Safety Science 88 (2016) 166–179

Contents lists available at ScienceDirect

Safety Science

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

An integrated hazard identification method based on the hierarchical Colored Petri Net

Rui Wang [a,b], Wei Zheng [a,*], Ci Liang [c,d], Tao Tang [e]

[a] National Research Center of Railway Safety Assessment, Beijing Jiaotong University, No. 3 Shang Yuan Cun, Haidian District, 100044 Beijing, China
[b] LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France
[c] Institut de Recherche Technologique Railenium, F-59300 Famars, France
[d] IFSTTAR-COSYS/ESTAS, F-59666 Lille-Villeneuve d'Ascq, France
[e] State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, No. 3 Shang Yuan Cun, Haidian District, 100044 Beijing, China

ARTICLE INFO

Article history:
Received 21 June 2013
Received in revised form 9 October 2015
Accepted 19 May 2016
Available online 28 May 2016

Keywords:
Hazard identification
Formal model
Hazard log
Chinese Train Control System

ABSTRACT

The traditional hazard analysis approaches applied to the socio-technical system cannot cover the complex organization structures, the interactions between systems and human behaviors, the interrelated factors among sub-systems and the safety culture of specific societies. This paper presents an integrated hazard identification approach named System-Theoretic Process Analysis Based on Formalization Model (BFM-STPA), which can solve the above issues. Firstly, the hierarchical control structure models of the socio-technical system are established through Colored Petri Nets (CPN) due to its strong description ability and executable ability, which may also be regarded as the graphical system specification. Secondly, the hazards can be identified according to the CPN models following a series of guide conditions. Thirdly, the comprehensive contributing factors to the hazards will be found out by tracing the former states within the reachability graph generated from CPN model. Finally, an integrated hazard log can be derived for further hazard analysis and safety-guided design. In this paper, the above method was applied in the Chinese Train Control System level 3 (CTCS-3). And the process of hazard identification for the scenario of *Temporary Speed Restriction issued* was elaborated in detail. Compared with the hazard log generated by Hazard and Operability (HAZOP), the hazard log generated by BFM-STPA covered not only the subsystem failures, but also the deviation of interactions among subsystems from design intent, human errors and socio-technical drawbacks related to the TSR Issued scenario of CTCS-3.

1. Introduction

Train control system is a typical safety–critical system due to the high operating speed and thousands of passengers on board. It was reported that the rail passenger traffic of China exceeded 1.862 billion trips in the year of 2011 (Jin, 2012) and the figure kept increasing (ASKCI, 2013). Among those passengers, approximate 23.6% of them chose to take the high-speed train (Jin, 2012; Zhang, 2012), which included all commercial train service with an average speed of 200 km/h or higher. Simultaneously, the total length of high-speed tracks in China was over 7500 km by 2012 and the figure will reach 18,000 km in the year of 2020. Therefore, in consideration of the increasing extensive rail network, the integrated safety of Chinese Train Control System (CTCS) is one of the most critical issues that railway stakeholders need to deal with.

In recent years, severe accidents of trains configured with CTCS still occurred from time to time, such as the 4–28 Jiaoji railway accident and 7–23 Yongwen railway accident. According to the investigation reports of accidents issued by China State Administration of Work Safety (SAWS, 2011), these two railway accidents were judged as the accidents mainly caused by staff's negligence after Temporary Speed Restriction (TSR) order loss or component failures (Ouyang et al., 2010; Dong, 2012). And even for the high-speed train whose operation speed is over 300 km/h (186 mph), the incidence and minor accidents occasionally occurred due to the organizational flaws and human errors, referring to the safety data of Wuguang Line. Here is an event happened in the year of 2009 on the Wuguang Line: a railway staff finished his maintaining work of a switch machine without checking the bolt of a pedal of the switch machine. And then a high-speed train passed the set of points driven by the above switch machine in full speed.

* Corresponding author.
E-mail addresses: rwang@laas.fr (R. Wang), wzheng1@bjtu.edu.cn (W. Zheng), ci.liang@railenium.eu (C. Liang), ttang@bjtu.edu.cn (T. Tang).

http://dx.doi.org/10.1016/j.ssci.2016.05.006
0925-7535/

Consequently, the unfixed pedal was inhaled under the train by the high-speed airflow and caused scratches on the bottom of the car body. Another event in 2010 was a collision accident between two maintenance locomotives aroused by lack of watching of one driver and one train running two times over the required speed for maintaining work. It led to the derailment of one locomotive and a 7-h interruption of the corresponding line. All the personnel related to the above accidents were either subjected to correspondent legal sanctions or given internal punishment. Though necessary punishment to people who violates the operation rules is certainly important, merely punishing the relative crews will not solve the existing potential defects in both technical aspects and organizational management. Therefore, it is an emergent task to find out a method, which has the ability to deal with this kind of complex system, to identify the potential hazards hidden in a system before the system is designed and put into operations. And the safety requirements obtained from the hazard log should be used to instruct the safety-guided design, which ensures the safety of the system to a large extent.

