- April 28 ~02:35 – Pu Xiaojun, the train scheduler in duty, immediately telephoned Wu Haichun, the director in duty of Jinan locomotive terminal about the speed limit. Wu Haichun said, the train 2245's driver had also reported to him about the problem. The scheduled asked about the speed limit in transport monitor, but Wu said he did not know because the one who is able to change the chip is not directed by the locomotive terminal, but by the electrical terminal.
- April 28 ~02:40 – The scheduler told to the driver of the next train, train 5025, when passing the railway section, if the speed limit show on the signal is different from the speed limit in train's LKJ (Cab signalling) monitor, passing the section at speed of 80 km/h.
- April 28 ~03:00 – Pu Xiaojun, the scheduler in duty, asked Zhoucun East and Wangcun stations' schedulers to tell train drivers for up and down directions, passing the railway section still under the requirement of commands 4240 and 4241 at 80 km/h.
- April 28 ~03:50 – Sui Fuhai, another scheduler in duty, asked train T25's driver what the speed limit was between Wangcun and Zhoucun East. The driver had not passed that section, so he told the scheduler he did not know about it. Then Sui asked the driver to limit the speed to 80 km/h there. When the train passed, the driver told the scheduler the onboard system was shown as limited to 145 km/h there.
- April 28 ~03:55 – Sui Fuhai contacted the T195's driver. There was a long talk, but the scheduler did not clearly tell the driver to limit the speed between Wangcun and Zhoucun east. Since train T195 was late and behind schedule, Sui asked the driver to drive faster, "Do rush on the way." The driver confirmed.
- April 28 04:02 – Jinan railway bureau issued command 4443 and 4444 according to Jinan railway transport mail File [2008] No. 154, required to recheck the speed limit, but the traffic control command was not sent to train T195.
- April 28 ~04:28, the T195 approached to Wangcun station. According to the regulation, the assistant in Wangcun station must contact with the T195's driver and told the driver to limit the speed to 80 km/h, but he did not do this because he saw the T25 had passed that section normally a moment before and thereby thought the T195's driver also knew the speed limit.
- April 28 ~04:38, the T195 derailed on the inside (left) track around a bend.

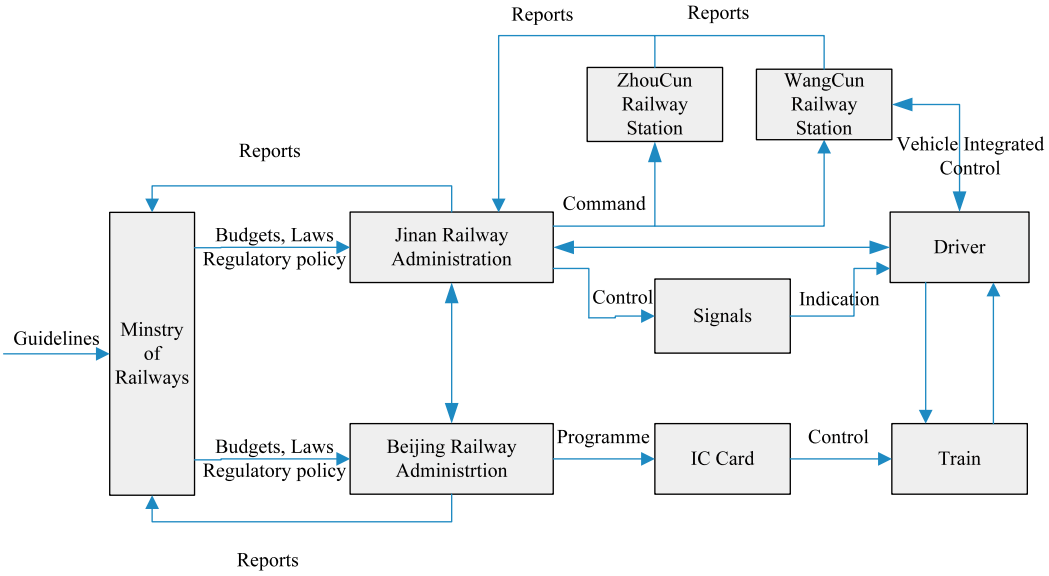
3.2. Causal analysis

3.2.1. The system hazards, system safety constraints, and control structure

According the procedure of STAMP-based accident analysis, the first step is to identify the system hazards, the system safety constraints, and the hierarchical control structure in place to enforce the constraints. The system hazard related to the China–Jiaoji railway accident is derailment of the train. This hazard needs the following system safety constraint: (1) Trains must run within limited speed. (2) Driver must know the correct limited speed through different kinds of ways (e.g. IC cards and the scheduler in duty). Then, according to the accident process introduced in Section 3.1, the hierarchical control structure to enforce above two constraints is shown in Fig. 4, and the safety-related requirements and constraints for each controller are also listed below in Fig. 4.

Each controller in the control structure plays a role in enforcing some safety constraints to prevent initial collapse. The Chinese government is responsible for establishing guidelines and legislations to ensure railway safety. Guidelines are provided to the ministry of railways, but responsibilities for railways safety are primarily delegated to each railway bureau. The ministry of railways is responsible for regulating and overseeing the safe operation of railway systems. They do this by passing laws and adopting government policies and by providing budgets to each railway bureau, such as Jinan railway bureau and Beijing railway bureau. The railway bureaux (Jinan railway bureau, Beijing railway

System Hazard: Train derails.
System Safety Constraints: The safety control structure must prevent derailment of the train.
(1) Train must run within limited speed.
(2) Driver must know the correct limited speed through different kinds of ways(e.g. IC cards and the scheduler).



