Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain

Asim Abdulkhaleq, Stefan Wagner
Institute of Software Technology, University of Stuttgart, Germany
Email: {Asim.Abdulkhaleq}, {Stefan.Wagner}@informatik.uni-stuttgart.de

***Abstract*—Hazard analysis is one of the most important elements in developing safe-critical systems. STPA (Systems-Theoretic Process Analysis) is a modern technique based on the new accident causation model STAMP (System-Theoretic Accident Model and Process) for analyzing hazard and safety issues, which can be applied early in the design process of a system to achieve an acceptable risk level. We have applied STPA to a well-known example of safety-critical systems in the automotive industries: Adaptive Cruise Control (ACC). The results of the application of STPA to our case study and the limitations and difficulties of applying STPA are presented.**

I. Introduction

A safety critical system is a system, which can cause hazards for humans, significant property or the environment. Many safety-critical systems rely on software to achieve their functions. Software can create hazards through erroneous control of the system or by misleading the system operators into taking inappropriate actions [1]. A comprehensive hazard analysis of such systems is of vital importance, because dysfunctions can result in accidents. Safety critical-systems are increasingly used in the automotive industry to provide convenience and safety features to vehicle drivers and passengers, with increasing levels of automation and control authority [2]. Modern systems become more complex, that is leading to accidents in which no components failed (e.g. accidents which arise from unsafe and unintended interactions among the system components). New powerful models of accident causation and hazard analysis techniques are needed to address these new failure modes. STAMP and STPA are modern hazard analysis techniques that model and identify hazard and accident scenarios that are not address by the traditional hazard techniques [3].

Problem Statement: Recently, STAMP/STPA has been applied to different applications areas. As a rather new technique, it is not described in enough detail to be applied in all contexts in practices. Safety is one of the essential and vital aspects for the automotive domain, which relies on many safety-critical embedded control units. In the automotive domain, there is only little experience with STAMP/STPA.

Research Objectives: The overall objective of this research is to investigate the benefits and the potential problems of applying STAMP/STPA in industry to get an understanding of their effect and problems in the applications. In particular, we aim first to understand how these approaches can be useful for automotive safety, and second to provide an assessment of the usage of these approaches.

Contribution: We use STPA in a case study in the automotive domain to investigate the scenarios of accidents. The case study analyses the application of STPA and its difficulties for a real system in a commercial vehicle. The result is a set of causal factors and recommendation for the future design of the system.

Context: The research concentrates on applying STPA to the automotive domain and is performed based on published knowledge from a case study with MAN Truck & Bus AG [4].

Related Work: STAMP and STPA have been successfully applied to different systems in different areas such as Space Shuttle Operations [5], Railroad Safety in China [6] and Darlington Shutdown System [7]. In the automotive domain, a preliminary example to apply STPA in the automotive domain was by Hommes [8]. We applied STPA to the whole ACC system and provided the causal factors of each part of the system.

II. Study Design

Study Object: We applied the STPA hazard analysis technique to Adaptive Cruise Control (ACC). ACC is an automotive feature that allows a vehicle's cruise control system to adapt the vehicle's speed to the traffic environment. ACC uses a long range radar sensor which is attached to the front of the vehicle and detects a target vehicle up to 150 meters in front. The ACC system is able to automatically adjust the driving speed as well as the distance to the vehicle ahead in accordance with the pre-settings

Research Questions: This paper addresses two research questions: 1) How can STPA improve the safety in the automotive domain? and 2) What are potential problems of applying STPA to automotive safety? To address these questions, we conducted a case study of applying STPA to safety-critical automotive systems.

Data Collection and Analysis: STPA can be applicable to an existing design or be used before a design has been created. STPA uses the existing knowledge about the system, control diagrams, functional requirements, safety constraints and safety requirements as fundamentals to guide the analysis process. Thus, we started with a thorough investigation of the structure, existing information, documentation and safety cases