Preliminary Hazard Analysis (PHA), as its name suggests, is one basic method to identify hazards of systems. And it was recommended and recorded in the standard of CENELEC EN 50126, Railway applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (CENELEC EN 50126, 1999). To get a complete survey of all possible hazards under the framework of this approach, it may benefit from using a hazard checklist. A typical hazard checklist includes energy source and propagation paths, hazardous functions (operations, components, and materials), lessons learned from similar type systems, etc. While PHA is less expensive and easier to implement, it suggests to be used in the early stage of the system life cycle, i.e., the phase of System Definition and Application Conditions (CENELEC EN 50126, 1999) and it might not be adequate to handle the hazard analysis for systems of great complexity as the only technique that is applied (Ericson, 2005).

Another commonly used hazard identification method is Hazard and operability (HAZOP) analysis. The Lloyd's Register of Shipping firstly introduced the HAZOP study, which had been usually applied to the process industry, into the field of computer system (Earthy, 1992). The classic HAZOP concentrates on the analysis of the properties and behaviors of flows in the pipelines linking the chemical containers, such as storage tanks, reactor vessels and pumps. Thus, if information flows between components are regarded as the pipe flows, HAZOP analysis can be applied effectively to software system (McDermid and Pumfrey, 1994). The ERTMS Safety Requirement & Objective Group (ESROG) conducted the Special Safety Study for European Rail Traffic Management System (ERTMS) with HAZOP to identify the potential hazards arising from the operation process in the condition of ERTMS Level 2 configuration (ESROG, 2000). In the year of 2010, Hwang et al. proposed one method called HAZOP-KR, which was applied to the Korean train control system for hazard identification (Hwang et al., 2010). However, due to the lack of prescribed way to present systems, the system representation models to be analyzed in HAZOP process are different among all of the above application cases. Earthy emphasized the importance of graphical model rather than the textual specifications and even codes (Earthy, 1992). Thus, the data flow diagrams and transaction network were chosen as the ideal form of diagram, but no further information of the diagrams was provided. Two years later, McDermid and Pumfrey (1994) elaborated the HAZOP study applied in software system, and complemented some details about the analysis procedure, including adjusting the common guide words into the ones which were suitable for software safety analysis, and putting forward the alternative strategies for the meaningful failure modes (hazards) as the design modifications or safety requirements for low-level design. And the authors used the system decomposition figure as the representation model with information flow consistently labeled. In 2000, ESROG established a set of comprehensive models to represent the system behaviors and information flow. The models were State Transition diagram (STD) and Sequence and Collaboration Diagrams (S&Cs) based on Unified Modeling Language (UML). Moreover, there were some constraints in both quantitative and qualitative aspects between the STD and S&Cs in order to ensure the consistency of representation across many diagrams (ESROG, 2000). The identified hazards by ESROG were much more numerous and specific. Hence, it can be concluded that the quality and quantity of the hazards are determined by the soundness of the system models analyzed in the HAZOP study. The reason for the inconsistency of the effect of this hazard identification method is that the approach was developed to point out the potential hazardous states for the process industry. Furthermore, according to the background that the analyses work is suitable for the Piping & Instrument Diagram (P&ID), the guide words are more specialized in depicting the corresponding properties, like temperature, pressure and liquid flow. Once this hazard identification approach is introduced into other engineering fields, the attendant cost of seeking out or even developing appropriate system representation models and interpreting the original guide words into the ones proper for the certain context will be enormous.

Concerning the complex system like CTCS, the factors that affect its safety referring to not only the technical ones within the train control system, but also the latent interactions with the management system and the external environment. The complex internal relations among its subsystems and the interactions with the external society and natural environment greatly restrict the operability of hazard identification. In order to generate comprehensive hazards of the complex system and improve the efficiency of hazard analysis, Leveson proposed the System-Theoretic Process Analysis (STPA) (Leveson, 2011) based on her system safety theory, which was named as STAMP (Systems-Theoretic Accident Model and Processes) and firstly put forward in 2004 (Leveson, 2004). In this theory, a hierarchical model was also provided to describe the system to be analyzed. Thence, STPA became a new concern of hazard identification approach. Pasquale et al. and Dong applied the STPA to identify unsafe control actions of Communication Based Train Control System (CBTC) and automated door controller system, respectively (Pasquale et al., 2003; Dong, 2012). But the superiority of STAMP was not demonstrated in the above paper due to the fact that the influence of socio-technical factors was ignored. Fleming et al. compared the safety assurance for air transportation conducted by STPA with the traditional methods developed approximate 50 years ago, and discovered the advantages of this new method in identifying the causes, the design requirements and the potential solutions to prevent accidents (Fleming et al., 2013). In another case, STPA has been applied in the safety assessment of road tunnel (Kazaras et al., 2012). Both the technical hazards and additional ones involving software-intensive complexity, organizational and human errors were found out in the above application. However, tunnel safety control structure seemed oversimplified, which was not sufficient to represent complex system (like CTCS). In addition, the inadequate expressive ability existing in the general form of control structure of STPA is obvious. The process and outcomes of the analysis are almost textual description, which is lack of readability and portability.

In this paper, we propose an innovative hazard identification method for complex system according to STPA, that is, STPA hazard identification Based on Formalization Model (BFM-STPA). The BFM-STPA combines the STPA hazard identification approach with the formalization method of Colored Petri Nets (CPN) to establish system control structure models, identify hazards, and generate hazard log. The distinct features of this method are listed: