Hazard Analysis of Collision Avoidance System using STPA

Sardar Muhammad Sulaman
Dept. of Computer Science, Lund University, Sweden.
Sardar@cs.lth.se

Taimoor Abbas
Dept. of Electrical and Information Technology, Lund University, Sweden.
Taimoor.abbas@eit.lth.se

Krzysztof Wnuk
Dept. of Computer Science, Lund University, Sweden.
Krzysztof.Wnuk@cs.lth.se

Martin Höst
Dept. of Computer Science, Lund University, Sweden.
Martin.Host@cs.lth.se

ABSTRACT

As our society becomes more and more dependent on IT systems, failures of these systems can harm more and more people and organizations both public and private. Diligently performing risk and hazard analysis helps to minimize the societal harms of IT system failures. In this paper we present experiences gained by applying the System Theoretic Process Analysis (STPA) method for hazard analysis on a forward collision avoidance system. Our main objectives are to investigate effectiveness in terms of the number and quality of identified hazards, and time efficiency in terms of required efforts of the studied method. Based on the findings of this study STPA has proved to be an effective and efficient hazard analysis method for assessing the safety of a safety-critical system and it requires a moderate level of effort.

Keywords

Hazard analysis, risk analysis, STPA, forward collision, safety critical

INTRODUCTION

The increasing dependence of our society on IT systems brings not only new development opportunities but also new, severe, risks and threats. As our daily life is dependent on IT systems, i.e., both for individuals and organizations (private and public), failures of these IT systems can have serious negative consequences and effects on the society. Diligently performing risk and hazard analysis helps to minimize the societal harms of the IT system failures (Leveson, 2012; Sulaman et al., 2013). However, the risk/hazard analysis of a modern socio-technical system is far from trivial, mainly due to the dynamic behavior that pervades almost every modern software intensive system and a high number of interacting components. As a result, many 'traditional' low level risk or hazard analysis methods fail to encompass the dynamic behavior of the systems, as they focus solely on the system component failures (Leveson, 2012). Therefore, new methods for performing risk and hazard analysis optimized for dynamic systems are highly required.

This study presents experiences gained by applying the System Theoretic Process Analysis (STPA) (Leveson et al., 2012) method for hazard analysis on a forward collision avoidance system as an example of a socio-technical safety-critical system. The main objective of this study is to investigate the effectiveness (number and quality of identified risks) and time efficiency (required effort) of the STPA hazard analysis method in the software intensive safety-critical system domain.

Based on the gained experiences from this study it can be concluded that STPA is an effective method as it in its first step identified 14 inadequate control commands or events with associated hazards. Regarding required effort it can be concluded that STPA requires a moderate level of effort.

RELATED WORK

There exist a number of low-level risk analysis methods for technical systems in general or for information systems in particular (Sulaman et al., 2013). Some of the most well-known methods are Fault Tree Analysis (FTA) (Ericson, 1999), Event Tree Analysis (ETA) (Tobioka et al., 1981), Failure Mode and Effect Analysis (FMEA) (McDermott et al., 1996), probabilistic FMEA (Aljazzar et al., 2009), Hazard and operability study

(HAZOP) (McDermid et al., 1995) and Cross-Impact Analysis (Bañuls and Turoff, 2011).

The afore-mentioned methodologies provide sufficient support for low-level risk or hazard analysis. However, they require detailed design specifications for the analysis and they do not take the dynamic behavior of systems into consideration. To tackle the lack of design specification in the early design phase, Johannessen et al. (2004) proposed an actuator-based approach for hazard analysis. Gleirscher (2013) suggested a framework for hazard analysis that helps to analyze dynamic behavior of technical systems. Leveson (2012) proposed a hazard analysis method, STPA, which tackles the dynamic behavior of the system by considering the safety as a control problem rather than a component failure problem. Nakao et al. (2011) evaluated the STPA technique in a case study where it is applied on an operational crew-return vehicle design. The feasibility and usefulness of STPA technique is also evaluated thoroughly for early system design phase in (Ishimatsu et al., 2010). These studies (Ishimatsu et al., 2010; Nakao et al., 2011) conclude that with STPA it is possible to recognize safety requirements and constraints of the system before the detailed design. Several authors (Leveson, 2012; Pereira et al. 2006; Thomas et al., 2011) reported positive outcomes from applying STPA on various systems.

BACKGROUND

System theoretic process analysis (STPA)

The System Theoretic Process Analysis (STPA) method for hazard analysis developed by Leveson et al. (2012) focuses on analyzing the dynamic behavior of systems, and in this way provides significant advantages over the traditional hazard analysis methods. STPA is a top-down method, just like FTA. On the contrary, STPA uses a model of the system that consists of a functional control diagram instead of a physical component diagram used by traditional hazard analysis methods. STPA is based on system theory rather than reliability theory, and it considers safety as a system's control (constraint) problem rather than a component failure problem. Among the benefits of using the STPA Ishimatsu et al. (2010) listed the efficiency of the later phases of STPA when the broader scenarios are analyzed. The later phases of STPA take into consideration the interactions of system components by considering the evaluated system and its components as a collection of interacting control loop. STPA requires a control structure diagram for hazard analysis consisting of components of a system and their paths of control and feedback. It is important to mention that STPA can be applied at any stage, such as in the design phase and in the operational phase. It is carried out in the following two steps:

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. A hazardous state is a state that violates the system's safety requirements or constraints and can cause a loss.
2. Determine how each potentially hazardous control action, identified in step 1, could occur. An inadequate control action can lead a system to a hazardous state in the following ways: 1) a control action required is not provided, 2) an unsafe (incorrect) control action is provided, 3) a control action is provided too early or too late (wrong time or sequence), or 4) a control action is stopped too early or applied too long.

Forward collision avoidance system

A forward collision avoidance system alerts a driver of a vehicle about a crash situation and applies automatic brakes if the driver does not respond to the warning alert. The system performs two main functions: 1) object/obstacle detection (by using forward-looking sensors) and 2) generation of warnings or activation of auto breaks (passive/active response). The forward-looking sensors could use techniques like radar, infrared, motion sensors, and cameras (Bond et al., 2003; Coelingh et al., 2010). Figure 1 shows the forward collision avoidance system (Bond et al., 2003) that has been divided into part A (the collision controller), part B (the brake controller), and part C (the engine torque controller).

The *collision controller* is connected with the *radar and the camera* through the *object detection system*. The *vehicle sensor complex* is also connected with the collision controller that generates a signal, and then sends it to the collision controller. The *vehicle sensor complex* consists of several vehicle system sensors, such as a brake position sensor, throttle position sensor, steering sensor, suspension sensor, speed sensor, and seat belt sensor. The *warning indicator* connected with the collision controller generates a collision warning signal in response to the collision-assessment of the collision controller. The collision controller gets input from the object detection system and the vehicle sensor complex when it performs the collision assessment.

The *collision controller* (shown in part A), works as follows: The *vehicle and object status* provider in the collision controller calculates and provides the current status of the object in front of the vehicle and the current status of the vehicle to the collision probability estimator. The *collision probability estimator* in the collision controller calculates the vehicle collision probability based on the received information. If there is a risk of collision then the estimator sends a signal to the indicator, which is for the vehicle's driver. The *collision*

controller uses an algorithm to estimate the risk of collision and generates a collision-assessment signal. If the vehicle's operator responds to the collision warning on time then the forward collision avoidance system resets all its components and calculated parameters. However, if the operator does not respond to the received warning then the *collision controller* sends a collision-assessment signal with the *object and vehicle status* signals to the *brake and engine torque controllers* to apply autonomous brake.

