Integrating State Machine Analysis with System-Theoretic Process Analysis

Asim Abdulkhaleq, Stefan Wagner

Institute of Software Technology
University of Stuttgart, Germany
asim.abdulkhaleq@informatik.uni-stuttgart.de
stefan.wagner@informatik.uni-stuttgart.de

Abstract: Safety becomes a critical aspect for software-intensive systems in different applications areas. Many hazard analysis techniques are proposed and used to investigate system design models to elicit hazards and design flaws. STPA (System-Theoretic Process Analysis) is a modern hazard analysis technique, which is based on a new systems-theoretic model of accidents for large and complex systems. With STPA, the system is viewed as interacting control loops and the accidents are considered as results from inadequate enforcement of safety constraints in design, development and operation. STPA still needs appropriate diagrammatic notations to represent the relation between the process model variables, control actions and hazards. For this purpose, we propose to integrate state machine analysis with STPA to provide a suitable notation of arguments between the states of controllers, control actions and hazards.

1 Introduction

A great challenge today in the development of software-intensive systems is how to develop a safe system that fulfills safety requirements and ensures safe functions of a system under all safety conditions. Thus, the safety analysis of a system needs to provide an understanding about the possibility of accidents occurring in the system. Safety analysis supports examining and investigating systems or subsystems to identify and classify each potential hazard according to its severity and likelihood of occurrences. It is also extremely important to prevent the hazards which can lead to injury and even loss of life. Increasing complexity and size of modern systems makes system safety a great challenge on how to design such system with acceptable level of risk.

A number of hazard analysis techniques have been proposed to perform system hazard analysis. Traditional hazard analysis techniques such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA)[Eri05] address only the failure of individual components and view the accidents as resulting from a chain or sequence of events. Instead, STPA analyses the complete system and addresses the component interaction failures and component failures as well. STPA is an efficient hazard analysis technique which has been developed by Leveson based on system theory [Lev12]. The main purpose of

STPA is to identify the new causal factors such as design errors, including software flaws, component interaction accidents, cognitively complex human decision-making error and social, organisational and management factors contributing to accidents that are not addressed by traditional hazard analysis techniques[Lev12, Tho12, Lev04].

Indeed, the hazard analysis techniques cannot describe well the dynamic behaviour and state transition of complex system. State machine models have emerged as one important modelling perspective on the reactive behaviour of complex systems. They represent the complete behaviour of the system using states and transitions and can easily define the constraints on transitions.

Problem Statement The safety analyst during STPA must augment the control structure with process models and examine the controller with process model variables to see if this process path can lead to unsafe control actions or not. STPA does not show, however, how to make these arguments.

Research Objectives The overall objective of this research is to fill this gap and find ways for including and better analysing the dynamic behaviour of systems during STPA hazard analysis. We plan to investigate various modelling and analysis techniques. In this paper, we focus on proposing the integration with state machine models.

Contribution For that, we integrated the state machine analysis with STPA to show how this formal modelling technique can be used to support the safety analysis practices carried out with STPA. The resultant methodology can assist safety analysts during STPA step three to investigate inadequate control actions and verify each path in the control loop with process state variables. Furthermore, we applied the proposed methodology to Anti-lock Braking System [Gmb07] to explore its advantages and limitations.

2 Background

2.1 STPA Hazard Analysis

STPA is a top down analysis approach that considers the dysfunctional interactions between software, hardware, operators, management and regulatory bodies. We summarise the main steps of STPA below [Lev12]:

1. **Step 1:** Establish the fundamentals of STPA before beginning the analysis by identifying system accidents or unacceptable loss events. Next, identify the hazards for the system and translate them into top-level system safety constraints. Next, draw a preliminary (high-level) safety control structure which depicts the components of the system and the paths of control and feedback.

2. **Step 2:** Use the control structure defined in step 1 as guide for investigating the analysis; identify the potentially unsafe control actions that could lead to a hazardous state. Then, refine system safety constraints according to these unsafe control actions. STPA uses control structure diagrams and system hazards to generate the system and component safety constraints and safety requirements.

