A Hybrid Human and Organisational Analysis Method for Railway Accidents based on STAMP-HFACS and Human Information Processing

Chenling Li[1,3], Tao Tang[1], Maria Mikela Chatzimichailidou[2], Gyuchan Thomas Jun[3] and Patrick Waterson[3]

[1] State Key Laboratory of Traffic Control and Safety,
Beijing Jiaotong University,
Beijing, 100044, China

[2]WSP UK
Systems Assurance Team,
Rail,
London, EC2M 4YE,
United Kingdom.

[3]Human Factors and Complex Systems Group,
Loughborough University Design School,
Loughborough University,
Loughborough, LE11 3TU,
United Kingdom.

Address for correspondence:
Prof. Tao Tang
State Key Laboratory of Traffic Control and Safety,
Beijing Jiaotong University,
Beijing, 100044, China

[1] Email: ttang@bjtu.edu.cn

A Hybrid Human and Organisational Analysis Method for Railway Accidents based on STAMP-HFACS and Human Information Processing

Abstract

Safety is a constant priority for the railway industry and there are numerous hazards in and around the rail system which may result in damage to train and environment, human injury and fatalities. Low levels of human and organisational performance have been shown to be a prime cause of railway accidents and a number of accident models and methods have been developed in order to probe deeper into the role played by organisational factors in accident causation. The Systems–Theoretical Accident Modelling and Processes (STAMP) method for example, represents a promising systematic and systemic way of examining sociotechnical systems such as the railway. Another method, the Human Factors Analysis and Classification System (HFACS), based upon Reason's model of human error in an organisational context, has also proved popular as a human factors accident analysis framework. However, human factors elements are still somewhat limited and under-specified and these managerial and social issues within an organisation are simply regarded as sources of failure in the control constraints of STAMP. HFACS likewise, categorises accident data rather than analysing it in more depth. In this context, a hybrid human and organisational analysis method based on HFACS-STAMP (HFACS-STAMP method for railway accidents, HS-RAs) is proposed to identify and analyse human and organisational factors involved in railway accidents. Using the categories of human errors derived from HFACS and the structured systematic analysis process of STAMP, the HS-RAs method provides a mechanism by which active failures can promulgate across organisations and give a systemic analysis of human error in accidents. Combined with human information processing, the HS-RAs method gives a detailed causal analysis of human errors from receiving information to implement control actions. At last, the HS-RAs method is demonstrated using a case study of the 2011 Yong-Wen railway collision. A number of prominent accident causes of human factors are revealed and necessary countermeasures are proposed to avoid the recurrence of similar accidents. The HFACS-STAMP hybrid method has several advantages and can contribute to railway safety by providing a detailed analysis of the role of human error in railway accidents.

Keywords: Human and organisational factors, STAMP, HFACS, human information processing, accident analysis, Yong-Wen railway accident

1. Introduction

At the end of 2015, the amount of track covered by the railway industry in China had reached 121,000km including 19.000km high-speed railway lines. In terms of passenger numbers China ranks in the first place in the world with over 1.1 billion trips made on high-speed bullet trains alone. The complex control system and serious operational demands circumstance of the Chinese railway system represent a typical socio-technical (Wilson et al., 2007) and safety-critical system (Li et al., 2013), in which any technical and human errors can lead to human death, injury and financial loss. A number of prominent railway accidents have happened recently. A high-speed railway derailment occurred in Germany on 3rd June, 1998 for example, resulting in 101 fatalities (Esslinger et al., 2004). In Chinas a high-speed railway crash at Wenzhou in July, 2011 caused 40 fatalities and 172 injuries (SAWS, 2011). More recently, the Santiago de Compostela derailment in Spain in July, 2013 resulted in 78 fatalities and 145 injuries (Shultz et al., 2016). Human error has long been recognised as the predominant factor in aviation mishaps (Reason, 1997). Estimates of the proportion of mishaps due to human error generally range between 60% and 80% (O'Hare et al., 1994). It is widely believed that human factors make a major contribution to most accidents across a range industries including railway, aviation, maritime and mining. Human error is generally thought as the result of a range of factors involving people tools, tasks, and operating environment (Wilson et al., 2007). Progress on safety comes from understanding the connections between these factors.

A number of human factors methods have been developed in order to identify the human and organisation factors involved in accidents. One of the most widely used systemic accident causation models (Dokas, et al., 2013; Chatzimichailidou and Dokas, 2016) is the Systems–Theoretical Accident Modelling and Processes (STAMP) method. STAMP is based on system and control theory and focuses on safety as a control problem and an emergent feature of the system (Leveson, 2004). STAMP regards human errors as the symptoms of the system rather than causal factors of accidents requiring analysts to consider how system conditions may lead to "errors". STAMP provides a holistic view of human errors and organisational factors in its analysis, the human factor element of STAMP is somewhat limited and under-specified and managerial and social issues in a socio-technical system are simply viewed as sources of failure in terms of control constraints (Harris and Li, 2011). In addition, STAMP does not provide extensive guidance for understanding why humans behave the way they do (e.g., constraints covering human information processing - France, 2017) and as a result analysts have found it difficult to identify human and organisational failures (Dong, 2012; Suo, 2012; Song, 2012; Niu et al., 2014).

The Human Factors Analysis and Classification System (HFACS) is another widely used human factors accident analysis framework. HFACS is a generic human error-coding framework based on Reason's Swiss Cheese Model (Reason, 1990) and developed by Shappell and Wiegmann (2000). HFACS analyses human error at four levels: Unsafe acts, Preconditions for unsafe acts, Unsafe supervision and Organisational influences. One problem, however, is that HFACS is sometimes seen as over-specifying the factors in the levels and analysts can miss out important factors simply because they were not covered by the method HFACS (e.g. interactions between groups and organisational decisions are often not included in the analysis - Stringfellow, 2010). One potential improvement might be that the HFACS classification system would be more comprehensive if it were applied to the control action analysis in the STAMP safety control structure. In the current paper, a hybrid human and organisational analysis method based on HFACS-STAMP for Railway accidents (HS-RAs) is proposed in order to improve the identification and classification of human and organisational factors involved in railway accidents. Combined with the general process of human information processing (HIP) made up of Detection, Identification, Decision and Action (Nagel, 1988), the HS-RAs method can give a detailed analysis of human errors (construct causal scenarios) and thereby probe deeper into the relationship between causal factors and human error. The proposed hybrid method is illustrated using a case study, namely the Yong-Wen railway collision which occurred on 23 July, 2011. The prominent accident causes of human factors are revealed, and necessary preventive measures are proposed to avoid the recurrence of similar accidents. As a result, we argue that the HFACS-STAMP approach can contribute railway safety by giving a detailed analysis of human errors in railway accidents.

2. Accident analysis, cybernetics and human error

2.1 Systems–Theoretical Accident Model and Processes (STAMP)

The STAMP method is based on systems and control theory and also draws on a rich tradition of work in cybernetics (Wiener, 1948) covering the interaction between humans and their environments. STAMP focuses on safety as a control problem and emergent system properties (e.g. safety) are controlled by imposing constraints on the behaviour and interaction of system components (Leveson, 2012). Similar to other earlier cybernetic models (e.g.. Beer's (1984) Viable Systems Model), STAMP views systems as interrelated hierarchical levels of controls and constraints with each level in the hierarchy imposing constraints on the level below. Three basic constructs are used by STAMP to determine why control was ineffective and resulted in an accident: safety constraints, hierarchical

safety control structures, and process models. Safety constraints can be barriers or activities which require some action to provide protection (i.e. detection, measurement, diagnosis or response to a hazard). Accidents occur when system safety constraints are inadequate or not enforced (Leveson, 2004). Hierarchical safety control structures are used by STAMP to describe the composition of systems. Each hierarchical level of a system imposes constraints on, and controls the behaviour of, the level beneath it. Control (two-way communication) processes operate between system levels to enforce the safety constraints. Process models are incorporated into STAMP as any human or automated controller requires a model of the process they are responsible for controlling if they are to be effective (Leveson, 2012). STAMP regards human error as the symptom of the system rather than of specific individuals and a key intention is to avoid the promotion of a blame culture. Mental models (the process model for human controller) have been introduced in the STAMP analysis in order to cover human control structures in the system (Leveson 2012; Ouyang et al., 2010). The analysis depicts flaws across the entire safety control structure of the system, as well as the interaction between those structures and their control failures that resulted in the accident. STPA (Systems Theoretic Process Analysis) is a hazard analysis method, and CAST (Causal analysis using STAMP) is an accident analysis method based on STAMP. STAMP has been used previously to analyse rail accidents and incidents (e.g. Ouyang et al., 2010; Song et al., 2012; Suo, 2012; Dong, 2012; Underwood, Waterson, 2014; Niu et al., 2014; Liu et al., 2016; Wang, 2016). Stringfellow (2010) and France (2017) have additionally added into STAMP a human error taxonomy and organisational error taxonomy to support analysis. However, the STAMP taxonomy of control failure is generic in nature (not restricted to a particular domain) and is thus less restrictive than that provided by HFACS (Salmon et al., 2012). STAMP applies control theory even to the analysis of human and organisational factors, so there is potential to adopt a human information processing framework or task-based framework in order to categorise/analyse human and organisational factors (Stringfellow, 2010).

2.2 Human Factor Analysis and Classification System (HFACS)

Based on the popular accident causation model, the Swiss Cheese model (Reason, 1990), HFACS was developed in order to provide a theory-driven structure to analyse and classify operator errors in naval aviation accidents and mishaps (Shappell and Wiegmann, 2000). The Swiss Cheese Model describes active failures (which are the errors proximal to the accident, associated with the performance of front-line operators in complex systems) and latent failures (distal errors and system misspecifications, which lie dormant within the system for a long time). Those failures act like the “holes” in the different cheese slices and can result in a hazard triggering an accident causing harm to people, assets and the

environment when the “holes” in a system’s defences alignment. There are four classification levels in HFACS for Unsafe Acts (Level 1), Preconditions for Unsafe Acts (Level 2), Unsafe Supervision (Level 3) and Organisational Influences (Level 4). Unsafe acts of front-line operators which led directly to the accident are viewed as arising through human error. Preconditions for Unsafe Acts represent the environmental conditions under which the unsafe acts took place, (e.g, poor team working, and the operators’ physiological state). Unsafe supervision is one of the most important defences for unsafe acts and their preconditions. Poor decision-making by management, for example, can directly affect supervisory practices, as well as the conditions and actions of operators. HFACS has been used to be used in the past to carry out railway accident analysis (Zhan et al., 2017; Madigan et al., 2016; Kim et al., 2008; Oh et al., 2006; Reinach and Vale, 2006).

2.3 Human information processing

The field of human factors examines the relationships between humans and technology. It is concerned with interactions, both physical and cognitive, between the human and their tasks, as well as the quality of performance of those tasks. Thus, it offers a way to understand why human errors happen in their dynamic task processing. Nagel (1988) has suggested that it is possible to cover most of the possible causes of human error in the cockpit with a three-stage information processing models of human performance, which are Information, Decision and Action. A commonly used model of human information processing is that described by Wickens and Flach (1988). Wickens and Flach (1988) summarise the process in which environmental input from the sensory system passes through successive stages of perception, working memory and decision-making. Long-term memory and short-term memory create a mental representation of the current state of the world, like the controller mental model for the controlled process state.

3. Methodology

3.1 Framework for the proposed methodology

Instead of using a single method in isolation, this study proposed a hybrid accident analysis methodology by integrating HFACS-STAMP with human information processing for railway accidents (the ‘HS-RAs’ method). There are different ways with which to integrate STAMP and HFACS methods. For example, Harris and Li (2011) developed HFACS-STAMP – an extension of the HFACS methodology – that can accommodate errors promulgating across organisational

boundaries reflecting the open system nature of modern airline operations. Lower et al. (2015) developed a hybrid model based on STAMP-HFACS and fuzzy sets in order to facilitate risk analysis of serious air traffic incident which focuses on identifying adverse relationships between the components by connecting the elements in the HFACS categorisation system with the STAMP control structure. In this present study, HS-RAs has been developed incorporating HFACS levels for errors categories into the STAMP safety control structure for analysis based on human information processing. The proposed conceptual model framework is presented in Figure 1.