Safety Requirements and Constraints:

Chinese Government:
- establishing guidelines to ensure the railway system safety.

Ministry of Railways:
- Establish codes of responsibilities, authority, and accountability for each railways administration.
- Provide oversight and feedback loops to ensure that each railways administration is doing their job adequately.
- Enact legislation, regulations and policies to protect the safe operation of trains.
- Ensure those in charge of each railways administration are competent to carry out their responsibilities.

Beijing Railway Administration:
- Program for the LKJ transport monitor according to working diagram and control command.
- Verify the context of received control command with the sender.
- Establish training requirements for train drivers.

Jinan Railway Bureau Operation Management:
- Monitor operations and enforce the legislation, regulations, and policies applying to safe operation of local railway systems.
- Establish training requirements for all staffs in the bureau.
- Establish feedback channels for problems found by drivers and the files and control commands issued by the scheduler in Jinan Railway bureau.

Jinan Railway Bureau Operation:
- Adjust the working diagram according to the railway conditions, establish a file for the adjustment, and send the file to all relative railway bureaus and administrations.
- Track the sending state of the file and control command.
- Establish the temporary control command according to railway conditions and information reported by drivers and staffs in the bureau.
- Send the temporary control command to all relative railway stations and drivers.
- Amend the speed limit signs beside the rails.

WangCun Railway Station:
- Implement the "Vehicle Integrated Control" carefully with the driver.

Driver:
- Notice the speed limit displayed on the LKJ transport monitor and operate the train according to that speed limit.
- Pay attention to the speed limit signs beside the rails and operate the train according to that speed limit.
- Operate the train according to the control command issued by the scheduler in Jinan railway bureau.
- Confirm the actual speed limit with the assistant in Wangcun station.

Fig. 4. The overall train operation control structure in the China–Jijiao railway accident and the safety-related requirements and constraints for each controller.

bureau) have primary responsibility for regulating and for enforcing legislations, regulations and policies that apply to the construction and operation of local railway systems. Each bureau has also responsibility for continuing education requirements for staffs to maintain competence as knowledge about railway safety, for sending control command to each railway station, for changing the speed limit sign beside the rails and for programming for the LKJ transport monitor. Each railway station has responsibility for

carefully implementing the "Vehicle Integrated Control" with the passing trains and confirming the safe operation information (including the control command issued by scheduler in local railway bureau) with the drivers. The drivers have direct responsibility for the train safety. They operate the trains according to the speed limit displayed on the LKJ transport monitor, the speed limit signs beside the rails, and the control command issued by the scheduler in local railway bureau. However, if they found some problems endangering trains safety, they must reports to the schedulers in Jinan railway bureau.

Together, the safety constraints enforced by all of these controllers must be adequate to enforce the overall safety constraints. Understanding the first accident requires understanding the role of each controller in the hierarchical control structure. The inadequate control (in terms of enforcing the safety constraints) exhibited by each controller in the China–Jiaoji railways accident are discussed in following subsections.

3.2.2. Driver

Most hazard analysis techniques and accident investigations consider the immediate operators of the system. Fig. 5 shows the results of a STAMP analysis of the flaws by train T195's driver. The safety requirements and constraints on the driver were that they must notice the speed limit displayed on the LKJ transport monitor and must operate the train according to that limit. However, the Beijing railway bureau received the control command requiring to cancel the temporary speed limit (80 km/h, contained in the control command 4240 issued in March) in that section before receiving the file 154 (changing the speed limit to be long-term limit), so the speed limit on train T195 in that section displayed on the LJK transport monitor was changed to be 145 km/h.

Although the problem (inconsistency between the speed limit on the LJK transport monitor and the actual speed limit) had been found and the Jinan railway bureau issued new control command 4443 and 4444 requiring drivers to limit the speed to 80 km/h in that section, this new control command was not sent to train T195. When train T195 approached to Wangcun railway station, according to the regulations, the staffs in that station should carefully implement the "integrated vehicle control" and confirm the actual speed limit with the driver. But due to their negligence, the driver passed that station without knowing the actual speed limit.

In addition, the speed limit signs beside the rail show the actual speed limit, but the driver did not pay attention to that. There may be several reasons for this mistake. First, due to busy operation task, most train drivers in china should work for more than 200 h every month, even over 300 h, which cause their tiredness. Moreover, there was only one driver operating at 4 o'clock in the morning (the time of the accident) that is the most tiredness time for human bodies. Second, it may be as result of his bad occupational habit. To ensure the train operated on schedule (If the train is late, the driver will take responsibility for that and his salary will be cut), drivers have to operate the train at a speed approached to the speed limit. Especially in this accident, the train was late while local scheduler in duty also asked him to do rush on the way, so the driver paid more attention on the LKJ transport monitor and operated the train at the speed approaching to the speed limit. Third, the diameter for the speed limit signs with yellow background and black font was only 30 cm while the driver operated the train at a speed 131 km/h, it is difficult to see clearly the signs. Forth, it is the most important thing for the driver to pay much attention to all speed limit signs besides the rails, but the driver did not take his responsibility and ignored its importance, which was also due to inadequate training.

Together, the driver did not know the actual speed limit while the train was late, and then the driver thought operation at a high speed according to the LJK transport monitor was safe, which caused the accident happened.

