An Integrated Hazard Identification Method for Socio-technical Systems based on STPA

Rui WANG, Wei ZHENG, Ci LIANG, Gilles MOTET

LAAS-CNRS
Université de Toulouse
7 avenue du colonel Roche
31077 Toulouse, France
rui.wang0309@gmail.com

National Engineering Research Center of Rail Transportation Operation and Control System
Beijing Jiaotong University
No.3 Shang Yuan Cun, Hai Dian District
100044 Beijing, China
wzheng1@bjtu.edu.cn

CASCO Signal Ltd.
6F Wanfengyihe Building, 12 Jia Yue Tan South Street
100045 Beijing, China
liangci321@126.com

LAAS-CNRS
Université de Toulouse
7 avenue du colonel Roche
31077 Toulouse, France
Gilles.Motet@insa-toulouse.fr

Abstract: The traditional hazard analysis approaches applied to the socio-technical system can not 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 methodology named BFM-STPA(STPA hazard identification Based on Formalization Model) based on formalization model, which can solve the above issues. Firstly, the hierarchical control structure models of the socio-technical system are built with 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 with in the reachable 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 CTCS-3.

Keywords: Railway Transportation; Hazard Identification; Colour Petri Net; STAMP;

1 Background

The train control system is a typical safety-critical system in terms of the high operating speed and thousands of passengers on board. In recent years, the major accidents of trains configured with CTCS still occurred from time to time, like the 4-28 Jiaoji railway accident and 7-23 Yongwen railway accident. According to the investigation reports of the major accidents from Chinese Government, these two railway accidents were assigned as the accidents mainly caused by staff negligence after Temporary Speed Restriction (TSR) order loss or component failures [Ouyang02] [Dong03]. And even for the high speed train whose operation speed is over 300km/h (186mph), the accidents occasionally occurred due to the organizational flaws and human errors. All the personnel related to the above accidents were either subjected to correspondent legal sanctions or given internal punishment. Though fair punishment to people who violates the operation rules is certainly important, merely punishing the relative crews will not solve the existing potential defects in technical aspects and organizational management[Leveson05]. 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 the complex system before the system is designed and put into operations. And the safety requirements obtained from the hazard log are utilized to instruct the safety-guided design, which ensures the safety of the system to a large extent.

In this paper, we proposed 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 combined 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:

1) Taking the advantage of the excellent description capability of CPN, we established the safety models of CTCS Level 3 (CTCS-3) in hierarchical structure. In this case, the control structure model was more explicit and more apposite to be analyzed as a substitute for a real physical system.

3) A comprehensive hazard log in regard to the TSR issued scenario of CTCS-3 had been generated, including the organizational and technical hazardous states. Moreover, the interactive factors among internal subsystems and external interferences could be identified in this method effectively.

4) We also proposed a formalized approach to conduct the hazard analysis, figuring out the causes leading to hazards. Namely, with the help of the reachable state graph derived from the CPN model, the causal factors of a hazard could be found out.

2 Introduction and Application of BFM-STPA

The ascendency of STAMP is the comprehensive consideration of all kinds of contributing factors to accident. However, the classic STAMP control structure model suffers from the lack of performance on formal description of specific system behaviors, the process models of controllers and the deficiency of data structure. Hence, an optimization method, the BFM-STPA, has been creatively put forward in this paper to supplement the drawbacks of modeling means of the STAMP. This method provides a series of hierarchical control structure models to describe the STS and facilitates analyzing the social and organizational flaws. Specifically, the systematic control structure models are composed of Socio-Technical Control Structure Model (ST-CSM), Operating Scenario Control Structure Model (OS-CSM), and Controller Process Model (CPM). Figure 1 illustrates the multi-layer structure of the three kinds of CPN models. CPN helps to improve the ability of modeling in a large scale. The multi-layer models use the different types of variables (that is the colored variable) to describe the commands and feedback messages between controllers of each level, and utilize the ML language to constrain the interactive conditions.