Figure 1 about here

The framework consists of three parts: (1) safety control structure and analysis steps are captured using STAMP; (2) HFACS is used to assist in identifying human and organisational errors which contributed to system accident; and, (3) the four stages of human information processing as described by Wickens and Flach (1988).

3.1.1 The extension - HFACS categories

Zhan et al. (2017) put forward a framework based on HFACS (HFACS-RAs) and accident/incident data in order to identify and classify human and organisation factors involved in accidents which occurred between 2009 and 2012 in China. In the HFACS-RAs framework, the accident causal factors are divided into four main categories and 21 relevant sub-categories with the definition and detailed description for each category of the HFACS-RAs framework. However, one drawback is that the definition and detailed description of each category are more about the operation process, as compared to the development process (e.g., purchasing of unsuitable and unqualified equipment such as train control equipment). Analysis of railway accidents requires a systematic analysis perspective which takes into account the various components of the system and their surrounding environment, including development and operation process. An extension of the definition and detailed description for HFACS categories is needed in order to cover the full range of human and organisational errors involved in both developmental and operational processes (Table 1).

Table 1 about here

3.1.2 Human information processing model for the STAMP model in accident analysis

A number of researchers have made modifications to STAMP, STPA and CAST (Thomas, 2013; Stringfellow, 2010; France, 2017). Thornberry (2014) for example, extended the human controller model based on human information processing and France (2017) extended the human controller mental model. According to Wickens and Flach (1988), human information processing models consists of information detection, information identification, decision making and action generation, and the process can be influenced by human factors, such as attention, fatigue (figure 2). Unsafe control actions refer to the factors inside of the human controller, such as the mental model flaws, and stimuli from outside, such as control actions from up-level controllers. The human controller receives the control command from up-level controllers. Feedback information of the controlled process from senses detects useful information based on the knowledge stored in the mental models. The next step involves identifying the information and classifying it into different parts, such as controlled processed, operational environment or other controllers. The identified information and mental models are then updated into new states. The human controller makes decisions and generates control actions based on updated mental models. Errors may occur in any part of the information process. Tracing back from the unsafe control action to the input information provides one way of tracing the factors contributing to unsafe control actions.

Figure 2 about here

Safety can be regarded as a system level propriety and as a result, accident and incident analysis should address system components from physical to organisational levels of analysis, as well as communication and coordination between components. Accordingly, France (2017) listed five contextual factor categories for the analysis shown in order to assist the analysis of an individual error or factor (table 2).

Table 2 about here

3.1.3 Integrating STAMP and HFACS

Aside from supporting the analysis at the level of human information processing there is also a need to support the analysis of errors at the organisational level. Stringfellow (2010), Thornberry (2014) and Lower (2018) have all incorporated individual and organisational error categories into STAMP.

Stringfellow (2010), examined the unsafe control actions at the individual controller and included six error categories with 23 subcategories. Lower et al (2018) added another category with five subcategories for the individual precondition from HFACS level 1 and level 2. Individual conditions describe the state of a human controller in terms of physiological and mental state, in this case five categories of level 2 of the HFACS structure (Zhan et al., 2017). These involve the following classifications:

1. Inadequate control goal [Entire];
2. The control algorithm does not enforce constraints[Part];
3. Model of the controlled process is inconsistent, incomplete, or incorrect[Part];
4. Model of the organisational structure (other controllers in the control hierarchy) is inconsistent, incomplete, or incorrect[Entire];
5. Inadequate coordination between decision makers[Part];
6. Inadequate execution of the control loop[Part];
7. Inadequate individual conditions[Entire];
    - 7.1 Adverse Physiological States
    - 7.2 Adverse Mental states
    - 7.3 Personal readiness
    - 7.4 Substandard condition of team
    - 7.5 Adverse conditions of Mission

For the analysis structure in figure 2, CATE 6 is about the control action execution, information input from up-level controller(s) and information feedback; CATE 5 is about communication information input; CATE 2 is about the control algorithm which is the way the controller make decision and select control action; CATE 3 and 4 are about the mental model of controller providing information for decision making and action generation. Individual errors will be divided into two categories – influence entire information processing [Entire] and influence part of information processing [Part], which have been marked in the seven categories. Those classifications are used in the analysis process. According to the organisational error taxonomy (Stringfellow, 2010), unsafe control actions at the organisational level occur due to seven categories with 12 subcategories. The first four categories are about the structure of the organisation, while the last three categories relate to organisational management. Lower et al. (2018) states that ‘inadequate safety management and learning processes’ can be influenced by the organisational factors and supervisory factors. However, the operational standards (table 2) are included in the organisational influences in HFACS level 4 and can contribute to the

assignment of goals, responsibility to controllers. 'Inadequate safety management and learning processes' involve dynamic system organisation and operation and is influenced by unsafe supervision. We therefore combine the HFACS factors into organisational errors as follows:

1. Inadequate assignment of goals, control authority and responsibilities to controllers;
   - 1.1 Inadequate coordination among controllers and decision makers
     - 1.1.1 Overlaps of responsibility
       - a) Inadequate organisational process
     - 1.1.2 Gaps in responsibility
       - a) Inadequate organisational process
   - 1.2 Role is not suitable for human control
     - 1.2.1 Inadequate safety culture
     - 1.2.2 Inadequate safety program
   - 1.3 Inadequate organisational change process for the reassignment of roles and goals
     - 1.3.1 Inadequate supervision
2. Inadequate allocation of resources to controllers throughout the organisation;
   - 2.1 Inadequate resources
3. Inadequate assignment of controller hierarchy;
   - 3.1 Hierarchy surrounding organisational processes do not support safe control
     - 3.1.1 Inadequate organisational process
4. Inadequate communication channels provided in the organisation;
   - 4.1 Communication channels do not exist
     - 4.1.1 Inadequate organisational process
   - 4.2 Communication channels do not have sufficient bandwidth
     - 4.2.1 Inadequate organisational process
     - 4.2.2 Inadequate equipment resources
   - 4.3 Communication channels are not created or eliminated in response to changing circumstances
     - 4.3.1 Inadequate supervision
     - 4.3.2 Failed to correct problems
5. Inadequate communication of system-level goals and constraints;
   - 5.1 Inadequate safety culture
   - 5.2 Inadequate safety program
6. Inadequate safety management and learning processes;
   - 6.1 Inadequate supervision
     - 6.1.1 Inadequate organisational process
     - 6.1.2 Inadequate resources
   - 6.2 Planned inappropriate operations
     - 6.2.1 Inadequate safety program
   - 6.3 Supervisory violations
7. Inadequate interactions with external bodies.

3.2 The ‘HS-RAs’ method

Figure 3 shows an overall flow diagram of hybrid accident analysis method. The analysis process consists of five phases**.** The first phase focuses on the system(s) and hazard(s) identification and system safety control structure documentation based on STAMP. The second phase concerns human and organisational error identification according to the extended HFACS categories in section 3.1.1. Examination of each component of the safety control structure that contains a human factor helps to identify human or organisational unsafe control actions. The focus of Phase 3 is on human error analysis based on STAMP and human information processing. Analysis of human unsafe control actions is based on the information processing model, the individual error taxonomy (section 3.1.2) and five contextual factors categories. The fourth phase represents an analysis of organisational factors based on STAMP. The final phase (phase 5) fifth phase supports the generation of recommendations, that is, filtering through each of the contributing factors (including causal factor and contextual factors) and identifying those which could potentially be changed, controlled or compensated for so that human and organisational errors could not occur again. In the next section of the paper we present a worked example of the hybrid method using the Yong-Wen accident.

Figure 3 about here

4. Case study

4.1 Yong-Wen railway accident

On July 23rd, 2011 at 20:30:05, an accident occured on the Yong-Wen High-speed railway in the precinct of Wenzhou, Zhejiang Province, China which resulted in 40 fatalities. A China Railway High-speed (CRH) train D301 crashed into another CRH train D3115 at a speed of 99 kilometres per hour. Six cars derailed and two of them went off a bridge 50 feet above the ground. The accident is considered to be the most serious railway accident in the development of Chinese railway history. The area where the accident occurred experienced severe lightning from 19:27 to 19:34 on July 23rd. The severe lightning which caused a fault in the control system. Both D3115 and D301 were behind schedule and reached Yongjia railway station at 19:51 and 20:12, respectively. D3115 was ordered to

leave Yongjia station and was notified to change its operational mode from FS mode to OS mode[2] because of a red-light displayed in the Train Control Centre (TCC) which indicated to the train controller that either a train was occupying that track circuit or that the track circuit had failed. Due to the lightning strikes, D3115 stopped automatically and failed to restart until nearly eight minutes later. During the re-start period, D3115 called the dispatcher six times and was called by the station operator three times, but all calls failed to connect. However, in this period, D301 was ordered to leave from Yongjia station as normal. Because of the failure of track circuits, D301 neither received the occupation information about D3115 nor stopped automatically and then two trains collided.

The Chinese Train Control System (CTCS) system is developed as a new train operation system which suits the national conditions after studying the European Train Control System (ETCS). It consists of five levels (CTCS-0 – CTCS-4) for the system that determine the basic functional requirements for each level. The signalling and train control system used on the accident line is the CTCS-2. The CTCS-2 system is composed of onboard control system (including the automatic train protective (ATP) system), wayside equipment (including track circuits, transponders and signals) and station control equipment (including the Train Control Centre and Station Interlocking computer).

4.2 Accident analysis using HS-RAs

4.2.1 Identify system(s) and system hazard(s), document the system safety control structure

Figure 4 shows the system control structure for the Yong-Wen line project development and operations. The operation process is also a complex process. Figure 5 shows the detail of the operation process in the system control structure.

Figures 4 and 5 about here

Based on the accident investigation report (SAWS, 2011), governmental documents (MOR Science & Technology Bureau and Transport Bureau, 2007a; 2007b; 2007c; 2007d; 2007e; 2009) and interview

[2] Full supervisor (FS) mode and the On sight (OS) mode are the operation modes of Chinese Train Control system. The CTCS on-board equipment shall be in the Full Supervision (FS) mode when all train and track data is available on board, The On Sight mode enables the train to enter into a track section that could be already occupied by another train, or obstructed by any kind of obstacle.

data with railway experts in China, the relevant system and system hazard in the development phase and the operational phase were identified. In this case the main hazard was the collision between the two trains. The China Railway Signalling and Communication Co. Lt (CRSC) is the integrator of the CTCS-2 system on this line. The TCC (Type: LKD2-T1) involved in this accident is located at Wenzhou south station and is designed by Beijing National Railway Research & Design Institute of Signal and Communication (CRSCD), belonging to the CRSC group. TCC equipment in Wenzhou south station is manufactured by Shanghai Railway Communication Company (SRCC), which also belongs to the CRSC group. Centralized Traffic Control is located in Shanghai Railway Bureau, which belonged to the Ministry of Railway (MOR), and was one of the 18 railway bureaus in China. Table 3 shows the system components in the high-speed railway including development and operations and system hazard in the accident.

Table 3 about here

The safety responsibilities and relevant control actions and feedback loops about the components related to this accident in the safety control structure are follows:

1. TCC is the controller of the train movement authority (MA) by getting track occupation information through the PIO board, coding the track signals to control the signal in the interval in order to ensure the safety of train operation. The safety integrity level of TCC is SIL4;
2. The onboard system of CTCS-2 is the controller for train control. The system gets track signals as the MA to control the train in specific operation mode, such as OS mode; onboard system cooperates with the train driver to ensure the train safety;
3. The CTC (Centralised Train Control) system is the operational control system that supports the assistant dispatcher to control trains within a certain area on the tracks; CTC has two kinds of operation mode – centralisation control mode and Station Control mode for the Abnormal Situation (SCMoAB); the centralisation control mode is the normal mode that dispatcher delivers dispatch commands through CTC to the station terminals to control the station components automatically, and deliver the dispatch commands to train drivers directly; SCMoAB mode is an abnormal control mode. When something is wrong about the CTC system, the dispatch delivers dispatch commands to station operators, and station operators control station components and the train operation in the SCMoAB control area;

4. The train driver should control the train through the onboard system, or directly based on the operational situation and dispatch commands from dispatcher or station operator;
5. The station operator should supervise the state of the station components and the operation state of trains in his control area and convey abnormal situation information to dispatcher and relevant train drivers. A key responsibility for the station operator is to control overall the station components and maintain levels of safety;
6. The dispatcher gives the appropriate dispatch commands to station components or operators and train drivers to ensure the all the trains operating in safe condition;
7. Shanghai Railway Bureau is the operation management and system development supervision unit to enforce safety management, e.g. staff training, supervision of the safety standard implement, and enforce supervision of the safety design of the new system to suit the system operation conditions;
8. Chinese Ministry of Railways publishes railway system regulations, standards and specifications and make the safety functions requirement for new equipment development and supervise the implement;
9. Beijing National Railway Research & Design Institute of Signal & Company Ltd. (CRSCD) is the designer of the TCC system in this accident and is responsible for a safe control system based on relevant standards, regulations and specifications;
10. China Railway Signal & Communication Corporation (CRSC) represents an upper-level management unit charged with enforcing safety management in CRSCD.