3.2.3. Beijing railway bureau

Fig. 6 summarizes the role of Beijing Railway Bureau in the accident. The Beijing Railway Bureau has primary responsibility for programming for the LKJ transport monitor according to the

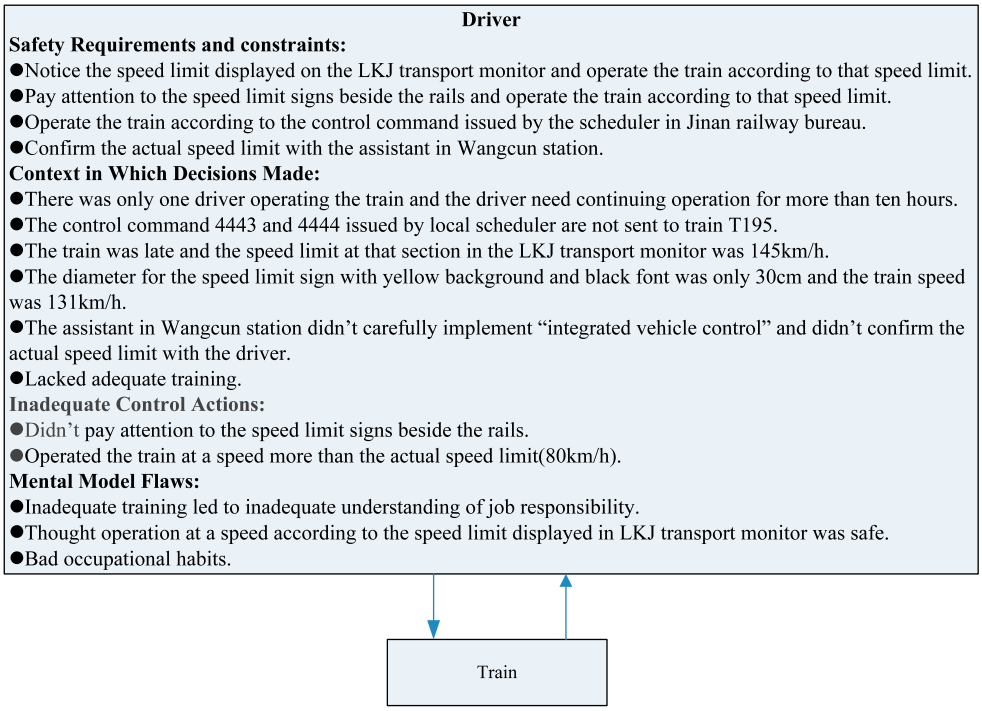


Fig. 5. The role of the train T195's driver in the accident.

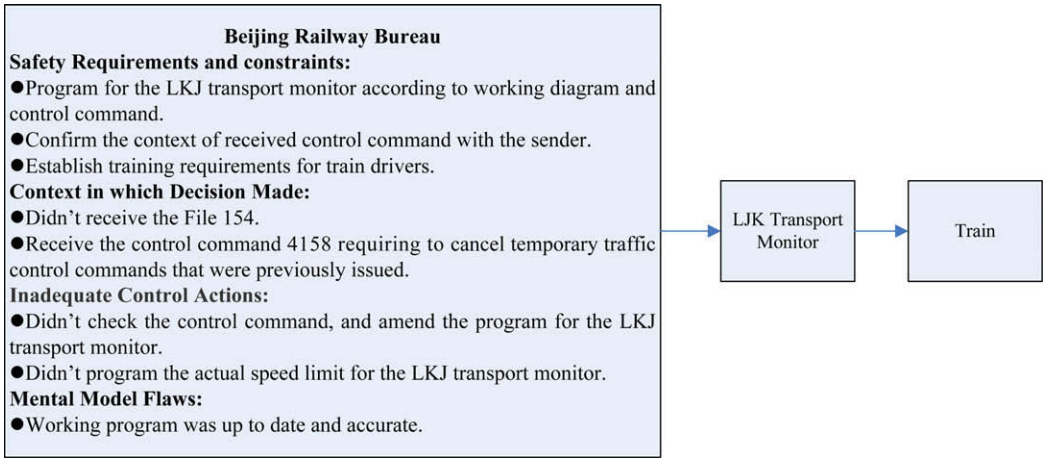


Fig. 6. The role of the Beijing railway station in the accident.

working diagram and control commands, confirming the context of received files or control command with the sender, and establishing training requirements for train drivers. However, they received the control command 4158 requiring to cancel the temporary speed limit in that section before receiving the file 154, so the speed limit on train T195 in that section had been programmed to be 145 km/h in the LJK transport monitor, which was not the actual speed limit 80 km/h. But in fact, the control command said: "According to the file 154 used for adjusting the working diagram, from the time 0:00 on April 28, 2008, cancel the control command 4240 issued on March 23, cancel the control command..." This command had referred to the file 154, Beijing Railway bureau did not check the file 154 and then amended the program for the LJK transport monitor so that the speed limit in that section returned to be 145 km/h, which was one reason to cause the accident.

3.2.4. Jinan railway bureau and Wangcun railway station

The accident happed in the place near the Wangcun railway station dominated by the Jinan railway bureau. In this section, the role of Jinan railway bureau and Wangcun railway station in the accident will be analyzed, as can be seen in the Fig. 7. Wangcun railway station has responsibility for carefully implementing the "Vehicle Integrated Control" with the driver. However, when train T195 approached to that station, the assistant did not confirm the actual speed limit with the driver. According to the investigation, there may be several reasons for this mistake. First, due to high traffic density, there were more than 160 vehicles passing through the Wangcun station per day. So the assistant had to implement the "Vehicle Integrated Control" with a driver every 9 min, even 2 or 3 min in the rush hour. This high workload increased the probability that the assistant did not carefully implement the "Vehicle Integrated Control" with the driver due to some subjective guess. Second, there was a rumor to abolish the Jinan railway bureau, some of which had been rectified. It made the people affiliated to Jinan railway bureau feel nervous and could not concentrate on their job. Third, due to inadequate training, the assistant ignored the importance of confirming the actual speed limit with the driver.

The assistant in Wangcun railway station did not intentionally violate the rules and put the train T195 at risk. Before train T195 approached to the station, train T25 with the same vehicle type had passed that section safely, and then the assistant thought train T195 should also have received the control command from the scheduler in duty in Jinan railway bureau and would be safe to pass that section.

To analyze the role of Jinan railway bureau in the accident, the discussion will be performed from two aspects. One is the Jinan railway bureau operation while the other is the management. For the former, they has primary responsibility for adjusting the working diagram according to the railway conditions, establishing a file for the adjustment and sending the file to all relative railway bureaux and administrations. However, the staff in the bureau ignored the high priority of abiding by the guidelines and regulations so that establishment process of the file 154 violated the regulation. According to the regulation, they must send the file 154 to the ministry of railways for confirmation and then amend the data for LJK transport monitor. But they did not do like that and they also did not check whether others had received that file so that the long-term speed limit in the accident section had not been amended correctly. At the same time, the scheduler in Jinan railway bureau thought the speed limit in that section had been changed to long-term limit 80 km/h, and then another control command to cancel the temporary speed limit in that section had been issued, which finally caused the speed limit in LJK transport monitor on train T195 was changed to 145 km/h. Although the problem (inconsistency between the speed limit on the LJK transport monitor and the actual speed limit) was found through the feedback by other drivers and new control command 4443 and 4444 requiring the speed limit to 80 km/h at that section was issued, this new command was forgotten to send to train T195. In addition, the scheduler in duty contacted with the train T195's driver through wireless phone, he did not clearly expressed his idea such that the driver still did not know the actual speed limit when the communication was over. These mistakes may be due to the inadequate training or the rumor to abolish the Jinan railway station, causing the staff in the bureau felt nervous and could not concentrate on their jobs. In addition, contacting with the driver only through wireless phones was not very effective, due to the man-made mistake, the wireless phones sometimes could not clearly express the idea, so more effective means could have been employed.

For the latter—Jinan railway bureau operation management, they have primary responsibility for monitoring operations and enforcing the legislation, regulations, and policies applying to safe operation of local railway stations, establishing training requirements for all staffs in the bureau, establishing feedback channels for problems found by drivers and the files and control commands issued by the scheduler in Jinan railway bureau. But from the above discussion, the disordered management indicated that they had inadequate monitoring and supervision of the operations, which may also be due to bad effect of the rumor. Moreover, the

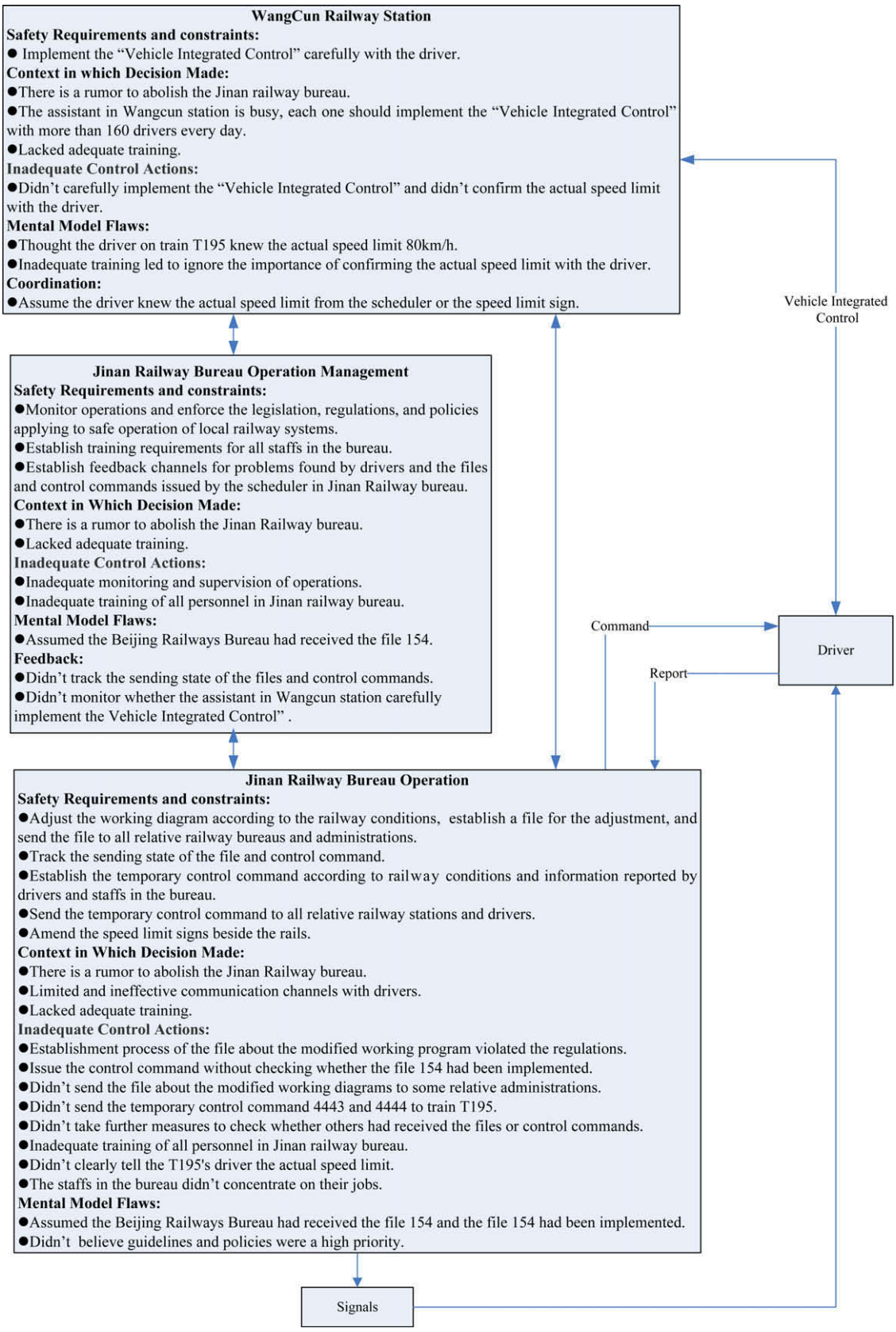


Fig. 7. The role of the Jinan railway station and Wangcun railway station in the accident.

Jinan railway bureau also did not perform adequate training to the personnel so that the staffs either violated the regulations or did not know the regulations. In addition, lacked feedback channels were also one reason to cause the accident, i.e. the Jinan railway

bureau did not track the sending state of the files and control commands, and they also did not monitor whether the assistant in Wangcun railway station carefully implement the "Vehicle Integrated Control".

3.2.5. Ministry of railways

Fig. 8 shows the role of ministry of railways in the accident. The ministry of railways is responsible for establishing codes of responsibilities, authority, and accountability for each railways administration, providing oversight and feedback loops to ensure that each railway administration is doing their job adequately, enacting legislation, regulations and policies to protect the safe operation of trains, and ensuring those in charge of each railway administration are competent to carry out their responsibilities. However, the ministry of railways had inadequate monitoring and supervision of the safety management for Jinan railways administration and did not carefully check the existing problems in Jinan railway bureau. Three month before the accident, On January 23, 2008, a major accident happened in Jiaoji railways, causing 18 fatalities and nine injuries. The disordered management in Jinan railways bureau was not found and curtly dealt with by the ministry of railways such that the poor management was not improved, causing this more major accident.

Moreover, the ministry had ignored the effect of the rumor of abolishing the Jinan railway bureau and no further measures were taken to reduce its bad effect, which caused all staffs in Jinan railway bureau felt nervous and could not concentrate on their jobs. Finally, as the traffic flows were increasing day by day, to ensure their operation on schedule, the ministry required the driver to operate the train at a speed approached to the speed limit, which enhanced the accident probability.

In this section, based on the STAMP approach, the derailment of train T195 has been analyzed and many causal factors have been identified. The improvement measures will be discussed in next subsection.

3.3. Improvement measures

In Section 3.2, based on the STAMP approach, the roles of each controller in the control structure have been analyzed and many causal factors have been identified. To prevent similar accident in the future, some improvement measures proposed as follow can be considered:

(1) Managers in all levels of railway system should strengthen personnel training and railways safety culture should be emphasized. Drivers, staffs or assistants in each railway station, schedulers and all other personnel in each railway bureau should be more competent and more familiar with their job responsibilities. They all should abide by regulations with a high priority. For example, drivers must pay much attention to speed limit signs; "Integrated Vehicle Control" should be implemented strictly according to the format requirements. The establishment process of important files must be based on the regulations. In addition, Staffs in some departments should not only know their own responsibilities, but also know the responsibilities of other departments. This will be helpful to deal with some problems related to many departments. For example, when inconsistency between the speed limit on the LJK transport monitor and the actual speed limit had been found, to find out the cause, the scheduler can save a lot of time to find the people responsible for amending speed limit on the LJK transport monitor if he's familiar with other departments' responsibilities.
(2) More train drivers and more assistants responsible for "Integrated Vehicle Control" are needed so that their workload can be reduced, which can decrease the probabilities of mistakes or violations caused by tiredness.
(3) Some regulations should be added or modified. For example, drivers should not be punished (cut salary) due only to behind schedule, some punishment or encouragement policies must consider the principle—safety first. In addition, the diameter, background color and font of speed limit signs besides rails should be adjusted so that they are striking and be easy for drivers to discern the contents.
(4) Ministry of railways and each railway bureau should pay more adequate monitoring and supervision on safety management. Once an accident happened, appropriate method should be used to analyze causal factors and then improvement measures should be taken to avoid future one. In addition, all managers in all levels should never ignore the bad effects of rumors and must take adequate measures to reduce their influences.
(5) Many feedback or communication channels in the control structure should be added or perfected. For example, the format of communication contents between driver and scheduler should be standardized so that ideas can be clearly delivered during the communication; A software is needed to automatically send all temporary control command to relative trains and these relative trains are determined by this software; A special device can be designed on the train which can show the actual speed limit when train enters a section and this can be realized by cooperation with China