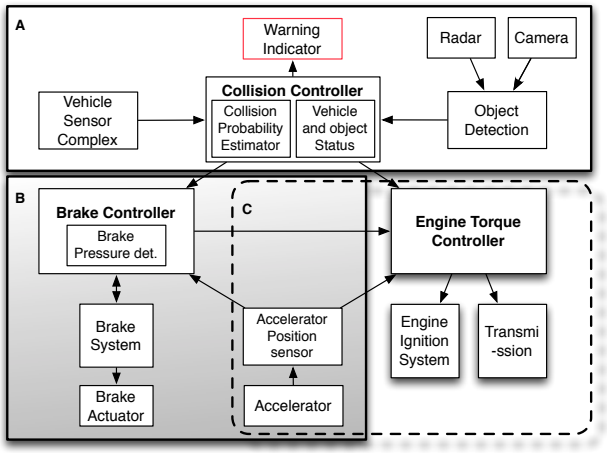

Figure 1: Forward collision avoidance system with autonomous braking (Bond et al., 2003)

As for part A of the system, part B and part C also consists of a number sub-systems that communicates through signals. The main objective of part B is to control the brakes based on input from the *collision control system* (part A) and the vehicle's operator. The main objective of the *engine torque controller* is to control the engine torque. In order to save space, part B and part C are not described as detailed as part A, although equally much information was available when the hazard analysis was conducted, see Bond et al. (2003).

HAZARD ANALYSIS

For hazard analysis the detailed control structure diagram of the system was acquired. Next, the first and the second author of this study analyzed the forward collision avoidance system and identified 14 inadequate control commands or events, including their causal factors. The results (both inadequate control commands or events and their causal factors) were analyzed and reviewed by the third and the fourth author. In this study, the authors have performed hazard analysis of the forward collision avoidance system by following their best interpretation/understanding of the STPA guidelines as presented by Leveson (2012) and Leveson et al. (2012). Table 1 shows an excerpt of the identified inadequate control commands or events[1] that could lead to hazardous states.

No.	Command or Event	Not Provided	Provided Unsafe	Provided			Stopped Too Soon
				Too Early	Too Late	Out of Sequence	
1	**Vehicle Status Signal**	Catastrophic- (Wrong brake pressure determination) [1a]	Catastrophic- (Wrong brake pressure determination) [1a]	N/A	Catastrophic- (Wrong brake pressure determination and wrong reaction time) [1a]	N/A	N/A
2	**Object Status Signal**	Catastrophic- (Wrong brake pressure determination) [2a]	Catastrophic- (Wrong brake pressure determination) [2a]	N/A	Catastrophic- (Wrong brake pressure determination and wrong reaction time) [2a]	N/A	N/A

Table 1. Inadequate Control Commands/Events

During step 1 of STPA, 14 inadequate control commands or events were identified in the forward collision avoidance system. Then, these control commands or events were analyzed, one by one, to identify their associated hazards. An excerpt of the identified hazards is shown in Table 1 in order to display the type of information that was derived. In this study, it was found that if the identified control commands or events are *not provided* then the system leads to hazardous states, in most cases of catastrophic level. Similarly, if the identified control commands or events are *provided too late* then the system leads to, in most cases, hazardous states of catastrophic level. On the other hand, if the identified control commands or events are *provided too early* then the system does not lead to catastrophic hazardous states; three lead to moderate and one to negligible level hazards. Interestingly, similar to a previous study (Ishimatsu et al., 2010), only one of the *stopped too soon* control commands or events could lead to a hazardous state. One possible interpretation of this result could be that STPA should be further evaluated on systems that contain more operations that are not only triggers but

[1] http://serg.cs.lth.se/index.php?id=89239

require time for completion. We assume that both our system and the system presented by Ishimatsu et al. (2010) have a limited number of such cases. Therefore, assessing the sensitivity of the STPA method in identifying these potential hazards should be further explored.

From the 14 identified inadequate control commands or events, we identified 22 hazards. The hazards were classified in three severity levels, catastrophic, moderate and negligible. Over 70% (16) of all the hazards were classified as *catastrophic* with potentially fatal consequences. Only three hazards were classified as *moderate* severity level that may lead to severe accidents and have risk of serious injury. The remaining three hazards have *negligible* severity level. The *negligible* hazards do not have any serious consequences if the pertaining component fails alone and the other components of the system work properly. Therefore, it is possible to hypothesize that the STPA method efficiently supports risk analysts with limited domain experience (in our case maximum 5 years) in the identification of a complete set of catastrophic hazards.