4.2.2 Identify human and organisational unsafe control actions

Examination of each component of the safety control structure (figure 4) was conducted in order to identify components that contain a human or organisational factor in the system. Table 4 summarises the components of human or organisational factors in both development and operation phases (the letter [D] means that a component may influence the system safety condition in the system development phase; [O] represents that a component may influence the system safety condition in system operation phase; [D, O] indicates that the influence may happen in both phases).

Table 4 about here

An accident can be thought of as nonlinear system state combining many factors from many parts of the system. One factor may not result in the accident happening, but can raise the probability of the accident. In terms of human and organisational factors, unsafe control actions are actions that are taken or not taken, or not taken in proper time or order and raise the probability of the accident happening. Human unsafe control actions can be identified in HFACS level 1 and organisational unsafe control action in HFACS level 3 and 4. For each component in Table 4, human and organisational unsafe control actions have been identified in the third column of table 5. The process (section 4.2.3 and 4.2.4) is an iterative process to analyse each human or organisational unsafe control action. In the following analysis, we take one unsafe control action of dispatcher and one relevant organisational action to show the analysis process. The final analysis is shown in Table 5 for all the human controllers and organisations.

Table 5 about here

4.2.3 Analyse human unsafe control action

The unsafe control action of dispatcher *A4: Dispatcher dispatched D301 into the interval without informing the red-light strip information* will be used to show the analysis process. In the five contextual factors, the fourth and fifth classifications are about contributing factors for organisational factors:

Unsafe control action:

A4: Dispatcher dispatched D301 into the interval without informing the red-light strip information

Identify the contributing factors in individual error taxonomy:

1. Action Generation:

   IEs-1: Dispatcher's control algorithm of train D301 did not match the scope of his control area: in the SCMoAB control, dispatcher could give the movement authority for train D301 to Wenzhou south station where the station operator controlled, but just received the equipment state from the station operator. This overlap of control responsibility led the dispatcher to issue this unsafe control command.
2. Decision:

IEs-2: Dispatcher's inadequate mental model of the track circuits' status resulted in him thinking the interval track circuit condition met the train tracing function requirement. The wrong judgement about the track circuits' status led him to make the decision to send D301 into the interval.

3. Identification:

IEs-3: Dispatcher thought he had received enough information to recognise the interval track circuits' condition according to his inadequate mental model of the interval track circuits: before train D301 was dispatched, the dispatcher thought the interval situation compliedwith the automatic blocking the automatic blocking function for train tracing based on the mode of the interval track circuits did not change and the signals in Yongjia station were normal based on confirming the equipment condition in Yongjia station on CTC and inquiring as to the interval track circuit condition through train D3212 driving from Wenzhou south station to Yongjia station.

4. Detection:

IEs-4: The dispatcher's inadequate mental model about the interval system led him to confirm the equipment status in Yongjia station and Wenzhou south station, the track circuit signal near Yongjia station and the operation status of D3212.

The contributing factors in the contextual factors analysis:

1. Physical system and technology factors

PTFs-1: TCC and track circuits' failures updated the track circuits' signals breaking the train tracing condition for safety;

PFTs-2: Physical system did not provide proper failure alarm and information;

PTFs-3: Inadequate operation rules for the emergency condition;

2. Individual and team factors

ITFs-1: Inadequate communication between the station operator and the train D3115 driver;

ITFs-2: Maintenance workers did not communicate in order to stop using the failed track circuit;

ITFs-3: Lack of experience about the failure condition;

ITFs-4: High workload and fatigue - the dispatcher worked a 12 hour shift and had to closely monitor a display for much of that time; during the 7 minutes after D3115 was dispatched and before dispatching D301, the dispatcher confirmed the field status of other stations along the line, confirmed again the station status of Wenzhou south station, learned other train operation status, and received and dispatched another 8 trains.

ITFs-5: Overconfidence about the physical system.

ITFs-6: Believed the system was fail-safe.

3. Organisational factors

OGFs-1: SRB did not supervise its staffs' actions for system safety;

OGFs-2: SRB arranged long work time and heavy work load for operation staff;

OGFs-3: SRB did not provide adequate operation rules;

OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations;

It is worth noting that the factors in individual and team factors also could be the individual factors like those identified in the information processing coming from the [Entire] factors listed in section 3.1.2. As a result, parts of the individual and team factors and all the individual errors identified will be listed as the causal factors for the UCA labelled as CF in the table 5. While the physical system and technology factors could trace back to the development process, the organisational factors listed above derive from organisational unsafe control actions identified in section 4.2.2. For example, OGFs-3 is the unsafe control action O1 (organisational influence factor in HFACS level 4) for SRB.

4.2.4 Analyse organisational unsafe control actions (errors)

In this part of the method, organisational unsafe control action will be analysed based on the organisational extented error taxonomy in section 3.1.2. In the five contextual factors, the last two classifications will be used to find the contributing factors for inadequate organisational factors. For *OGFs-3(O1): SRB did not provide adequate operation rules*, the analysis is following:

Organisational unsafe control action:

OGFs-1(O1): SRB did not provide adequate operation rules:

Identify the contributing factors in organisational error taxonomy:

OEFs-1: SRB did not have an adequate safety management for formulating adequate operation rules for its own operation system:

OEFs-2: SRB did not allocate specific human resource to custom adequate operation rules for its own operation system:

OEFs-3: Low degree of safety culture.

The contributing factors in the contextual factors analysis:

1. Physical system and technology factors

PTFs-1: The CTC system development company did not provide adequate operation rules for the emergency condition: requiring for more information about the development company (did not exist in the accident official report).

2. Regulatory factors

RGFs-1: MOR did not supervise the safety management of SRB;

RGFs-2: MOR did not do to improve the degree of support to the safety culture in SRB.

Similar to the situation in section 4.2.3, the organisational error (e.g. OEFs-1, OEFs-2) will be listed as the causal factors for SRB unsafe control action labelled as CF. While the physical system and technology factors could trace back to the development process. Regulatory factors are also the unsafe control action of MOR which will be analysed in MOR analysis.

4.2.5 Recommendations

One goal of the accident analysis is to determine how to change or re-engineer the safety-control structure in the most cost-effective and practical way in order to prevent similar accident processes in the future. Once the STAMP analysis has been completed, generating recommendations is relatively simple and follows on directly from the analysis results (Leveson, 2012, p. 384). Going through each of the causal factors and contextual factors and identifying those which could potentially be changed, controlled or compensated to prevent a similar accident will happen in the future, accident countermeasures can be generated. According to the analysis, there are influential ways from organisation to individual human controller, from operation process to development process, so systematic countermeasures can be generated. Based on the analysis results of sections 4.2.3 and 4.2.4, the recommendations can be developed from each causal factor with 76 countermeasures for human and organisational errors in the fifth column of Table 5. One causal factor can be mitigated by one or several safety constraint(s), and then the repeated safety constraints merged to provide a list for one component.

5. Discussion

5.1 Summary of Findings

The summary of the contributing factors for Yong-wen railway accident identified by HS-RAs is shown in Table 6. In HS-RAs method, the precondition for unsafe acts is used as the context for unsafe acts to occur. There are three levels in the accident contributing factors list.

Table 6 about here

In the first part of the process, HFACS classification was instrumental in preliminary factor identification. STAMP facilitated identification of the causal factors in the system development phase as well as the operational phase. Seventeen unsafe acts by the Dispatcher, the Station Operator, D3115 driver, maintenance workers and design staff were identified alongside 12 contributing factors covering unsafe supervision; most of these appeared in system development phase and 14 organisational factors. In the second part of the process, the STAMP analysis identified 112 causal factors including 64 causal factors from individual human errors, 23 causal factors related to unsafe supervision and 25 causal factors categorised as organisational errors. These factors not only include all the factors in the official report, but also identify the dangerous factor about the gap and overlap of human controller control authority, such as *D3115 driver::CF2: D3115 driver was under control of the dispatcher and the station operator in the failure section*. This dangerous condition is caused by *PTFs-2: Inadequate operation rules about the emergency condition*. Inadequate CTC operation rules give the control authority of D3115 driver to the dispatcher and the station operator resulting in the unsafe control for train D3115. Inadequate operation rules (MOR Science & Technology Bureau and Transport Bureau, 2007c) caused D3115 driver to assume that he was controlled by the dispatcher in the track section where the station operator was responsible for the supervision and control of the system.

5.2 Comparison with other analysis cases using STAMP and/or HFACS

There are three typical system accident analysis models based on HFACS – HFACS-RR (Reinach and Viale, 2006), HFACS-RAs (Zhan et al., 2017) and a System-Theoretic model and process with Human Factors (Lower et al. 2018). HFACS focuses on the causal factors in system operation phase. Thus, Reinach and Zhan just look the factors coming from HFACS four or five levels as the causal factors in the system operation phase for the accident. Those “causal factors” are only the symptoms not the causes. Therefore, countermeasures based on the outcomes of HFACS cannot be useful to prevent a future accident. Zhan et al. (2017) promoted HFACS-RAs and used it to analyse Yong-wen railway accident. The summary of the causal factors identified is in Table 7.

Table 7 about here

There are 4 outcomes for unsafe acts, 6 outcomes for unsafe supervision and 7 outcomes for organisational influences. This is less than HS-RAs (22 vs 46). The causal factors are all not related to the relevant system components, such as the description like "A2: *Fail to contact with train D301 and inform the driver of the information of train D3115*" is ambiguous because there is not an actor for the unsafe act. In contrast, the similar description about the unsafe acts "A3: *Dispatcher did not track the D3115 run status in time, just informed the red-light strip information to the driver*" and "A5: *Dispatcher did not inform the red-light strip information to D301 driver*" are more practice. Subsequently, HFACS-RA(s) gets the prevention measures based on the outcomes of HFACS four classifications directly. While HS-RAs takes the detailed analysis based on STAMP to find the root causes which hidden in system operation and management. Therefore, HS-RAs can find out more causal factors in detail. This is demonstrated in the case study in section 4 (see in Table 5).

Harris and Li (2011) and Lower et al (2018) combined HFACS and STAMP to identify and analyse human and organisational error respectively. Harris and Li (2008) took the control engineering and safety constraint of STAMP into HFACS to link the factors in different level to show the influence chain from organisation to human individual controller. While Lower et al (2018) integrated HFACS categories into STAMP analysis to explain how organisational influences and supervision influence the Process Model Flaws and Decision making Context resulting in unsafe control actions. HS-RAs by contrast, combined human information processing to analyse unsafe control actions and we would argue adds an extra dimension which complements an analysis of unsafe control actions covering organisational factors, design flaws and operation and technical specification flaws.

6. Conclusions, study limitations and future work

In this paper, we have attempted to integrate STAMP and HFACS in order to construct a hybrid method which is suitable for human and organisational errors analysis for complex social-technical system accident with human cognitive process. This involved combining components and elements from STAMP and HFACS in a way that the methods might be integrated and introducing a human information processing element to the analysis. We then applied this to the Yong-Wen accident and compared the analysis results of HS-RAs with other analyses (e.g. HFACS-RAs analysis for Yong-

wen railway accident, Zhan et al., 2017; STAMP analysis for Yong-wen railway accident, Dong, 2012). In this work, preliminary results offer evidence that the HS-RAs approach can contribute to railway safety by giving a detailed analysis of human and organisational errors in railway accidents. We acknowledge that there is room for improvement on hybrid accident analysis methods. First, further studies need to be carried out in order to improve the effectiveness of the countermeasures of the HS-RAs analysis. Various countermeasures at different system levels were identified from the analysis, but a clearer understanding of the relationships among them is needed to ensure the overall system safety (i.e., what Leveson (2012, p.311) calls 'intent specification'). For example, SRB and CRSC could establish their own safety management system based on the safety management regulation of MOR. Secondly, a more detailed analysis of human errors needs to be carried out based on the mental model (Leveson, 2012, p.273; Johnson-Laird, 1995) in order to probe deeper into possible patterns. The human controller's mental model consists of not only the models of automation and the controlled process (Leveson, 2012, p.281), but is also influenced by other factors including physiological state and human information processing capacity. Finally, the proposed methodology needs to be applied and evaluated with other case study examples, both within the context of railway systems and other domains of application.

Acknowledgements

This paper has been supported by the High-speed Railway United Found of National Natural Science Foundation of China (U1434209), the Research Funds for the Central Universities (2013JBM125), the Fund from State Key Laboratory of Rail Traffic Control and Safety (RCS2015ZQ001). The first author was a visitor in the Human Factors and Complex Systems Group, Loughborough University over the period 2015-16.

Word count = 6, 782 words (excl. tables, figures).

References

Chatzimichailidou, M., M., Dokas, I. M. (2016). Introducing RiskSOAP to communicate the distributed situation awareness of a system about safety issues: an application to a robotic system. Ergonomics, 59, 409-422.

Dokas, I. M., Feehan, J., Imran, S. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. Safety Science, 58, 11-26.

Dong, A. (2012). Application of CAST and STPA to Railroad Safety in China (Doctoral dissertation, Massachusetts Institute of Technology).

Esslinger, V., Kieselbach, R., Koller, R., Weisse, R. (2004). The railway accident of Eschede – technical background. Engineering Failure Analysis, 11, 515-535.

France M.E. (2017).Engineering for Humans: A New Extension to STPA. Master's Thesis, MIT.

France. M.E. Multer, J. Safar, H. (2018). New Guidance for CAST: Case Study of a US Freight Rail Stop Overrun and Collision. The 7th MIT STAMP/STPA Workshop, MIT, March 26-29.

Harris, D., Li, W.C. (2011). An extension of the Human Factors Analysis and Classification System for use in open systems. Theoretical Issues in Ergonomics Science, 12(2), 108-128.

Johnson-Laird, P.N. (1995). Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness. Harvard University Press, Cambridge, Massachusetts, USA.

Kim, D.S., Baek, D.H., Yoon, W.C., 2008. Developing a Computer-Aided System for Analyzing Human Error in Railway Operations. World Congress on Railway Research (Seoul, Korea).

Leveson, N. (2004). A new accident model for engineering safer systems. Safety Science, 42(4), 237-270.

Leveson, N. (2012). Engineering a safer world: systems thinking applied to safety. The MIT Press, Cambridge, Massachusetts, USA.

Li, C.L., Tang, T., Li, K.C., Lv, J.D., Huang L. (2013). Model-based generation of safety test-cases for Onboard systems. 2013 IEEE International Conference on Intelligent Rail Transportation (ICIRT), Beijing, 191-196.

Liu, J. T., Tang, T., Zhu, J. B., Zhao, L. (2016). An extended system-theoretic hazard analysis method for the safety of high-speed railway train control systems. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 0954409716664931.

Lower, M., Magott I., Skorupski, J. (2015). Risk analysis of serious air traffic incident based on STAMP-HFACS and fuzzy sets. 3rd European STAMP Workshop, Amsterdam, 4th – 6th October. Available at: http://www.amsterdamuas.com/binaries/content/assets/subsites/aviation/stamp/2015/presentations/day-2/michal-lower---risk-analysis-of-serious-air-traffic-incident-based-on-stamp-hfacs-and-fuzzy-sets.pdf (Last accessed February 13th 2017)

Lower, M., Magott, J., Skorupski, J. (2018). A System-Theoretic Accident Model and Process with Human Factors Analysis and Classification System taxonomy. Safety Science, 110 (PA):393-140. https://doi.org/10.1016/j.ssci.2018.04.015

Madigan, R., Golightly, D., Madders, R. (2016). Application of Human Factors Analysis and Classification System (HFACS) to UK rail safety of the line incidents. Accident Analysis and Prevention, 97, 122-131.

MOR Science & Technology Bureau and Transport Bureau. (2007a). CTCS-2 system technical specification, No.43. (In Chinese)

MOR Science & Technology Bureau and Transport Bureau. (2007b). CTCS-2 system Train control centre technical specification, No.158. (In Chinese)

MOR Science & Technology Bureau and Transport Bureau. (2007c). Regulation of railway technical operation. China Railway Publishing House. (In Chinese)

MOR Science & Technology Bureau and Transport Bureau. (2007d). Railway transportation dispatching rules. China Railway Publishing House. (In Chinese)

MOR Science & Technology Bureau and Transport Bureau. (2007e). CTCS-2 system onboard system technical specification, No.45. (In Chinese)

MOR Science & Technology Bureau and Transport Bureau. (2009). Railway passenger dedicated line management rules, No.116. (In Chinese)

Nagel, D. (1988). Human error in aviation operations. In Wiener, E.L., Nagel, D.(EDS). Human factors in Aviation, Academic Press, London, 263-303.

Niu, R., Cao, Y., Ge, X., Tang, T. (2014). Applying System Thinking to Learn from Accident of Modern Automatic Control Systems. Chinese Journal of Electronics, 23(2), 409-414.

Oh, J., Washington, S. P., Nam, D. (2006). Accident prediction model for railway-highway interfaces. Accident Analysis & Prevention, 38(2), 346-356.

O'Hare, D., Wiggins, M., Batt, R., Morrison, D. (1994). Cognitive failure analysis for aircraft accident investigation. Ergonomics, 7, 1855-1869.

Ouyang, M., Hong, L., Yu, M. H., & Fei, Q. (2010). STAMP-based analysis on the railway accident and accident spreading: Taking the China–Jiaoji railway accident for example. Safety Science, 48(5), 544-555.

Reason, J. (1990). Human Error. Cambridge University Press, New York.

Reason, J. (1997). Managing the risks of organizational accident. Ashgate Publishing Ltd, Aldershot.

Reinach, S., Viale, A. (2006). Application of a human error framework to conduct train accident/incident investigations. Accident Analysis & Prevention, 38(2), 396-406.

Salmon, P., Cornelissen, M., Trotter, M. (2012). System-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. Safety science, 50, 1158-1170.

SAWS. (2011). Investigation report of the "7.23" Yong-Wen Railway accident. Beijing, State Administration of Workplace Safety. Available at: http://old.chinasafety.gov.cn/jgjc/sgcc/tbzdsgdcbg/201112/t20111228_130586.shtml (Last accessed Jun 10th 2018)

Shappell, S.A., Wiegmann, D.A. (2000). The human factors analysis and classification system – HFACS. Federal Aviation Administration Technical Report No. DOT/FAA/AM-00/7. National Technical Information Service, N Springfield.

Shultz, J.M., Garcia-Vera, M.P., Santos, C.G., Sanz, J., Bibel, G., Schulman, C., Bahouth, G., Guichot, Y.D., Espinel, Z., Rechkemmer, A. (2016). Disaster complexity and the Santiago de Compostela train derailment. Disaster Health, 3(1), 11-31.

Song, T., Zhong, D., Zhong, H. (2012). A STAMP Analysis on the China-Yong-Wen Railway Accident. Proceedings of the 31st International Conference, SAFECOMP, Magdeburg, Germany, 376-387.

Stringfellow, M.V. (2010). Accident analysis and hazard analysis for human and organisational factors. Doctoral Thesis, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, USA.

Suo, D. (2012). A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident. The first STAMP workshop, MIT.

Thornberry, C.L. (2014). Extending the Human-Controller Methodology in Systems-Theoretic Process Analysis (STPA). Master thesis, MIT.

Underwood, P., Waterson, P.E. (2014). System thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, Accimap and STAMP models. Accident Analysis and Prevention, 68, 75-94.

Wang, R., Zheng, W., Liang, C., Tang, T. (2016). An integrated hazard identification method based on the hierarchical Colored Petri Net. Safety Science, 88, 166–179.

Wickens, C.D., Flach, J.M. (1988). Information processing. In E.L. Wiener and D.C. Nagel (Eds.), Human factors in aviation (pp. 111-55). San Diego, CA: Academic Press.

Wiegmann, D.A., Shappell, S.A. (2003). A human error approach to aviation accident analysis: the Human Factors Analysis and Classification System. Aldershot: Ashgate.

Wiener, N. (1948). Cybernetics, or control and communication in the animal and the machine. Cambridge, MA: The MIT Press, and Wiley.

Wilson, J.R., Farrington-Darby, T., Cox, G., Bye, R., Hockey, G.R. (2007). The railway as a socio-technical system: human factors at the heart of successful rail engineering. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 221(1), 101-115.

Zhan, Qingjian., Zheng, Wei., Zhao, Bobo. (2017). A hybrid human and organizational analysis method for railway accidents based on HFACS-Railway Accidents (HFACS-RAs). Safety Science, 91, 232-250.

Figures:

Figure 1: The conceptual framework for the proposed hybrid method

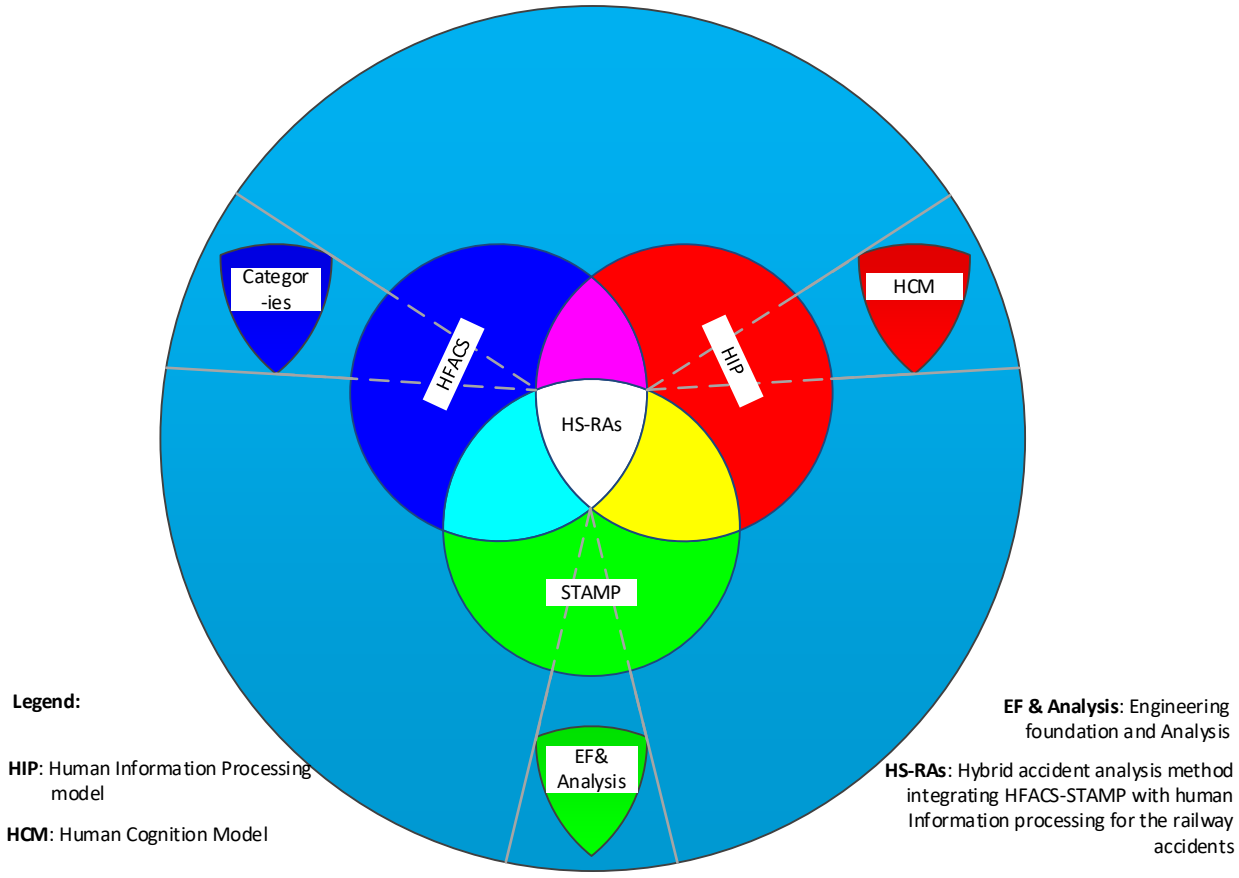


Figure 2: the human information processing and analysis model (Adapted from Wickens and Flach (1988))

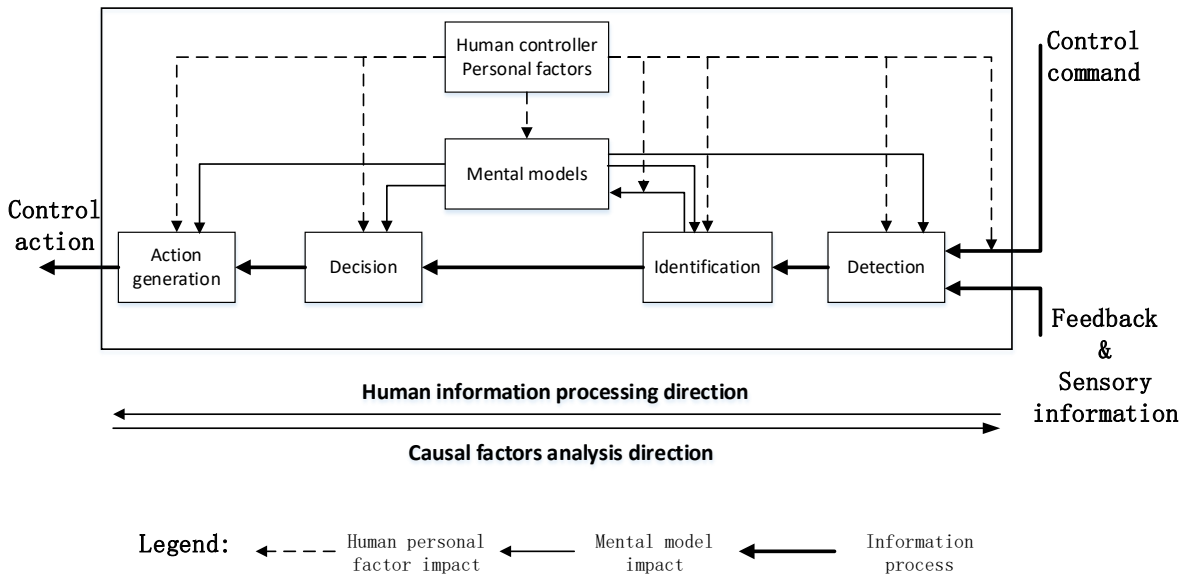


Figure 3: The flow diagram of HS-RAs method.

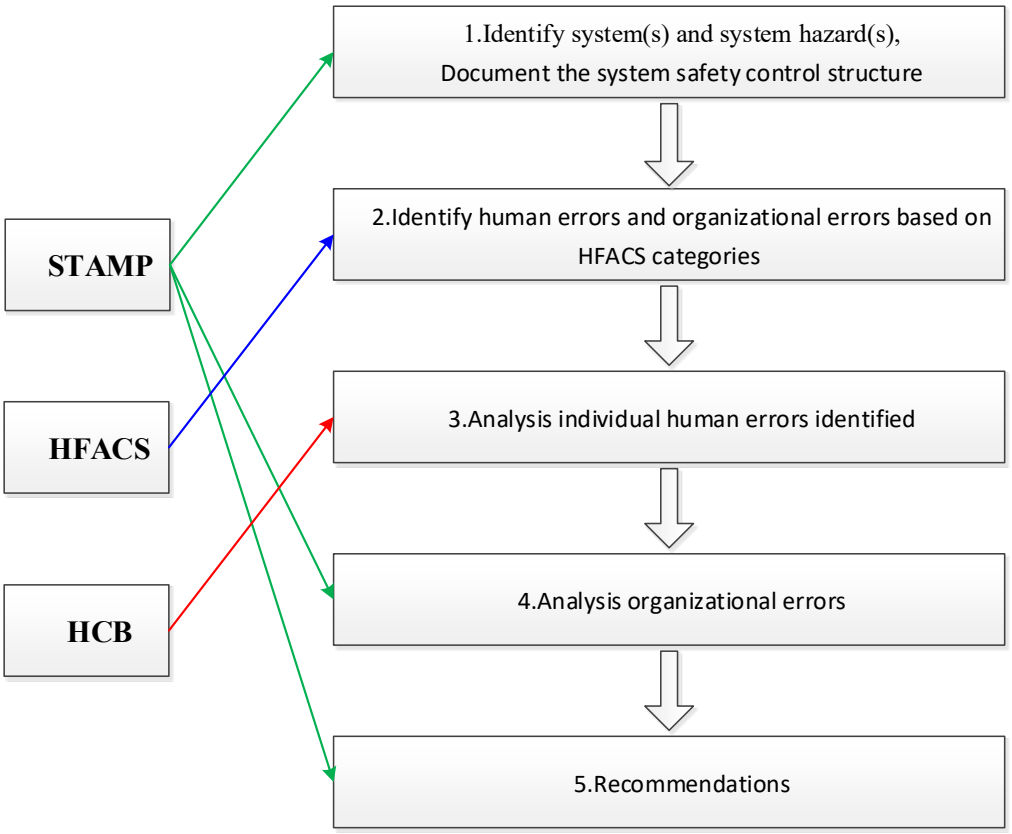


Figure 4: Safety control structure of Yong-wen high-speed railway accident (This is an adaptation of the generic loop provided by Leveson 2012 in page 82 (fig 4.4) and page 66 (fig 3.2))

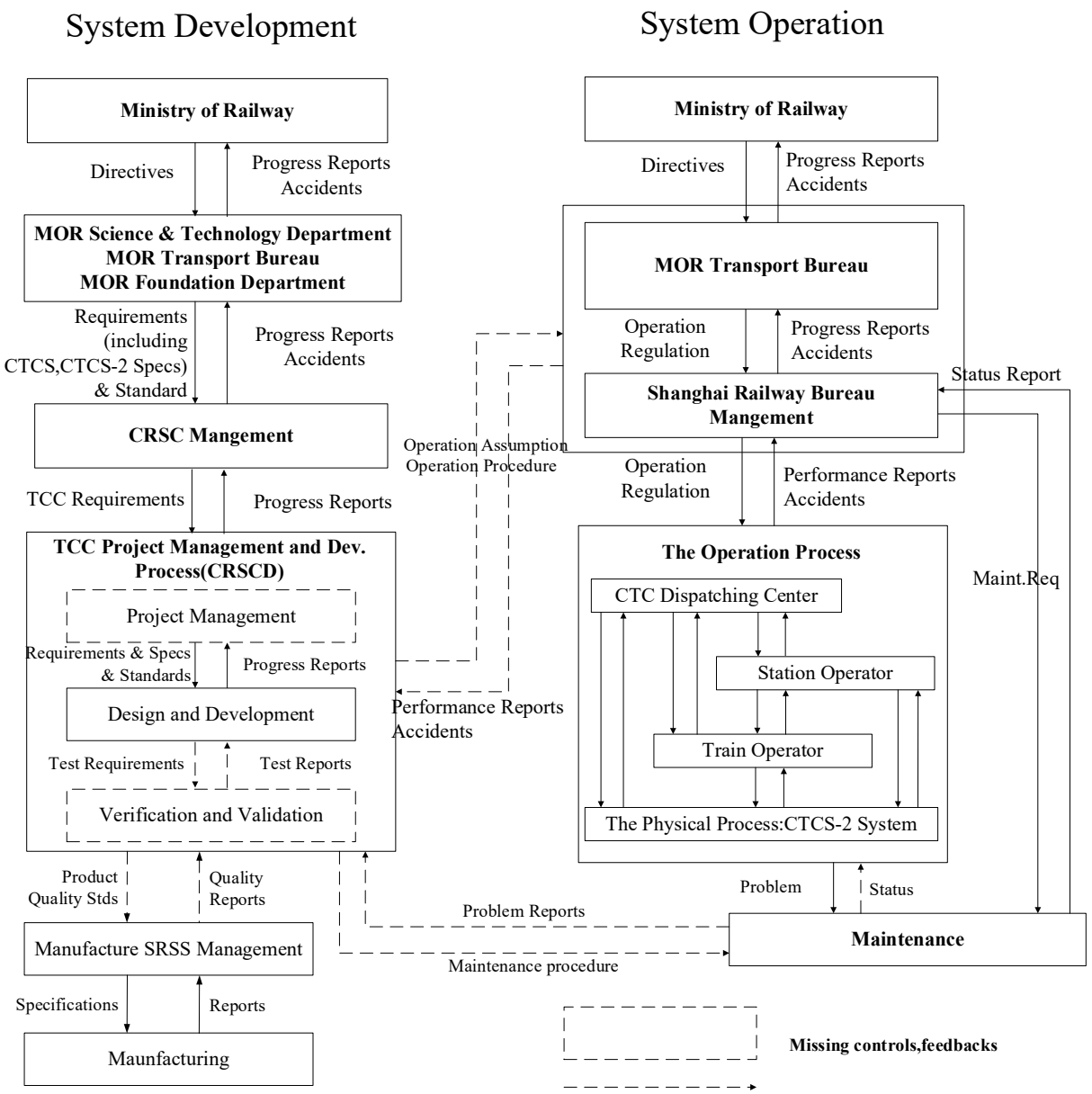
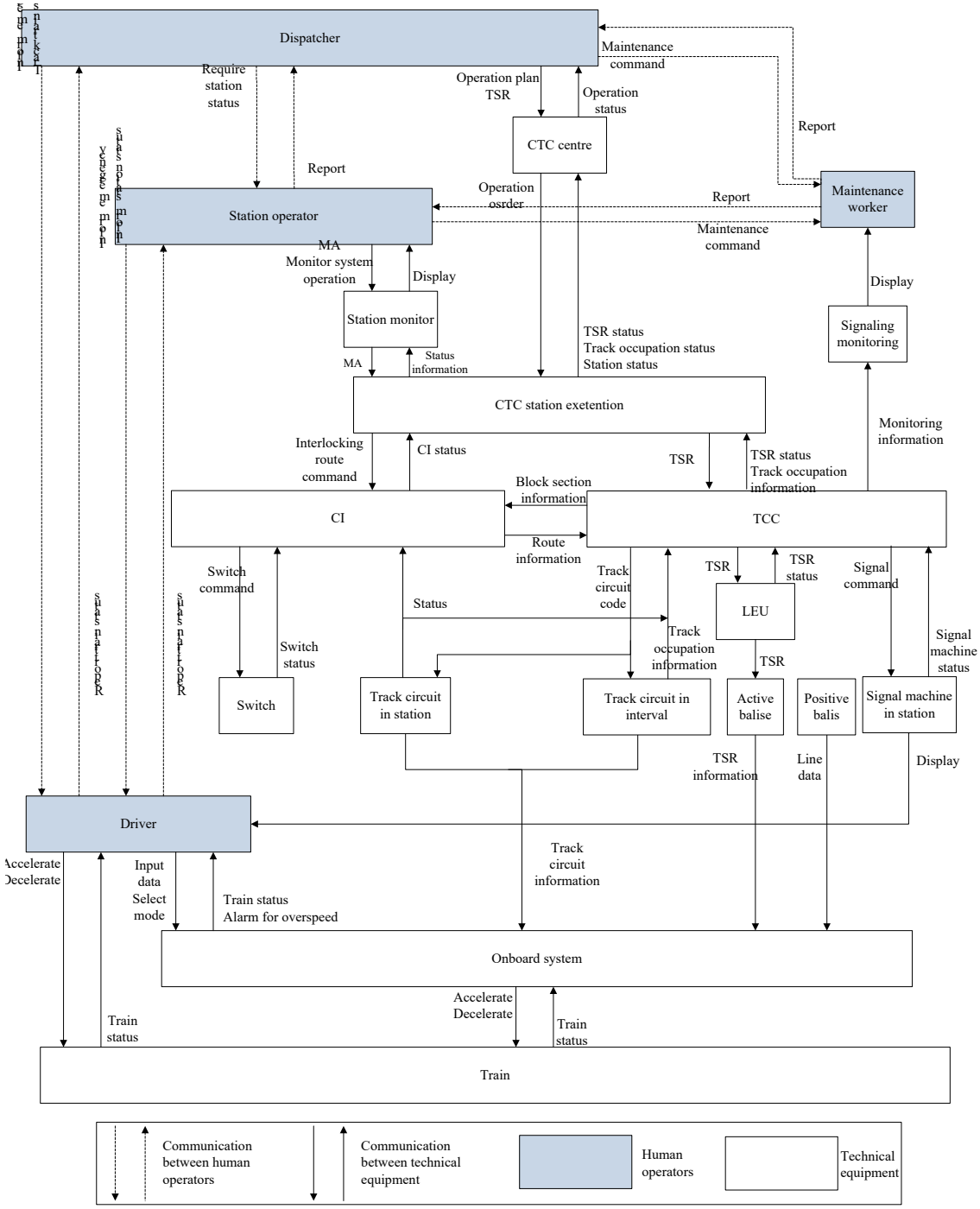


Figure 5: The physical operating safety control structure of "7•23" accident



Tables:

Table 1 Brief description for STAMP-HFACS categories (Modified from Table 1 in Zhan et al. (2017), p239)

Main categories	Sub-categories		Description
Organisational Influences	Resources management	Human Resources	Deficiencies of selection and training of railway employees ***for system development or operation***
		Financial Resources	Poor financial situation or adverse allocation of funds such as cost-cutting ***in system development and operation***, operating loss and lack of funding
		Equipment Resources	Purchasing of unsuitable and unqualified equipment such as train control equipment ***or giving out the inadequate requirements for equipment development***
	Organisational process	Operational Standards	Lack of appropriate Technical standards for operation and maintenance of trains and tracks
		System Policies	The rules and regulations for promotion and punishments, or keeping organisational justice ***in system development or operation process***
		System Procedures	Policies, documentations, instructions and emergency plans for the railway system ***in system development or operation process***
	Safety climate	Safety Culture	The safety climate, the faith of safety and recognition of safety in railway system ***in system development or operation process***
		Safety Program	The rules for safety training, training result tracking, safety oversight, etc. ***in system development or operation process***
Unsafe Supervisions	Supervision disorder	Inadequate Supervision	Negligence of duty, fail to provide equipment maintenance, fail to provide skill and safety training and training track the qualifications of equipment ***in system development or operation process***
		Planned Inappropriate Operations	Inappropriate plan to the actual conditions, such as substandard maintenance plan and dispatching plan, etc. Fail to provide correct information and data, maintenance and construction mission not in accordance with regulations, ***in system development or operation process***
		Failed to Correct Problems	Failed to identify existing equipment failure and error operation, fail to initiate corrective action ***in system development or operation process***
		Supervision Violations	Regulators authorized unqualified staff for duty, authorized mission not in accordance with regulations, fail to enforce rules and regulations ***in system development or operation process***

Preconditions for Unsafe Acts	Substandard Conditions of Operators	Adverse Physiological States	Pathological conditions such as medical illness, physical trauma, physical fatigue for individual ***in system development or operation process***
		Adverse Mental States	Attention-deficit, mental fatigue, self-satisfied, haste, misplaced motivation, etc. ***in system development or operation process***
		Personal Readiness	Violation of staff rest requirement and alcohol inspection, excessive physical training before work, lack of experience, poor training results, etc. ***in system development or operation process***
	Substandard Condition of Team		Inappropriate assignment of team members, an insufficient number of team members, lack of team leader and poor teamwork ***in system development or operation process***
	Adverse conditions of Mission		Time limitation, task difficulties ***in system development or operation process***
	Adverse Physical Environment		Foggy and rainy weather, debris flow, landslide, etc.
Unsafe Acts	Errors	Decision Errors	Misdiagnosed emergency and wrong response to an emergency, a wrong plan due to exceeding ability, improper procedure, poor decision, etc. ***in system development or operation process***
		Skill-based Errors	Omitted step in the procedure, poor technique ***in system development or operation process*** Wrong operations ***in operation process***
	Violations		Operation and maintenance not in compliance with standards, not qualified for the mission, fail to properly for work, speeding, etc. ***in system development or operation process***

Table 2 Contextual factors categories for accident and incident analysis (France (2018))

CATEs	Factors
1.Physical system and technology factors (PTFs)	1.1 Operating environment design(including system operation rules)
	1.2 Interface design (e.g. displays and alerts)
	1.3 Maintenance/operational status of physical systems
	1.4 Availability or non-availability of job aids
	1.5 Other physical factors (e.g. weather)
2. Individual and team factors(ITFs)	2.1 Communication and teamwork; coordination
	2.2 Distractions/competing demands for attention
	2.3 Experience level; qualification and training
	2.4 Fatigue; work schedule
	2.5 Medical fitness for duty
	2.6 Expectations; similar situations encountered
3.Organisational factors(OGFs)	3.1 Supervisory priorities/safety culture
	3.2 Resource constraints & production pressures

	3.3 Policies and procedures (work schedules, training, discipline, etc.)
	3.4 Degree of feedback from employees
4.Regulatory factors(RGFs)	4.1 Degree of support to/control over organisations
	4.2 Feedback (data) collected from organisations
	4.3 Regulations regarding employees
	4.4 Regulations regarding physical systems and Technologies
5. External/Environmental factors; "Other" (EEFs)	5.1 High-level societal, governmental, etc. influences
	5.2 Economic context, funding sources
	5.3 Demands for service driving production pressures
	5.4 Political climate's effects on funding, regulation, etc.

Table 3: System and system hazards in the Yong-Wen accident

Development		**Operation**		**System hazard**
System phases	**System components in Chinese railway system**	**System components in Chinese railway system**	**System phases**	
Governments regulation agencies	Chinese Ministry of Railways	Chinese Ministry of Railways	Governments regulation agencies	Train control system failed to protect the safe distance between two trains.
Maintenance and Evolution	Shanghai Railway Bureau	Shanghai Railway Bureau	Safety Assurance and Supervision	
Project Management	China Railway Signal & Communication Corporation (CRSC)	Electrical & Signal Office	Maintenance	
Design	Beijing National Railway Research & Design Institute of Signal & Comm Co. LTD	Transportation Office	Operation	
Manufacture	Shanghai Railway Communication Company (SRCC)	Wenzhou Station	Operation & Maintenance	
Physical system	Train control system	Train control system	Physical system	

Table 4: Component with human or organisational factors

Component	Organisational factors	MOR [D,O]
		CRSC [D]
		CRSCD [D]
		TCC Project Team (TPT) [D]
		SRCC [D]
		Shanghai Railway Bureau(SRB) [D,O]
	Human factors	Dispatcher [O]
		Station operator [O]
		D3115 Train driver [O]
		D301 Train driver [O]
		Maintenance worker [O]

Table 5 Yong-wen accident causation analysis results based on HS-RAs framework

HS-RAs main categories	Component	Unsafe control actions	Individual causal factors	Contextual factors	Countermeasures
Unsafe acts	Dispatcher	A1:Dispatcher did not check and confirm the track condition in time	CF1: Dispatcher had inadequate understanding of Emergency status CF2: Inadequate understanding of how his controlled process was influenced by feedbacks from Station, Trains and Maintenance CF3: The method for updating track situation was inadequate without complying with procedure or timeline or chronology CF4: Expected train feedback was missing CF5: Lack of experience about the failure condition; CF6: Too busy and Fatigue	PTFs-1: Inadequate operation rules for the emergency condition [related to operation rule creation process]; ITFs-1: Inadequate communication with maintenance and station operator; ITFs-2: Maintenance workers did not feedback to stop using the failure track circuit [Maintenance::A2]; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	SC1:Dispatcher should improve his understanding of system emergency situation [P:[SRB:O-SC1][TPT::O-SC5]] SC2: Dispatcher should improve his ability about the system functions [P:[SRB:O-SC1][TPT::O-SC5]] SC3: Dispatcher should check track situation complying with operation procedure in timeline or chronology[P:[SRB:O-SC1][TPT::O-SC5]] SC4: Dispatcher should know how to solve the emergency situation without expected feedback [P:[SRB:O-SC1][TPT::O-SC5]] SC5: Dispatcher should realise the failure of the communication channels and know how to deal with it [P:[TPT::O-SC5] [SRB::O-SC6]] SC6: Dispatcher should put the system safety in highest priority[P:[SRB:U-SC5][SRB::O-SC5]] SC7: Dispatcher should know that the control target in the emergency situation is safety [P:[SRB:O-SC3]] SC8: Dispatcher should know the specific operation procedures in the emergency situation [P: [SRB::O-SC6]]
		A2:Dispatcher did not check the maintenance status about the failure equipment	CF1: Dispatcher put the system safety in a lower priority than efficient CF2: Dispatcher thought maintenance workers would feedback the maintenance status CF3: Dispatcher thought there was no feedback from maintenance workers meant that the track situation was still failed and compliance with fail-safe concept CF4: Lack of experience about the failure condition; CF5: Too busy and Fatigue	PTFs-1: TCC and track circuits' failures updated the track circuits' signals breaking the train tracing condition for safety [related to physical development]; PFTs-2: Physical system did not provide proper failure alarm and information [related to physical system development]; PTFs-3: Inadequate operation rules for the emergency condition [related to operation rule creation process]; ITFs-1: Inadequate communication with maintenance; ITFs-2: Maintenance workers did not feedback to stop using the failure track circuit [Maintenance::A2]; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1];	

				OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	SC9:Dispatcher should know the system functions and the specific operation procedures in the emergency situation [P:[TPT::O-SC5][SRB::O-SC6]] SC10: Dispatcher should connect with maintenance workers periodically to confirm the equipment status [P:[SRB:O-SC6]] SC11: Dispatcher should know this responsibilities in the emergency situation [P:[SRB::O-SC3]] SC12: Dispatcher should not assume the status of D3115 and confirm it with Wenzhou south station without clear information about the system status [P:[SRB:O-SC1][TPT::O-SC5]] SC13: Dispatcher should know the system functions in emergency situation [P:[SRB:O-SC6][TPT::O-SC5]] SC14: Dispatcher should know how to solve the emergency situation without expected feedback [P:[SRB:O-SC6][TPT::O-SC5]] SC15: Dispatcher should know the risk of his operation [P:[SRB:O-SC2][TPT::O-SC5]] SC16: Dispatcher should improve his understanding of system functions in emergency situations [P:[SRB:O-SC6][TPT::O-SC5]]
		A3:Dispatcher did not track the D3115 status in time, just informed the red-light strip information to the driver	CF1: Dispatcher just assumed that D3115 could pass the fail section under OS mode and had reached Wenzhou south station CF2: Lack of experience about the failure condition; CF3: Too busy and Fatigue	PTFs-1: TCC and track circuits' failures updated the track circuits' signals breaking the train tracing condition for safety [related to physical development]; PFTs-2: Physical system did not provide proper failure alarm and information [related to physical system development]; PTFs-3: Inadequate operation rules for the emergency condition [related to operation rule creation process]; ITFs-1: Inadequate communication between the station operator and the train D3115 driver; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
		A4:Dispatcher dispatched D301 into the interval without informing the red-light strip information	CF1: Dispatcher's control of train D301 did not match the scope of his control area CF2: Dispatcher 's mental model of the track circuits was inconsistent with the real situation CF3: Dispatcher believed the system was itself fail-safe	PTFs-1: TCC and track circuits' failures updated the track circuits' signals breaking the train tracing condition for safety [related to physical development]; PFTs-2: Physical system did not provide proper failure alarm and information [related to physical system development]; PTFs-3: Inadequate operation rules for the emergency condition [related to operation rule creation process];	