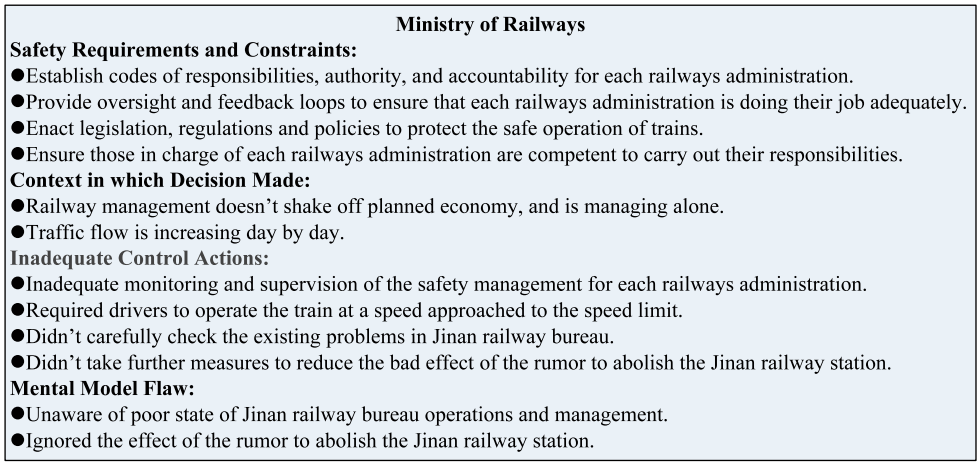


Fig. 8. The role of ministry of railways in the accident.

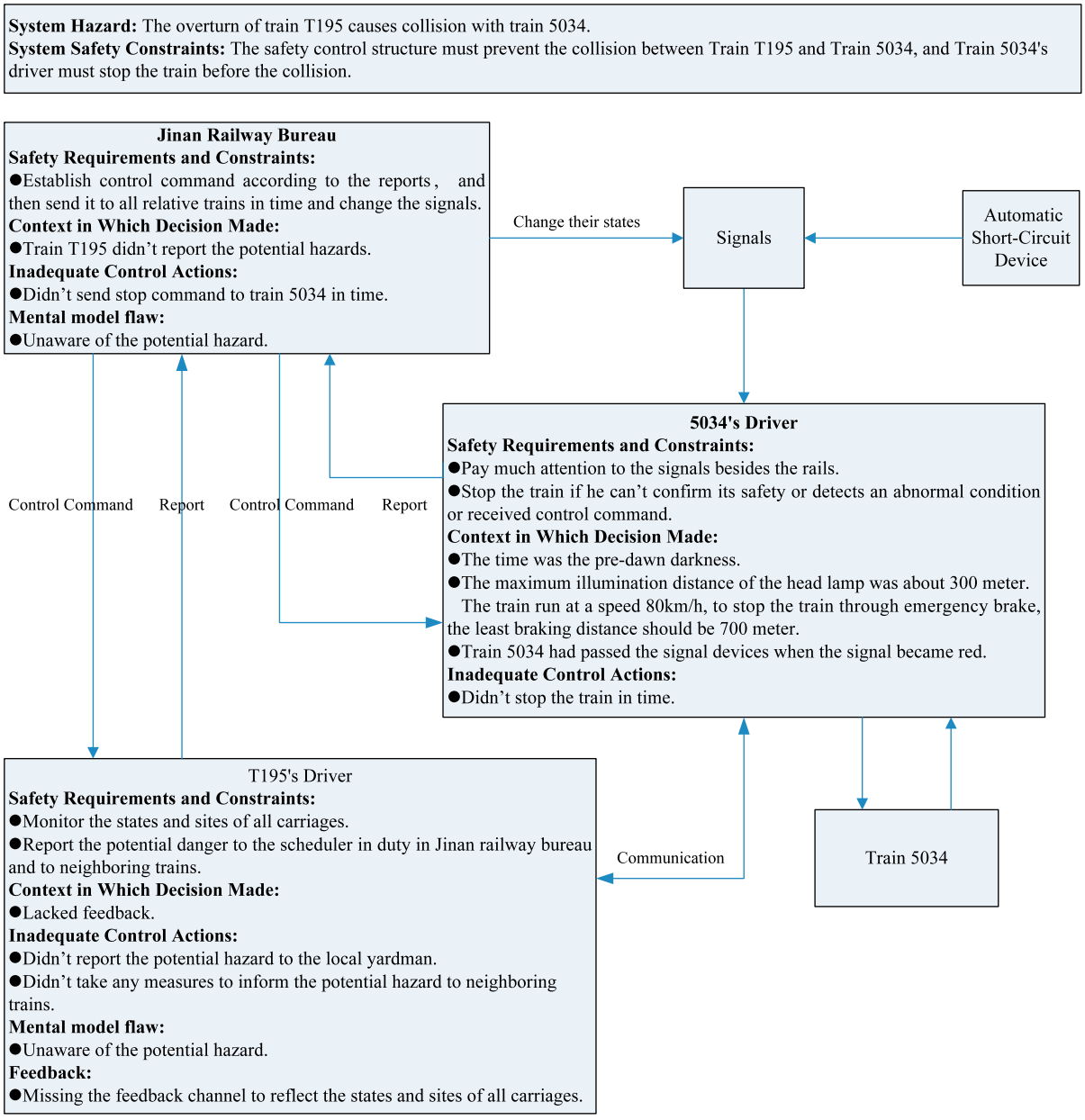


Fig. 9. The system hazards, the system safety constraints, the control structure and system component safety constraints in the second accident.

Mobile. In addition, many feedback channel should be added, such as a feedback channel should be established by each bureau to check the content of each control command and each file from other bureaux; a feedback channel should be established to track sending state of files and control commands; a feedback channel should be established to monitor whether "Integrated Vehicle Control" has been carefully implemented.

4. STAMP-based analysis on the second accident—collision between train T195 and train 5034

4.1. Accident process

After train T195 derailed at 04:38 China Standard Time (CST) on the inside (left) track around a bend, train 5034 from Yantai to Xuzhou, coming from the other direction on the outside track, collided with it at the K290 + 940 m mileage marker on the double tracked Jiaoji Railway at approximately 04:41 CST.

When the T195's driver operated the train to the accident site, he felt the train tail shook and then tried to stop the train, but found that the train had been ceased by itself. (This function has been considered in the process of train design.) After checking the train, he found the train had no net pressure, no wind pressure, and no abnormity. According to the regulation, the driver must count the number of carriages, and then he found some carriages had separated. But he did not know these carriages had derailed and toppled on the other rails.

The overturn of train T195 triggered the automatic short-circuit device and all the signals in that zone became red, and then no train can enter into that zone. But it is unfortunate that train T195 had entered into that zone. The time was the pre-dawn darkness while the maximum illumination distance of the head lamp for train 5034 was about 300 m. Moreover, if train 5034 was

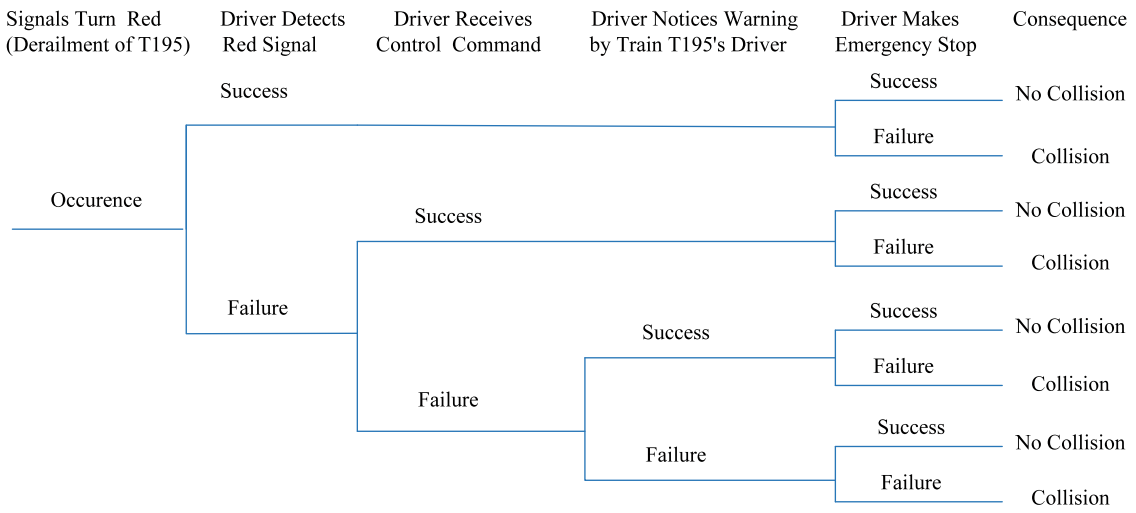


Fig. 10. Event sequences for the collision after the derailment of train T195.

running at a speed 80 km/h, to stop the train through emergency brake, the least braking distance should be 700 m. So emergency brake was useless and it is too late when train 5034's driver found the hazard. Finally train 5034 collided with the toppled carriages of train T195, increasing the number of injuries and fatalities.

4.2. Causal analysis

According to the procedure of STAMP-based accident analysis, the system hazards, the system safety constraints, the control structure and system component safety constraints have been shown in the Fig. 9. The system hazard related to the second accident was that the overturn of train T195 cause a collision with train 5034. This hazard leads to the following system safety constraints: the safety control structure must prevent the collision with train T195 and the train 5034's driver must stop the train before the collision.

For train T195's driver, he has the responsibility for monitoring the states and sites of all carriages and reporting the potential danger to the scheduler in duty in Jinan railway bureau and to neighboring trains. However, when train 195 derailed, due to lacked feedback to monitor the sites of all carriages, the driver did not know the train had toppled on the other rails and did not report the potential hazard to the local scheduler in duty and also did not take any measures to inform train 5034 on the other rails. Further, the Jinan railway bureau was also unaware of the potential hazard and they didn't send stop command to train 5034.

Although the automatic short-circuit device caused all signals in that zone became red, it is unfortunate that the train had entered that zone and the driver saw no signals. Because the braking system of train 5034 only had limited capability, the driver could not stop the train in time when he found the danger. Finally, the second accident happened, causing more injuries and fatalities.

4.3. Improvement measures

In Section 4.2, based on the STAMP approach, the causal factors in the second accident have been identified. To prevent similar accident in the future, some improvement measures proposed as follow can be taken:

(1) Many feedback or communication channels in the control structure should be added. If train 5034 had a signal device, which could reflect the state of the automatic short-circuit device and forcibly stop the train when the driver does not make an appropriate response, and then the train 5034 may be stopped in time and the second accident can be avoided. In addition, if train T195 had a device to reflect the states of all its carriages, and then he could find the potential danger in time so that the Jinan railway bureau could send new control command in time or train T195's driver could take some measures to inform train 5034's driver, and finally the second accident may be avoided.
(2) Some devices on the train should be updating. For example, head lamps should be replaced by more effective ones and braking systems should be more capability so that the maximum illumination distance of head lamp is larger than braking distance and then train can be stopped before collision.

5. Modeling accident spreading process

From above analysis, it can be found that the second accident is the spread of the first accident. To quantify the relationships between them, Probabilistic Risk Assessment (PRA) method can be used. This method needs to identify all possible accident event sequences leading to the accident and then take an appropriate measure to estimate the accident sequence. So the most important thing is to find out accident occurrence conditions, whose correctness has a large impact on the validity of analysis results. Usually, the derivation of occurrence conditions depends on the subjective judgment of system analyst and designers, which might cause an error. To obtain an objective accident occurrence conditions, the STAMP-based analysis is useful. From the control structure in Fig. 9, train 5034 was directly affected by its driver and decisions of 5034's driver were influenced by three factors: the signals, the Jinan railway bureau and train T195's driver. To affect the decisions of 5034's driver, the Jinan railway bureau was through sending control commands and T195's driver was by use of warning. So there are totally four factors leading to the second accident after the first accident happened. They are respectively, the signals, the Jinan railway bureau, train T195's driver and train 5034's driver. According to these factors, the relationship between the two accidents can be described by the event tree in the Fig. 10.

In the China–Jijiao railway accident, accident event sequences leading to the second accident were the lowest case in the Fig. 10, namely, derailment of train T195—signals turn red—driver did not detect the red signals—driver did not receive control command—driver did not notice warning by train 5034's driver—driver makes emergency stop, but it is pity that it is too late for

the driver to find the danger while the braking system was incapability, finally, the second accident happened. By use of event tree, we can further calculate the probability of occurrence of the second accident after the first accident happened, and then it is possible to analyze the accident spreading, and further be useful to accident response management and design safer system in a board sense.

6. Conclusion

Each hazard analysis technique is based on a model of accident causation. Most of traditional accident models view accidents as resulting from a chain or sequence of events, such models are usually used to assign blame for the accident and ineffective to prevent future ones. Just as the example investigated in this paper, although some people in the China–Jijiao railway accident have been arrested for their errors, it is ineffective to prevent future one so that another accident happened about half a year latter on October 13, 2008. The STAMP model based on basic system theory concepts is effective to understand why accidents happened so that many improvement measures can be found to prevent future ones.

In this paper, taking the China–Jiaoji railway accident happened on April 28, 2008 as an example, the STAMP-based accident analysis method has been used to analyze railway accident. Some improvement measures have been proposed after the discussion. Moreover, the occurrence of one accident can cause many other accidents happen, this paper has analyzed the spreading process and their relationships have been modeled. The quantitative analysis on the spreading probability is the next step in this research. When the interaction can be quantified, then the accident spreading process can be analyzed in a broad sense, which will be helpful to design constraints to prevent the spreading and establish effective emergent measures for accident response management.

References

Ferry, T.S., 1988. Modern Accident Investigation and Analysis, second ed. Wiley, New York.

Fukuda, Hisaji, 2002. A study on incident analysis method for railway safety management. Quarterly Report of RTRI 43 (2), 83–86.

Herring, Margaret Stringfellow, Owens, Brandon D., Leveson, Nancy, Ingham, Michel, Weiss, Kathryn Ann, 2007. A Safety-driven, Model-based System Engineering Methodology, Part I. MIT Technical Report, December 2007. <http://sunnyday.mit.edu/papers.html#system-safety>.

Hollnagel, E., 2004. Barriers and Accident Prevention. Ashgate, Hampshire.

Kohda, Takehisa, 2008. Accident Analysis of Complex Systems Based on System Control for Safety. Handbook of Performability Engineering. Springer, London. pp. 683–697.

Leveson, N.G., 2002. System Safety Engineering: Back to the Future. Aeronautics and Astronautics Department, Massachusetts Institute of Technology, Cambridge, MA. <http://sunnyday.mit.edu/book2.pdf>.

Levenson, Nancy, 2004. A new accident model for engineering safer systems. Safety Science 42 (4), 237–270.

Leveson Nancy G. 2008. Applying systems thinking to analyze and learn from events. In: Proceedings of Network 2008, Event Analysis and Learning from Events 42.

Leveson, N.G., Allen, P., Storey, Margaret-Anne, 2002. The analysis of a friendly fire accident using a systems model of accidents. In: Proceedings of the 20th International System Safety Conference, Denver, Colorado, 5–9 August.

Niwa, Yuji, 2009. A proposal for a new accident analysis method and its application to a catastrophic railway accident in Japan. Cognition, Technology & Work. 11 (3), 187–204.

Qureshi, Z.H., 2007. A review of accident modelling approaches for complex critical sociotechnical systems. Proceedings of the Twelfth Australian Workshop on Safety Related Programmable Systems.

Reason, J., 1990. Human Error. Cambridge University Press, Cambridge, UK.

Reason, J., 1997. Managing the Risks of Organizational Accidents. Ashgate, Aldershot, Hants.

Santos-Reyes, J., Beard, A.N., 2006. A systemic analysis of the Paddington railway accident. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 220 (2), 121–151.

Santos-Reyes, Jaime, Beard, A.N., 2008. A systemic analysis of the Edge Hill railway accident. Accident Analysis and Prevention. doi:10.1016/j.aap. 2008.05.004.