Looking at two example hazards, i.e., 1a and 2a, identified in Table 1, we can notice that they are caused by inadequate control commands from the vehicle and object status signals. Hazard 1a is the incorrect brake pressure determination caused by missing vehicle status signal. Hazard 2a is the incorrect brake pressure determination caused by missing object status signal. Both hazards, 1a and 2a, are same but they have different causal factors. For example, the causal factors for the hazard 1a could be: i) Failure of vehicle sensor complex, ii) Malfunctioning of collision controller due to incomplete process model, iii) Communication failure or error (no signal), iv) Delayed communication (System will fail to provide active safety on time). The causal factors for the hazard 2a could be: i) Failure of Object detection, ii) Malfunctioning of collision controller due to incomplete process model, iii) Communication failure or error (no signal), iv) Delayed communication (System will fail to provide active safety on time). In this study the majority of the identified hazards and their causes correspond to the dynamic behavior of the studied system. We conclude that our results corroborate with the findings presented by Ishimatsu et al. (2010) and Pereira et al. (2006).

DISCUSSION

STPA worked well for the identification of hazards or risks in this study and we believe that the results could be an important input to an actual implementation of this type of system. Specifically, the initial phase (Step 1) of STPA is effective and it does not take too much time and effort. Our experiences show that persons with limited domain experience (maximum 5 years) required one week of effort (interrupted by other activities conducted in parallel) to perform the first step of the analysis and two weeks of interrupted effort (not full time) to perform the second step. In these effort estimates, we assume that the detailed functional diagram is already available. These findings also suggest that STPA is suitable for the situations when both domain expert and hazard analyst with limited experience have to complement and supervise each other that yields better results. However, we have noticed that the straightforward application of STPA on any safety-critical system (especially socio-technical) greatly depends on the availability of the control structure (structural and functional) diagram. Therefore, the quality of the results of applying STPA method is directly dependent on the quality of the control structure diagram and the amount of included system functional information.

In order to achieve the best possible outcome using STPA, the main focus should be put on step 1. Step 2 of the method is similar to the traditional hazard analysis methods i.e. FTA. At the same time, several causes of hazards associated with the dynamic behavior of the system were also identified during step 2. According to our experiences the main strength of STPA is that it covers the dynamic behavior of the system by finding component failures and communication failures. In this way STPA also takes into consideration component interactions in the system. To limit the scope of this study, further actions (deriving constrains and safety requirements) after identification of hazards and their causal factors were not performed.

To summarize, our results corroborate with previously reported positive experiences from STPA application in several domains, e.g., space (Ishimatsu et al., 2010), air traffic (Leveson et al., 2012), defense (Pereira et al., 2006), rail transportation (Thomas et al., 2011), and extend these positive outcomes by an example from the software-intensive automotive domain. This study presents our experiences about how the STPA method can be used to improve the safety in the development or operation of safety-critical systems. The goal of this study is not to present the existing risks of the forward collision avoidance system instead its focus is on the effectiveness and time efficiency of the STPA method.

CONCLUSIONS

This study presents the results of a hazard analysis performed using the STPA hazard analysis method on a safety-critical system; forward collision avoidance system. Based on the findings of this study STPA has proved to be an effective and efficient hazard analysis method for assessing the safety of a safety-critical system from the automotive domain. Using STPA we identified 14 inadequate control commands or events in the analyzed system with their associated hazards. We believe that the reason for the effectiveness of STPA is that it considers

and greatly focuses on the control commands or events and their feedbacks in step 1 instead of focusing on individual component failures. Regarding the effort required to apply STPA on a safety-critical system, based on the results found in this study, it can be concluded that STPA requires moderate effort in relation to the level of experience of the study participants. We believe that the effort efficiency of the use of STPA for hazard analysis allows domain experts and hazard analysts to complement each other.

However, there are some aspects to consider with the application guidelines (Leveson, 2012; Leveson et al., 2012) and there are some missing details about the deriving constrains and safety requirements as a further action after identification of hazards and their causal factors. These shortcomings can easily be mitigated by writing the detailed instructions or guidelines for STPA application. Our positive experiences with STPA suggest that performing both steps 1 and 2 in a group of both domain experts and risk analysts increase the discussion opportunities and lead to a more effective process and more in-depth results. We experienced that the identified risks and hazards had more technical depth and constituted a better view on the analyzed system safety. Future studies are planned to explore the effects of the application of STPA in groups with more domain experts and hazard analysts and to compare the results with other traditional hazard analysis methods, i.e., FTA and FMEA.

ACKNOWLEDGEMENT

This work was funded by the Swedish Civil Contingencies Agency under a grant for PRIVAD, Program for Risk and Vulnerability Analysis Development.

REFRENCES

1. Aljazzar, H., Fischer, M., Grunske, L., Kuntz, M., Leitner-Fischer, F. and Leue, S. (2009) Safety analysis of an airbag system using probabilistic FMEA and probabilistic counterexamples, *6:th International Conference on the Quantitative Evaluation of Systems (QEST)*, Hungary, pp. 299 – 308.
2. Bañuls, Vctor A. and Turoff, Murray (2011) Scenario construction via Delphi and cross-impact analysis, *Technological Forecasting and Social Change*, v 78, no 9, pp. 1579-1602.
3. Bond et al. (2003) Collision mitigation by braking system, *US Patent* 6607255B2.
4. Coelingh, E., Eidehall, A. and Bengtsson, M. (2010) Collision warning with full auto brake and pedestrian detection - a practical example of automatic emergency braking, in *proc. of the 13:th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 155–160.
5. Ericson, C. A. (1999) Fault Tree Analysis–A History, *in proc. of the 17:th Int. System Safety Conference*.
6. Gleirscher, M. (2013) Hazard analysis for technical systems, Software Quality: Increasing Value in Software and Systems Development, *5:th International Conference, SWQD*, v 133, p 104-124, Austria.
7. Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y. and Nakao, H. (2010) Modeling and hazard analysis using STPA, in *Proc. of the 4th IAASS Conference Making Safety Matter*, p.10.
8. Johannessen, P., Torner, F. and Torin, J. (2004) Actuator based hazard analysis for safety critical systems, *in Computer Safety, Reliability, and Security*, v 3219, pp. 130–141.
9. Leveson, N. G. (2012) Engineering a Safer World: Systems Thinking Applied to Safety, *The MIT Press*.
10. Leveson, N. G., Fleming, C. H., Spencer, M., Thomas, J. and Wilkinson, C. (2012) Safety assessment of complex, software-intensive systems, *SAE International Journal of Aerospace*, v 5, pp. 233-244.
11. McDermid, J., Nicholson, M., Pumfrey, D. J. and Fenelon, P. (1995) Experience with the application of HAZOP to computer-based systems, *in proc. of the 10:th Annual Conference on System Integrity, Software Safety and Process Security, COMPASS*, pp. 37–48.
12. McDermott, R., Mikulak, R. and Beauregard, M. (1996) The Basics of FMEA, 2nd Ed. *Taylor & Francis*.
13. Nakao, H., Katahira, M., Miyamoto, Y. and Leveson, N. (2011) Safety guided design of crew return vehicle in concept design phase using STAMP/STPA, *in Proc. of the 5:th IAASS Conference,* pp. 497-501.
14. Pereira, S. J., Lee, G. and Howard, J. (2006) A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System, *in Proc. of the AIAA Missile Sciences Conference*, Monterey, California.
15. Sulaman, S. M., Weyns, K. and Höst, M. (2013) A review of research on risk analysis methods for IT systems, *in Proc. of the 17:th International Conference on Evaluation and Assessment in Software Engineering*, Porto de Galinhas, Brazil, ACM, pp. 86–96.
16. Thomas, J. and Leveson, N. G. (2011) Performing Hazard Analysis on Complex, Software- and Human-Intensive Systems, *in Proc. of the 29:th ISSC Conference about System Safety*.
17. Tobioka, T. and Bertucio, R.C. (1981) Use of event tree analysis in development of a LOCA test program, *Transactions of the American Nuclear Society*, v 39, pp. 590-591.