			CF4: Dispatcher was overconfident about the technical system CF5: Lack of experience about the failure condition; CF6: Too busy and Fatigue	ITFs-1: Inadequate communication between the station operator and the train D3115 driver; ITFs-2: Maintenance workers did not feedback to stop using the failure track circuit [Maintenance::A2]; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
		A5: Dispatcher did not inform the red-light strip information to D301 driver after dispatching it into the interval	CF1: Dispatcher thought it was not necessary to inform the red-light strip to D301 driver CF2: Dispatcher had an inadequate understanding of the system operation was influenced by D301 status CF3: Dispatcher did not get enough emergency rule to deal with the emergency situation CF3: Dispatcher believed the system was itself fail-safe CF4: Dispatcher was overconfident about the technical system CF5: Lack of experience about the failure condition; CF6: Too busy and Fatigue	PTFs-1: Inadequate operation rules for the emergency condition [related to operation rule creation process]; ITFs-1: Inadequate communication between the station operator and the train D3115 driver; ITFs-2: Maintenance workers did not feedback to stop using the failure track circuit [Maintenance::A2]; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
		A6: Dispatcher did not inform the station operator to hand over the train D301 after dispatching it	CF1: Dispatcher's control of train D301 did not match the scope of his control area CF2: Dispatcher believed the system was itself fail-safe	PTFs-1: Inadequate operation rules for the emergency condition [related to operation rule creation process]; ITFs-1: Inadequate communication between the station operator;	

			CF3: Lack of experience about the failure condition; CF4: Too busy and Fatigue	OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
	Station operator	A1:The station operator did not perform the junction control with D301 and did not inform D301 about the status of D3115 in time	CF1: The station operator's control of train D301 did not match the scope of his control area CF2: The station operator just waited for the D3115 driver calling in; CF3: The station operator's mental model of the track circuits was inconsistent with the real situation; CF4: Lack of experience about the failure condition; CF5: The station operator believed the system was itself fail-safe CF6: Weak perception about danger	PTFs-1: Inadequate operation rules about the junction control; ITFs-1: Inadequate communication with the train D3115 driver; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB arranged the long work time and heavy work load for operation staff [SRB::O1]; OGFs-3: SRB did not provide adequate operation rules [SRB::O2]; OGFs-4: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	SC1: The station operator should know operation procedures in emergency situation [P:[SRB:O-SC1][TPT::O-SC5]] SC2: The station operator should realise the failure of the communication channels and know how to deal with it [P:[SRB:O-SC6][TPT::O-SC5]] SC3: The station operator should connect with maintenance workers periodically to confirm the equipment status [P:[SRB:O-SC6]] SC4: The station operator should connect with Dispatcher workers periodically to feedback the equipment status in station [P:[SRB:O-SC6][TPT::O-SC5]] SC5: The station operator should know his responsibilities in the emergency situation [P:[SRB:O-SC6][TPT::O-SC5]]
		A2:The station operator did not report the equipment maintenance status to dispatcher in time	CF1: The station operator's control of the maintenance work was not exclusive CF2: The station operator though he did not need to check the equipment maintenance status forwardly and maintenance workers could report to Dispatcher directly	PTFs-1: Inadequate operation rules about the emergency condition; ITFs-1: Inadequate communication with the dispatcher and maintenance workers; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB did not provide adequate operation rules [SRB::O2]; OGFs-3: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	

		A3:The station operator knew that D3115 failed to turn to OS mode for three times and did not report this to dispatcher	CF1: The station operator had inadequate understanding of his control authority in the emergency situation CF2: The station operator just waited for the dispatcher asking CF3: Weak perception about danger	PTFs-1: Inadequate operation rules about the emergency condition; ITFs-1: Inadequate communication with the dispatcher and maintenance workers; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB did not provide adequate operation rules [SRB::O2]; OGFs-3: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
		A4: The station operator did not command D3115 driver to drive out of the failure track section	CF1: The station operator had inadequate understanding of his control authority in the emergency situation CF2: The station operator believed the system was itself fail-safe CF3: Weak perception about danger	PTFs-1: Inadequate operation rules about the emergency condition; PTFs-2: Operation rules regulated that everyone should comply with dispatcher's command at any situation ITFs-1: Inadequate communication with the dispatcher and D3115 driver; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB did not provide adequate operation rules [SRB::O2]; OGFs-3: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
	D3115 driver	A1:D3115 driver insisted to select OS mode to restart the train to run out of the failed section, just waiting for the right kinds of code for the on-board equipment to OS mode for 7 minutes and 40 seconds	CF1: D3115 driver put the dispatcher's command following at a higher priority than safety CF2: D3115 driver did not know that the command did not match the scope of the process under control in the emergency situation CF3: D3115 driver did not think about the influence to other trains of the long-time stay CF4: D3115 did not get any guide for this kind of emergency situation before	PTFs-1: Operation rules regulated that everyone should comply with dispatcher's command at any situation PTFs-2: Inadequate operation rules about the emergency condition; ITFs-1: Inadequate communication with the dispatcher [Dispatcher::A3]and the station operator; OGFs-1: Nanchang railway bureau [requiring information of Nanchang railway bureau];	SC1: D3115 driver should put the system safety in highest priority [P:[SRB:O-SC5][TPT::O-SC5]] SC2: D3115 driver should improve his understanding of system functions [P:[SRB:O-SC1][TPT::O-SC5]] SC3: D3115 driver should know the risk of the long-time stopping[P:[SRB:O-SC6][TPT::O-SC5]] SC4: D3115 should be given some guide for the emergency

			CF5: D3115 failed to connect with Dispatcher and the station operator to get new command CF6: Weak perception about danger		situation [P:[SRB:O-SC6][TPT::O-SC5]] SC5: D3115 should realise the failure of communication channel and know how to deal with it [P:[SRB:O-SC6][TPT::O-SC5]] SC6: D3115 driver should improve his understanding of system functions and be give a clear sign about the fail section [P:[SRB:O-SC6][TPT::O-SC5]] SC7: D3115 driver should know check the failure status periodically and find the new things about the failure [P:[SRB:O-SC6][TPT::O-SC5]] SC8: D3115 driver should be alert in advance for the failure situation [P:[SRB:O-SC6][TPT::O-SC5]] SC9: D3115 driver should realise the abnormal status about the track circuits and take actions to deal with it [P:[SRB:O-SC6][TPT::O-SC5]]
		A2: D3115 driver failed to report the condition to dispatcher and station operator	CF1: Communication interruption blocked the communication with dispatcher and the station operator	PTFs-1: Communication interruption	
		A3: D3115 insisted to report the situation to dispatcher	CF1: D3115 driver thought dispatcher could control him directly in the emergency situation CF2: D3115 driver was under control of the dispatcher and the station operator CF3: D3115 thought dispatcher had the higher control authority for him in the emergency situation	PTFs-1: Operation rules regulated that everyone should comply with dispatcher's command at any situation PTFs-2: Inadequate operation rules about the emergency condition; ITFs-1: Inadequate communication with the dispatcher and the station operator; OGFs-1: Nanchang railway bureau [requiring information of Nanchang railway bureau];	
		A4: D3115 driver did not supervise the operation of train D3115 to find the abnormal situation	CF1: D3115 driver just thought there was a normal failure on the track and the signal could turn red normally CF2: D3115 driver thought that he just needed to do something after the train braked down CF3: D3115 driver did not know using the stop point to confirm the failure condition	PTFs-1: Operation rules did not provide the requirements for the driver's supervision PTFs-2: Inadequate operation rules about the emergency condition; ITFs-1: Inadequate communication with the dispatcher [Dispatcher::A3] and the station operator; OGFs-1: Nanchang railway bureau [requiring information of Nanchang railway bureau];	
	Maintenance worker	A1:Maintenance workers did not follow the repair procedure to stop using the failed equipment	CF1: Maintenance workers put safety in a lower priority CF2: Maintenance workers did not know the regulated repair procedure	PTFs-1: there was not the operation rules existing for maintenance workers by hand ITFs-1: Inadequate coordination among maintenance workers; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	SC1: Maintenance workers should put system safety in highest position [P:[SRB:O-SC5]] SC2: Maintenance workers should know their responsibilities in emergency situation with emergency rules [P:[SRB:O-SC6][TPT::O-SC5]]

		A2:Maintenance workers did not report the failure conditions to the dispatcher or the station operator	CF1: Maintenance workers thought they should feedback the information to the dispatcher or the station operator after they solved the problem or the dispatcher or the station operator asked the failure information CF2: Maintenance workers did not know the regulated repair procedure CF3: Weak perception about danger	PTFs-1: there was not the operation rules existing for maintenance workers by hand ITFs-1: Inadequate coordination among maintenance workers; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	SC3: Maintenance workers should know the risk of their actions [P:[SRB:O-SC3][TPT::O-SC5]] SC4: Maintenance workers should connect with Dispatcher or the station operator periodically to confirm the equipment status [P:[SRB:O-SC6][TPT::O-SC5]] SC5: Maintenance workers should know the system functions [P:[SRB:O-SC2][TPT::O-SC5]]
		A4:Maintenance workers did not find the reason for the failure, and even not notice the PIO board failure alarm information from the signalling monitor system	CF1: Maintenance workers did not know how to do in the emergency situation CF2: Maintenance workers did not know the exact mean about the equipment alarm	PTFs-1: there was not the operation rules existing for maintenance workers by hand ITFs-1: Inadequate coordination among maintenance workers; OGFs-1: SRB did not supervise its staffs' actions for system safety [SRB::S1]; OGFs-2: SRB did not provide the proper training to operation staffs for emergency situations [SRB::O3];	
Unsafe supervision	MOR	S1:MOR did not inspect the safe operation and the safety rules execution of Shanghai Railway Bureau [O]	CF1: MOR did not clearly know its responsibilities for system safety CF2: MOR implemented an inadequate safety management	RGFs-1: There was not the regulations for MOR safety supervision implement	U-SC1: MOR should improve its understanding of system safety and recognize its responsibilities for system safety clearly U-SC2: MOR should establish proper safety management U-SC3:MOR should take the future situations into consideration when establishing up system development goals U-SC4: MOR should establish a proper management procedure for product technical reviews U-SC5: There should be an independent safety part to supervise MOR action
		S2: MOR had rushed to speed up the construction and system development, in order to catch up or be ahead of the schedule, and did not put enough considerations and actions on safety [D]	CF1: MOR did not implement adequate safety management CF2: time pressure CF3: MOR put safety in a lower priority	EEFs-1: There was not an independent safety part to supervise MOR action	
		S3:The product technical reviews lacked of sound basis and foundation [D]	CF1: MOR implemented an inadequate safety management CF2: There were inadequate assignments of the product technical reviews	PTFs-1: the materials supporting technical review was inadequate; ITFs-1: MOR needed to speed up [MOR::S2]	

			CF3: “fly-fix-fly” wrong safety concept		
	SRB	S1: SRB did not supervise its staffs’ actions for system safety [O];	CF1: SRB did not have an adequate safety management for formulating adequate operation rules for its own operation system: CF2: SRB did not allocate specific human resource to custom adequate operation rules for its own operation system: CF3: Low degree of safety culture.	PTFs-1: The CTC system development company did not provide adequate operation rules for the emergency condition: requiring for more information about the development company (did not exist in the accident official report). RGFs-1: MOR did not supervise the safety management of SRB [MOR::S1]; RGFs-2: MOR did not do improve the degree of support to the safety culture in SRB [MOR::O2].	U-SC1: SRB should establish proper safety management for rules execution and inspection based on the MOR safety management U-SC2: SRB should assign a proper position to execute the inspection based on its safety management procedure U-SC3: SRB should establish a proper assignment of the goals of the equipment validation and verification based system safety analysis U-SC4: SRB should supervise the priority of system safety of its staff [P: [SRB::O-SC5]]
		S2:SRB was not strict enough in the execution of the emergency operation rules, was not effective in monitoring the regulation execution in operation [O]	CF1: SRB did not have an adequate safety management for rules execution and inspection CF2: SRB did not know how to achieve the system safety goal in expectation CF3: SRB did not assign a proper position to execute the inspection	RGFs-1: Inadequate emergency operation rules RGFs-2: MOR did not supervise the safety management of SRB [MOR::S1]; RGFs-3: MOR did not do improve the degree of support to the safety culture in SRB [MOR::O2]; RGDs-4: The product technical reviews lacked of sound basis and foundation [MOR::S3].	
		S3:SRB did not follow the safety management standards to stop the equipment using in the new line without a comprehensive validation and verification [D]	CF1: SRB established the inadequate assignment of the goals of the equipment validation and verification CF2: SRB did not assign specific position to execute the equipment validation and verification CF3: “fly-fix-fly” wrong safety concept	PTFs-2: Underdeveloped system [TPT::O2&S1] RGFs-1: Inadequate safety management regulation RGFs-2: MOR did not supervise the safety management of SRB [MOR::S1]; RGFs-3: MOR did not do improve the degree of support to the safety culture in SRB [MOR::O2].	
	CRSC	S1:CRSC did not inspect the safety and quality management of CRSCD, and did not review the process for design and development activities [D]	CF1: CRSC did not assign a specific position to implement the inspection and review CF2: CRSC did not assign the clear goals and responsibilities of inspection and review	PTFs-1: System development based on an underdeveloped system [TPT::O2&S1] PTFs-1: The design flaws [TPT::S1&S2] RGFs-1: MOR did not supervise the safety management of CRSC [MOR::S1]; RGFs-2: MOR did not do improve the degree of support to the safety culture in CRSC [MOR::O2].	U-SC1: CRSC should assign a proper position to execute the inspection based on its safety management procedure U-SC2: CRSC should establish a proper assignment of the goals and responsibilities of

		S2:CRSC did not perform comprehensive validation and verification for the TCC system to ensure the product meets national safety and quality requirements [D]	CF3: CRSC did not have adequate safety management for the safety of its products CF4: CRSC did not assign the clear goals and responsibilities for product validation and verification	RGFs-1: MOR did not supervise the safety management of CRSC [MOR::S1]; RGDs-2: The product technical reviews lacked of sound basis and foundation [MOR::S3].	inspection and review based system safety analysis U-SC3: CRSC should establish proper safety management for rules execution and inspection based on the MOR safety management U-SC4: CRSC should establish a proper assignment of the goals and responsibilities of product validation and verification based system safety analysis
	CRSCD	S1:CRSCD made the decision to update TCC system based on the oral report from TPT, and did not effectively evaluate the quality and safety of the TCC been developing at that time [D]	CF1: CRSCD did not have adequate safety management for its sub-departments and products design CF16: CRSCD did not have an adequate communication channel with its sub-departments	RGFs-1:CRSC did not inspect the safety and quality management of CRSCD, and did not review the process for design and development activities [CRSC::S1]	U-SC1: CRSCD should establish proper safety management for its sub-departments and products design based on the CRSC safety management U-SC2: CRSCD should establish an adequate communication channel with its sub-departments based on its safety management U-SC3: CRSCD should establish a proper goal of the review based system safety analysis U-SC4: CRSCD should establish proper goals and responsibilities of product validation and verification based system safety analysis U-SC5: CRSCD should assign a proper position to execute the validation and verification based on its safety management procedure
		S2:CRSCD did not inspect the safety and quality management of TPT, and did not review the process for design and development activities [D]	CF1: CRSCD did not have proper safety management for its products CF18: CRSCD did not assign a clear goal of the review	RGFs-1:CRSC did not inspect the safety and quality management of CRSCD, and did not review the process for design and development activities [CRSC::S1]	
		S3:CRSCD did not perform comprehensive validation and verification for the TCC system [D]	CF1: CRSCD did not assign clear goals and responsibilities of the validation and verification CF2: CRSCD did not allocate specific position to implement the validation and verification	RGFs-1:CRSC did not perform comprehensive validation and verification for the TCC system to ensure the product meets national safety and quality requirements [CRSC::S2]	
	TPT	S1:TPT decided to research and develop LKD2-T1 TCC system based on an	CF1: TPT did not have proper safety management (such as hazards analysis and track) for its products	RGFs-1:CRSCD made the decision to update TCC system based on the oral report from TPT, and did not effectively evaluate	U-SC1: TPT should establish proper safety management for its products design based on the CRSCD safety management

		uncompleted product, and did not take a complete hazard analysis for new product [D]		the quality and safety of the TCC been developing at that time [CRSCD::S1] RGFs-2:CRSCD did not inspect the safety and quality management of TPT, and did not review the process for design and development activities [CRSCD::S2]	
Organisational influences	MOR	O1:MOR did not have a specialized department which is responsible for safety issues [O]	CF1: MOR did not have adequate assignment of safety goal CF2: MOR had inadequately allocated the control and management of the safety issues into difference departments	RGFs-1: There was not the regulations for MOR specific safety department EEFs-1: There was not an independent safety party to supervise MOR organisation	O-SC1: MOR should assign the safety goal based on its safety management O-SC2: MOR should allocate the control and management of the safety issues into proper departments based on its safety management O-SC3:MOR should know its responsibilities for system safety O-SC4: MOR should establish an adequate safety culture of preventing similar accident happen again into its safety management O-SC5: MOR should establish an adequate communication channel to collect all the emergency or incident situations based on its safety management O-SC6:MOR should establish proper emergency and failure management rules based its safety management O-SC7: MOR should establish a proper management for system regulations and standards O-SC8: MOR should make a management to control the change among regulations and standards
		O2:MOR just took punishment way to enforce the Shanghai Railway Bureau and its system operators to follow the safety rules [O]	CF1: MOR did not know how to implement the safety management in a scientific way CF2: MOR did not have an adequate safety culture	RGFs-1: Inadequate safety climate & culture	
		O3:Emergency and failure management rules were not complete [D]	CF1: MOR did not have an adequate communication channel to collect all the emergency or incident situations CF2: MOR did not have proper procedures to established adequate emergency and failure management rules	RGFs-1: Inadequate safety construction RGFs-2: Inadequate safety climate & culture	
		O4:The regulations and standards for the dedicated passenger line systems were not complete [D]	CF1: MOR did not have proper management of system regulations and standards CF2: All the regulations and standards changed respectively without thinking about others	RGFs-1: Inadequate safety construction RGFs-2: Inadequate safety climate & culture	
		O5:There were function overlaps between different departments inside of the organisation [D]	CF1: MOR did not have adequate assignment of safety goals	RGFs-1: Inadequate safety construction RGFs-2: Inadequate safety climate & culture	

		O6:The product technical reviews lacked sound basis and foundation [D]	CF1: There were not proper management of the product technical reviews CF2: MOR did not make a clear goal and responsibility for the product technical reviews	RGFs-1: Inadequate safety construction RGFs-2: Inadequate safety climate & culture	O-SC9: MOR should establish a proper management of its product technical reviews based on its safety management
	SRB	O1: SRB did not provide adequate operation rules[O]	CF1: SRB did not know the signalling functions in normal and abnormal situation CF2: There was not a proper communication channel between signalling monitoring system and operation system	RGFs-1:The regulations and standards for the dedicated passenger line systems were not complete [MOR::04]	O-SC1: SRB should establish proper safety management and training processes based on the safety management of MOR O-SC2:SRB should clear the contribution to system safety of the management and training processes O-SC3:SRB should take a good understanding of signaling monitoring functions O-SC4: The communication channel between signalling monitoring system and operation system should be established for the system safety based on system hazard analysis O-SC5: SRB should put the system safety in highest priority O-SC6:MOR should establish proper emergency and failure management rules based its safety management [P:[MOR::O-SC6]]
		O2: SRB arranged the long work time and heavy work load for operation staff [O]	CF1: SRB did not know the adequate work time and work load for operation staff	RGFs-1:The regulations and standards for the dedicated passenger line systems were not complete [MOR::04] RGFs-2: SRB just arranged the work based on experience;	
		O3: SRB did not provide the proper training to operation staffs for emergency situations[O]	CF1: Inadequate safety management CF2: Inadequate safety supervision on operation staff CF3: Lack knowledge of emergency situations	RGFs-1:Emergency and failure management rules were not complete [MOR::O3] RGFs-2:The regulations and standards for the dedicated passenger line systems were not complete [MOR::O4] RGFs-3: SRB did not supervise its staffs' actions for system safety to find existing problem [SRB::S1];	
	CRSC	O1:CRSC did not establish a safety management program for the CRSCD [D]	CF1: CRSC did not know the responsibilities of safety management CF2: CRSC did not know the goals of the safety management	RGFs-1:CRSC did not inspect the safety and quality management of CRSCD, and did not review the process for design and development activities [CRSC::S1] RGFs-2:There were function overlaps between different departments inside of the organisation [MOR::O5]	O-SC1:CRSC should clear the responsibilities of safety management based on the system functions and MOR safety management O-SC2: CRSC should establish a proper goal of the safety management based on system hazard analysis

	CRSCD	O1:CRSCD did not give out the safety requirements and safety design principles for TCC system development, just allowed the TPT referenced the experience of an uncompleted product [D]	CF1: CRSCD did not have proper safety management for its products and sub-departments CF2: CRSCD did not realize the goals of establishment of safety requirements and safety design principles for TCC system CF3: CRSCD just thought TPT could compliance the product safety requirements by itself	RGFs-1:CRSC did not establish a safety management program for the CRSCD [CRSC::O1] RGFs-2:CRSC did not inspect the safety and quality management of CRSCD, and did not review the process for design and development activities [CRSC::S1] RGFs-3:The regulations and standards for the dedicated passenger line systems were not complete [MOR::O4]	O-SC1:CRSCD should establish proper safety management for its products and sub-departments based on the safety management of CRSC O-SC2: CRSCD should always clearly know the goals of safety requirements and safety design principles for TCC system O-SC3: CRSCD should always take safety management to its sub-departments and never assume the working status of them O-SC4: CRSCD should clear the contribution to system safety of the management
		O2:CRSCD did not establish a safety management program for the TPT [D]	CF1: CRSCD did not realize the importance of the safety management program	RGFs-1:CRSC did not establish a safety management program for the CRSCD [CRSC::O1] RGFs-2:CRSC did not inspect the safety and quality management of CRSCD, and did not review the process for design and development activities [CRSC::S1]	
	TPT	O1:TPT did not establish a fix research and development group for LKD2-T1 development, just through oral report to report the design and development process to CRSCD [D]	CF1: TPT had an inadequate safety management system for its products and did not think about the change of external factors CF2: There was an inadequate communication channel provided for the product development	RGFs-1:CRSCD did not establish a safety management program for the TPT [CRSCD::O2]	O-SC1: TPT should establish an adequate safety management system for its products based on the safety management of CRSCD and take the external factors into consideration when implement safety manage O-SC2: An adequate communication channel provided for the product development should be established between different product design groups O-SC3: TPT should establish adequate safety management for its products based on the safety management of CRSCD O-SC4: TPT should establish adequate safety management for its products and learning processes based on the safety
		O2: TPT did not make a complete product design plan for LKD2-T1 and a design materials track management rules. That led the design materials missing in the design process [D]	CF1: TPT had not an inadequate safety management CF2: Design staff was lack of safety concept CF3: Design staff violated the safety regulation CF4: Design staff was lack of safety evluation	RGFs-1:The regulations and standards for the dedicated passenger line systems were not complete [MOR::O4] RGFs-2:TPT did not establish a fix research and development group for LKD2-T1 development, just through oral report to report the design and development process to CRSCD [TPT::O1]	
		O3:TPT did not have a staff competent assessment plan and make a training plan to	CF25: TPT did not have inadequate safety management and learning processes	RGFs-1:CRSCD did not establish a safety management program for the TPT [CRSCD::O2]	

		improve staff competent [D]			management of CRSCD and system hazard analysis O-SC5:TPT should provide documents for equipment functions and instructions for equipment users

Note：1. The form A::B means that B is an action or factor of A, A stands for component, e.g. SRB; [A::B] is a symbol means that the factor relates to this item; 2. [D] is a symbol means that a component may influence the system safety condition in the system development phase; [O] is a symbol represents that a component may influence the system safety condition in system operation phase. While [D, O] indicates that the influence may happen in both phases; [P] is a symbol represents that this is the precondition for a safety countermeasure.

Table 6: The summary of the results of HS-RA(s) analysis (the details in Table 4-3)

	Preliminary factor Identification			Analysis		Recommendation
HS-RA(s) level	**System phase**		**Total**	**Causal factors**	**Contextual factors**	**Countermeasures**
	Development	**Operation**				
Unsafe acts	3	17	20	64	48	35
Unsafe supervision	9	3	12	23	18	19
Organisational influences	10	5	14	25	12	25
Total	22	25	46	112	78	79

Table 7: The summary of the results of HFACS-RA(s) analysis (from Zhan et al., 2017, p243)

HS-RA(s) level	**Causal factors**
Unsafe acts	4
Preconditions for Unsafe Acts	5
Unsafe supervision	6
Organisational influences	**7**
Total	22