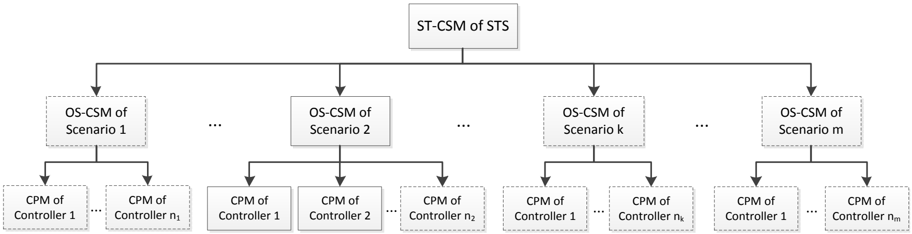

Figure 1: The multi-layer structure of CPN models

The procedure of the BFM-STPA hazard identification method is shown in Figure 2. There are 5 steps to implement this analysis work. The specific steps of performing the hazard identification on STS with BFM-STPA are described as follows:

1) Establishing the three-layer hierarchical control structure models in accordance with the functional requirements and system requirements of the CTCS-3;

2) According to the fundamental hazards and safety constraints on the system level, identifying the potential inadequate control actions that lead to hazardous states with the given guide conditions. The inadequate control actions or the situation of breaking the safety constraints could be caused by the occurrence of the following guide conditions:

F1. Required control actions (for safety) are not provided;

F2. Incorrect or unsafe control commands are given;

F3. Potentially correct control commands are provided at the wrong time (too early or too late), or in wrong sequence;

F4. Control is stopped too soon or applied too long.

3) Generating the SSRG of the CPN model with CPN tools;

4) Based on the SSRG and control structure models, figuring out the ways how the hazardous control actions identified in Step 3) could happen in the following 3 paths.

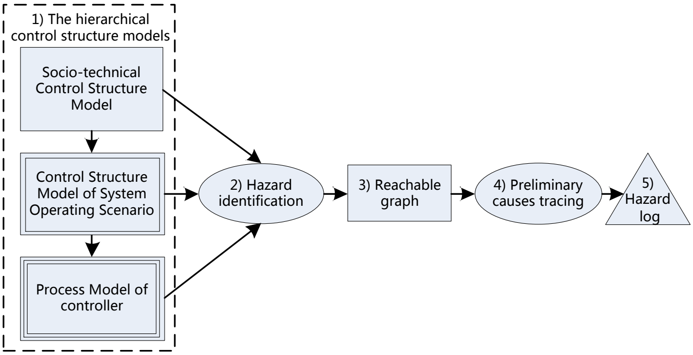
1) The hierarchical control structure models
Socio-technical Control Structure Model
Control Structure Model of System Operating Scenario
Process Model of controller
2) Hazard identification
3) Reachable graph
4) Preliminary causes tracing
5) Hazard log

Figure 2: Frame of BFM-STPA hazard identification method

a. Tracing the possible causes that lead to the hazards with SSRG.

Ⅰ. Finding out the reachable state in which the control action carries out, based on the specific tokens in places shown in SSRG;

Ⅱ. Tracing back to the previous states and searching for the causes. Basically, the errors causing the hazards can be categorized into system error and stochastic error. Here, it is more appropriate to divide the human error and the organizational flaw from the system error so as to pay more attentions to these two types of errors. Thus, the system error mainly refers to the dysfunction of software, and the stochastic error is component failure of which the distribution is generally in concordance with the Bathtub curve [Norros06].

b. Identifying the potential causes resulting in unsafe control actions with the hierarchical control structure models. For each hazardous control actions, all parts of the corresponding control loops have to be examined; there may be conflicts and potential coordination problems that need to be identified, when multiple controllers are responsible for the same component or the same safety constraint.

c. Speculating how the control actions could degrade over time, and adding the preventive measures, including:

Ⅰ. Setting up adjustment mechanism of organizational structure to assure implying the safety constraints where some changes appear;

Ⅱ. Implementing the performance audit；

The performance audit is the prerequisite for operating audit and control. Only in this way, can the safety constraints be implied.

Ⅲ. Tracing the abnormal situations found in the accident analyses;

5) Generating the comprehensive hazard log which should be suitable for being maintained in following stages of system life cycle.

Due to the complexity of CTCS-3 system, we apply BFM-STPA methodology to the scenario of temporary speed restriction issued for instance. To analysis the result of this method, we compared the BFM-STPA with the method of HAZOP (Table 1) against the same scenario of TSR Issued in ETCS-2. For there was no published work that conducts the HAZOP on CTCS-3 system and the ETCS-2 system had the exactly same operating mechanism with the CTCS-3, we made this comparison between these two system. BFM-STPA identified 49 hazards in total, including 6 hazards related to socio-technical factor and 9 hazards involving human factor. However, 14 hazards related to this scenario were identified by method of HAZOP[ESROG07] involving only 1 hazards of human factor. Therefore, BFM-STPA hazard identification presented in this paper not only covers socio-technical factors and human factors, but also contains more comprehensive technical factors.

Furthermore, the HAZOP requires great quantity of HAZOP sessions and expertise to build models and identify the hazards. However, the BFM-STPA demands some personal experience to establish the control structure models and less systematic knowledge to identify the inadequate control actions and causal factors due to the enough information contained in the models. And it makes the process of system hazard identification standardized, and reduces the dependence on experience of experts.

Table 1 Result of contrasting BFM-STPA method with HAZOP method

Method	**#Socio-technical Factor**	**#Human Factor**	**#Technical Factor**	**#Hazards in Total**
BFM-STPA	6	9	34	49
HAZOP	0	1	13	14

3 Conclusion

This paper presented the hazard identification method of BFM-STPA mainly for STS and its application. And the incorporation of CPN mode, which helped to substitute the original control structure model in STPA, largely enriched the systematic features that could be modeled before. As we all know, the more details of a system were describe in models, the more valuable hazards with significant guidance to system design could be identified. Besides, though the accident causation model of classic STAMP focused on the social part of contributing factors that leading to mishaps, the proposed method in this paper involved a large number of technical elements as well. Furthermore, taking the advantage of the CPN tools, the reachable graph could also be utilized to analyze the causes of a certain hazard. During the process of analyzing CTCS-3 in this paper, we obtained the following experience of how to effectively utilize this method.

On one hand, it should be emphasized that the CPN models have to involve as many details of system as possible on the basis of analysis requirement. Hence, the control structure models can become the graphical specification of the system. Although the complexity of models requires more expertise, it is worthy of figuring it out in this stage and decompose immense STS in order to avoid the large-scale workshops of the hazards identification conducted afterwards.

On the other hand, the CPMs should be analyzed with the guide conditions as well. For we find that the guide conditions limit the hazards in the layer of the analyzed control actions, the only possibility to identify the detailed hazards exists in studying more control actions in CPMs, where there are lots of functions and interactive messages.

In addition, this method is highly recommended to be widely applied in the other STS and the future work will be the risk analysis based on the hazards identified by the BFM-SPTA.

References

[Ale04] Ale B. J. M., Bellamy L. J., Cooke R. M., et al., 2006. Towards a causal model for air transport safety—an ongoing research project. Safety Science, 44(8): 657-673.

[ASKCI01] ASKCI, 2013, China's Railway Market Forecast and Industry Research Report (2013-2017). http://www.askci.com.

[Ouyang02] Ouyang M., Hong L., Yu M. H., et al., 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.

[Dong03] Dong A., 2012, Application of CAST and STPA to railroad safety in China. mit.edu.

[Ale04] Ale B. J. M., Bellamy L. J., Cooke R. M., et al., 2006. Towards a causal model for air transport safety—an ongoing research project. Safety Science, 44(8): 657-673.

[Leveson05] Leveson, N.G., 2011. Engineering a Safer World: Systems Thinking Applied to Safety (Engineering systems). MIT Press, Cambridge, MA.

[Norros06] Norros, L., 1996. System disturbances as springboard for development of operators' expertise. Cognition and communication at work, 159-176.

[ERTMS07]ERTMS Safety Requirements and Objectives Group (ESROG), 2000. ERTMS Scope, Boundary and Hazards, ESROG-SBH-01, Issue 1 Draft 3.