3. **Step 3:** Determine how each potentially hazardous control action, which was identified in step 1, could occur. Next, identify the process models of the controllers. Finally, augment the control structure with process models for each control component and examine the paths of the control loop to see if they could cause unsafe control action. Recommendation for the system design should be developed for additional mitigations.

2.2 State Machine Analysis

Finite State Machines (FSM) are a formal model for describing the dynamic behaviour of a system by using states and state transitions. It shows how the input drives changes in the state of a system and how output is produced [NRJA11]. It consists of a set of input events, a set of states, an initial state and a set of transitions.

Finite state machines are known as event-driven models which have been widely used in different areas for representing discrete events of systems. They can be used to model both functional and dysfunctional behaviours of system. FSM can be used also to analyze the trace of the accidents and it takes the occurrence of system failure as trigger event where the accidents arose as the result of inadequate enforcement of constraints on system behaviour [FGZZ11, AP11]. Therefore, using the characteristics of the event driven state transition of FSM in the safety analysis can aid effectively in providing a way to notate and assess the process model paths of system and whether they lead to hazards.

3 Proposed Methodology

As stated in the previous section, STPA shows the system behaviour as a set of interconnected boxes that represent the sub-components of system model and their relations. STPA addresses component interaction failures and component failures. FSM can model the dynamic behaviour of components and complete systems and, hence, enable the assessment of both. According to our experience with STPA hazard analysis, we found that the integration between FSM and STPA could assist the safety analyst in identifying and evaluating dysfunctional behaviour of a system. The goal of analysing the behaviour of a system is to identify the hazardous control actions by considering the operating modes of the system and mitigating the catastrophic effects. Our proposed methodology (as shown in Figure 1) aims to:

- Use STPA to identify the potential for inadequate scenarios of the system that could

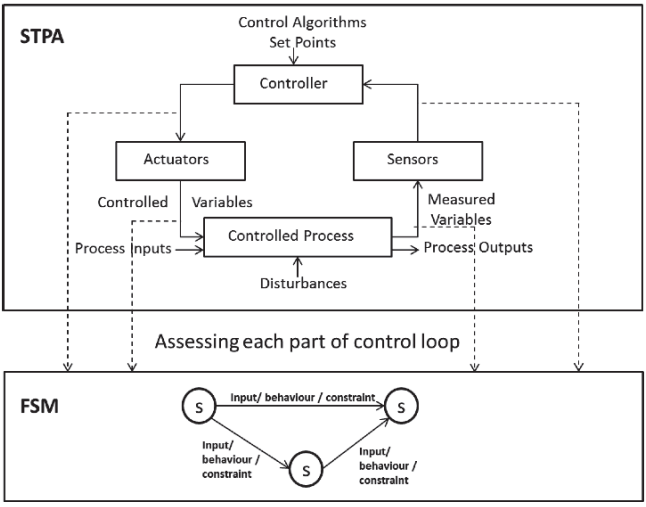

Figure 1: The integrating of FSM with STPA.

lead to a hazardous state.

- Identify the process model of each controller and identify its process state variables.
- Use FSM to model the dynamic behaviour of the controllers and show how the behaviour changes over the history of its inputs.
- Use FSM to model the safety constraints identified using STPA with states and state transitions of the system.
- Assess each part of the control loop of the system with FSM and analyse each part for identifying the hazardous control actions based on all the possible states, which have an effect on the control action.
- Extend the control action table, identified using STPA in step 2, to include the operating modes (system states) and its effect on the control action as additional columns.
- Refine the safety constraints and design decisions.

4 The Integration of FSM with STPA

An illustrative example is given here, which considers an Anti-lock Braking System (ABS) for modern automobile, to show the hazard analysis with STPA and how to integrate FSM with STPA. First, we applied STPA to ABS to identify unsafe control actions and causal factors. Then, driven by the STPA results, we mapped these results to an FSM. Finally, we refined the control action table and the safety constraints.