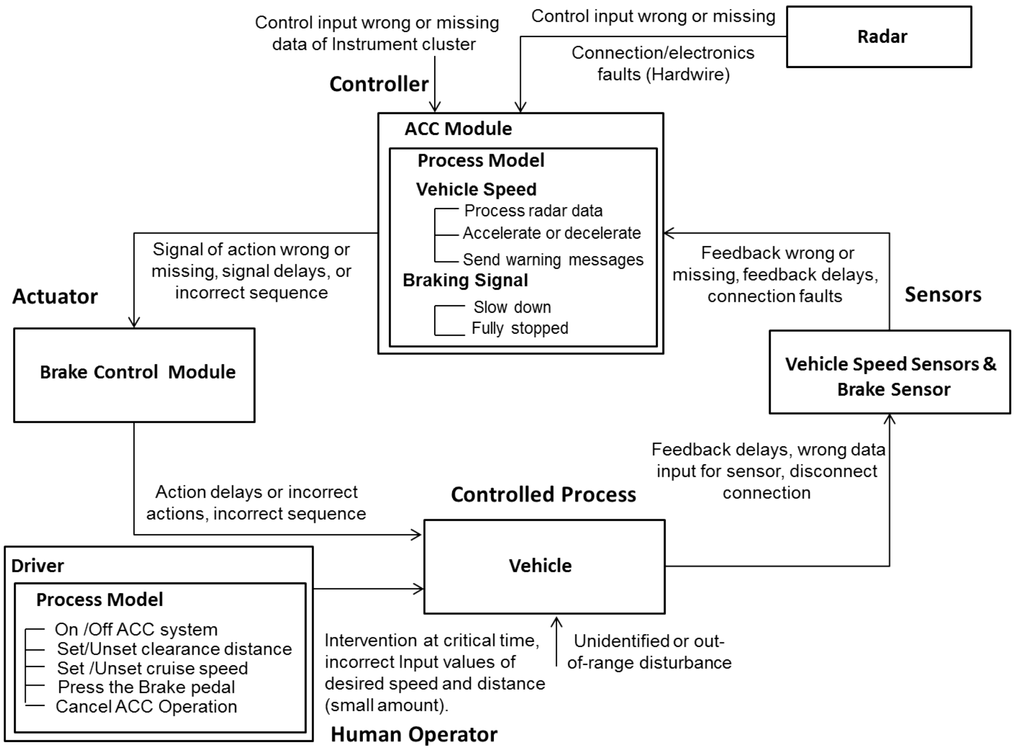
Control input wrong or missing data of Instrument cluster
Control input wrong or missing
Radar
Connection/electronics faults (Hardwire)
Controller
ACC Module
Process Model
Vehicle Speed
Process radar data
Accelerate or decelerate
Send warning messages
Braking Signal
Slow down
Fully stopped
Signal of action wrong or missing, signal delays, or incorrect sequence
Actuator
Brake Control Module
Feedback wrong or missing, feedback delays, connection faults
Sensors
Vehicle Speed Sensors & Brake Sensor
Feedback delays, wrong data input for sensor, disconnect connection
Action delays or incorrect actions, incorrect sequence
Controlled Process
Vehicle
Driver
Process Model
On /Off ACC system
Set/Unset clearance distance
Set /Unset cruise speed
Press the Brake pedal
Cancel ACC Operation
Intervention at critical time, incorrect Input values of desired speed and distance (small amount).
Unidentified or out-of-range disturbance
Human Operator

Fig. 1. The Process Model for ACC Module with Causal factors leading to hazards.

of the ACC system to get a full understanding about the study object and establish the fundamentals. The case study uses the three steps of STPA for identifying the potential hazard scenarios of the ACC system. The following describes the process of analysis in the case study:

1) Investigate the system structure, goals, components, requirements, functions and components interaction.
2) Elicit the system requirements, safety constraints.
3) Identify the potential accidents and unacceptable losses for the system, the system hazards at system level.
4) Draw the functional control diagram of the system.
5) Apply step 2 and step 3 of STPA to the control structure.
6) Refine the safety requirements and constraints.

III. Results

In this section, we present a part of our results:

1) **System Accidents:** The accidents to be considered are:
   - **Accident 1:** The ACC vehicle crashes with a vehicle in front when the ACC system is in active mode (Forward collision vehicle to vehicle).
   - **Accident 2:** The vehicle behind crashes the ACC vehicle when the ACC system detects an object in the ACC path (Backward collision vehicle to vehicle).
2) **System-Level Hazards:**
   - **H.1:** ACC violates the safe distance between ACC vehicle and vehicle in front.
   - **H.2:** ACC estimates wrong values of distance and speed of vehicle ahead.
3) **Safety-Control Structure Diagram:** Figure 1 shows the safety control structure diagram of the ACC module and the brake control module at the system level of the ACC system. The generic control loop is used to guide the analysis process.
4) **Safety-Control Actions:** An example of an safety control action is providing radar data which can be documented with four types of hazardous control actions:
   Not Given: Radar sensor does not provide the relative speed and distance of objects ahead of vehicle.
   Given Incorrectly: Radar sensor provides incorrect data of target vehicle speed.
   Wrong Timing or Order: The data of radar sensor comes too late when the distance to a forward vehicle is too close.
   Stopped too soon or applied too long: Radar sensor is stopped too soon that the ACC module does not get the relative data signal of target vehicle.
5) **Safety-Related Constraints:** Each unsafe control action is then translated into a component-level safety constraint (e.g. the radar sensor must detect the small objects which are in the path of the vehicle and send the data early to the ACC module).
6) **Causal Factors:** To create causal scenarios, the control structure (shown in figure 1) is first augmented with process models for each component. For example, con-

sider an unsafe hazardous control action: the braking is commended when there is no slowed or stopped object in the vehicle path. The analysis in this step shows that one potential cause of that action is an incorrect process model of ACC module which is may be due to failed radar sensor or the feedback of brake status or the feedback may be delayed or corrupted.