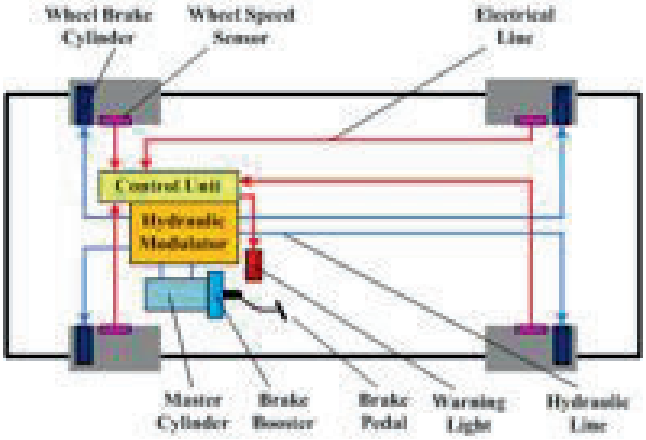

Figure 2: The ABS architecture [Cle12].

4.1 An Illustrative Example: Anti-Lock Braking System (ABS)

ABS is now becoming a standard in the automotive world and it assists the driver by preventing the wheels from completely locking during an emergency stop by applying the optimum braking pressure to the individual wheels, thus ensuring the vehicle can still be steered and shortening braking distances on slippery surfaces [Cle12, AZHS11, Gmb07].

Typical ABS components (as shown in Figure 2) include[Cle12, AZHS11]: *Electronic Control Unit (ECU)*, which acts as controller unit and receives information from the sensors, determines when a wheel is about to lockup and controls the hydraulic control unit;*Hydraulic Control Unit (HCU)*, which is also called hydraulic pump and controls the pressure in the brake lines of the vehicle; *Modulator valves*, which are presented in the brake line of each break and are controlled by the hydraulic control unit to regulate the pressure in the brake lines; and *Wheel speed sensors* (up to 4), which measure wheel-speed and transmit information to an electronic control unit.

4.2 Hazard Analysis of the ABS

In accordance with the proposed methodology, we start the hazard analysis process with STPA based on the high-level control structure model of the system. Our analysis focuses specifically on the hazards that arise due to the interaction between electronic control unit and hydraulic control unit. For example, the ECU reads signals from the electronic sensors which monitor wheel rotation. If a wheel's rate of rotation suddenly decreases, the ECU orders HCU to reduce the line of pressure to that wheel's brake. In the following, we will describe in details the STPA hazard analysis process and the integration of FSM with it:

Step 1: *The safety analyst must establish the following fundamentals:*

- **System Level Goals:**
  - **G.1:** Prevent wheel lockup during an emergency stop.
  - **G.2:** Provide controlled stopping by maintaining maximum tire to road friction.
  - **G.3:** Permit the driver to maintain steering while braking.
- **Accident:** The accident to be considered is the ABS vehicle crashes with a vehicle and the occupants are injured while ABS is involved (A.1).
- **System Level Hazards:**
  - **H.1:** Loss of steering control during braking operation (A.1).
  - **H.2:** ABS did not manipulate optimal wheel slip and stop in the shortest distance (A.1).
- **Safety Constraints:**
  - ABS must engage automatically when rapid deceleration are detected.
  - ABS must sense the motion of each wheel to detect a skid condition and be able to pulse the braking hundreds of times per second.
- **Design Constraints:**
  - ABS must be engaged after brake pedal is pressed.
  - ABS must prevent wheel lock-up in hard braking situations (e.g. when the speed of vehicle is over 15 mph) when lockup may occur.
- **Design Requirements:**
  - ABS shall stop the vehicle in the shortest distance.
  - ABS shall maintain the safe stop distance on loose road surface (e.g. snow-covered, gravel-roads, etc.).
- **Functional Control Structure:** Once the hazards to be evaluated have been reviewed, the safety analyst develops a control structure diagram of the system. Figure 3 shows the control structure diagram which depicts the interacting control loop between ECU and HCU in ABS system.

Step 2: *Identify potentially unsafe control actions*: Based on the control structure in Figure 3, we can identify the potentially unsafe control actions, which can lead to a hazardous state. A hazardous state is a state that violates the safety constraints that are defined for the system. Each control action should be analysed in four ways (shown in Table 1) to determine if it is hazardous as defined by the system-level hazards or not. For example, if we consider the situation that the brake pedal is pressed during an emergency stopping situation in which wheels lock up but the ABS does not engage. This situation can be considered as hazardous because it can lead to hazard H.1 in our example.