A. *Improvement potentials*

By applying STPA to our object study, we derived the following improvement potentials to the ACC system:

- The radar sensor in the front shall detect small objects (e.g. a motorcycle) or a vehicle driving far off center.
- An extra radar sensor should be added in the back of the vehicle to detect the speed and distance of vehicles behind.

B. *Problems*

According to our experience, the third step of STPA needs a lot of effort, time and deep knowledge for examining the controller with process models variables and assessing each path of the control loop to see if this path can lead to unsafe control actions. Moreover, STPA does not show or provide a systematic way on how to make these arguments, e.g. examine inadequate control algorithm, to help the analyst in this step. STPA needs a systematic method to notate the relation between the process model variables, control actions and hazards. We also found STPA has limitations for analyzing multiple controllers in the control loop of a system. For example, the ACC system has two controller modules: ACC module and Engine Control Module (ECM), which are connected together and used to control the vehicle speed. Both of them receive the vehicle speed information from the brake control module. ECM sends brake switch command to the ACC module and the ACC module sends the ACC state target speed to ECM. It is not clear how we can provide an action table and casual factors for multiple controllers with interference among the actions.

C. *Comparison*

We conducted a case study applying safety cases for the same ACC system [4]. In comparison, we found STPA to have a more systematic, step-by-step process, while safety cases provide clear means to structure the risk argumentation. STPA considers the safety of a system as a control problem, assumes worst-case scenarios and identifies potential scenarios that could lead to that worst case while the safety case presents the argument that shows the system under consideration is acceptably safe in a given operating context. The combination of STAMP and STPA is suited for an in-depth analysis of the complete systems and its internal control. It has no detailed description, however, how to present the final argumentation about the hazards avoided and remaining risks. Safety cases could fill this void, but they are not well suitable for the system analysis.

We also compare our case study with a preliminary example of applying STPA to ACC system which was presented by Hommes [8]. We extended her example by considering the two types of vehicle collisions which are related to the ACC system (e.g. forward collision and backward collision) and more hazards at the system level. Moreover, we considered the intervention between driver and ACC system. We also considered the application of STPA to a whole ACC system as comprehensive analysis and provided the potential causal factors for each part of control loop of ACC system. Finally, we provided recommendations for a further design of the system. The details will appear in the full version of the paper.

IV. Conclusion

We investigated the application of STAMP/STPA to automotive domain and its difficulties in that domain. In analyzing accidents and potential inadequate controls, we have found STPA to be a more powerful and useful technique that can be used to evaluate safety-critical systems in the automotive domain by identifying the potential accident scenarios that include the entire accident process, including design errors, software flaws, component interaction accidents and human decision-making errors contributing to accidents.

We aim as future work to integrate a state machine analysis with STPA to provide a suitable notation of arguments between the states of controller and control actions. Moreover, we plan to integrate our experience with safety/risk cases and examine additional potential benefits of STPA in the automotive domain.

References

[1] N. G. Leveson, “A systems-theoretic approach to safety in software-intensive systems,” *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 66–86, 2004.

[2] J. C. Knight, “Safety critical systems: challenges and directions,” in *Proceedings of the 24th International Conference on Software Engineering*, ser. ICSE ’02. New York, NY, USA: ACM, 2002, pp. 547–550.

[3] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, ser. Engineering Systems. MIT Press, 2011.

[4] S. Wagner, B. Schatz, S. Puchner, and P. Kock, “A case study on safety cases in the automotive domain: Modules, patterns, and models,” in *Proceedings of the 2010 IEEE 21st International Symposium on Software Reliability Engineering*, ser. ISSRE ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 269–278. [Online]. Available: http://dx.doi.org/10.1109/ISSRE.2010.31

[5] B. D. Owens, M. S. Herring, N. Dulac, N. G. Leveson, M. Ingham, and K. A. Weiss, “Application of a Safety-Driven Design Methodology to An Outer Planet Exploration Mission,” in *IEEE Aerospace Conference 2008, Big Sky, Montana*, Mar. 2008.

[6] A. Dong, “APPLICATION OF CAST AND STPA. TO RAILROAD SAFETY IN CHINA,” Master’s thesis, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, Vereinigte Staaten, USA, May, 2012.

[7] Y. Song, “Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis. Open Access Dissertations and Theses, Paper 6801,” Master’s thesis, McMaster University, Hamilton, ON L8S 4L8, Canada, April, 2012.

[8] Q. V. E. Hommes, “Applying STPA to Automative Adatpive Cruise Control System,” Master’s thesis, STAMP Workshop, MIT Building 32, Boston, USA, April, 2012.