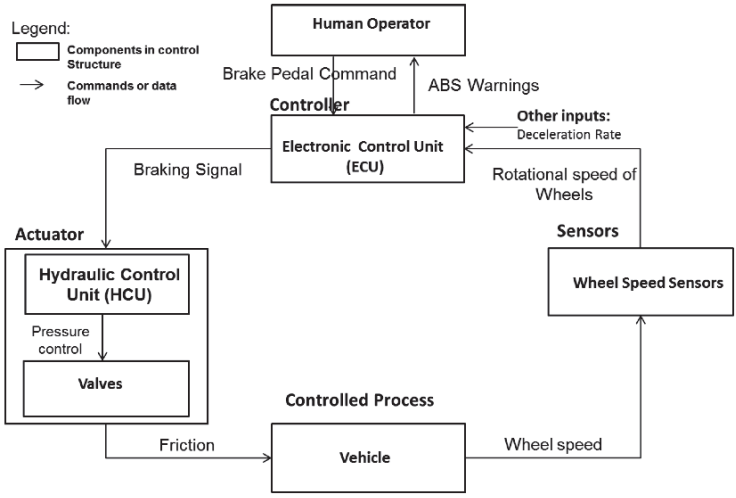

Figure 3: The control structure of ABS (ECU-HCU).

Step 3: *Causal factor analysis*: This step of STPA is first to augment the control structure (Figure 2) with process models and then to determine how hazardous control actions (Table 1) could occur. Figure 4 shows the process models for the ECU and human operator as an example. In this process model, the ECU senses the brake pedal's situation and receives the information about the wheel rotational speed from speed sensors. If it detects wheel locking, it reduces the braking force repeatedly until the wheel starts rotating again. Based on the process models developed, the next step is to identify the causal factors for the hazards. The causal analysis starts with each hazardous control action identified in Step 2 to determine how it could happen. In the control structure diagram of ABS, an unsafe behaviour can be resulted from either a missing or an inadequate constraint on the process or inadequate enforcement of the constraint that leads to its violation. As an example, consider the unsafe control action of not braking when the brake pedal is pressed. In this case, the hazard in the controller component could result if the information from the wheel sensors or the brake pedal command is not provided or is not implemented correctly or the process model is incorrect. Consequently, there are three cases which can be considered: 1) the brake pedal command is sent but not received by the ECU; 2) the ECU received the brake pedal command but it does not execute it. After the causal factor analysis is done, more details can be performed and 3) the brake pedal command is not sent to the ECU (component is defect).

4.3 FSM Construction

So far, there is no diagrammatic notation to represent the relation between the process model state variables (system states), control actions and safety constraints. Moreover,

Table 1: Examples of potentially inadequate control actions of the ABS system

Control Action	Not Given	Given Incorrectly	Wrong Timing or Order Cause Hazard	Stopped too soon or applied too long
Brake pedal command	Brake event applied but not received by ABS [see H.1]	Brake event is too short	Brake provided too late	Brake stopped too soon
Wheel speed sensors	Wheel speed data does not provide [see H.1, H.2]	Wrong current wheel speed provided [see H.1]	Current wheel speed updated too late [see H.1]	Wheel speed sensors stopped too soon [see H.2]

STPA does not include the operating modes of components, which will have an effect on the causal factors analysis and may determine the safety of the action or event. Therefore, FSM can be used to determine the system states that affect the safety of the control actions. In our example, the ECU controller has four operating modes: *inactive*, *handelLock*, *applyBrakePedal* and *reducePressure*. For the valve actuator component, there are three modes: *open*, *block* and *release* and for HCU actuator, there are three modes: *inactive*, *stopPump* and *openPump*. Next, we model the dynamic behaviour of the system by constructing a finite state machine which visualises the system states, control actions and safety constraints to support the safety analyst during STPA step three. Figure 5 shows the finite state machine of the controller in the ABS system. By using FSM, we are able to show the relations of potential combinations of relevant process state variables and according to these states we can identify the control action and determine whether issuing that control action leads to a hazardous state. As an example, if we consider the control action *brake pedal command* that can be a hazardous control action, it consists of the values of the following process model state variables: the brake pedal is pressed, the deceleration rate exceeds a preset maximum level, valve is close, wheel is locked and hydraulic pressure is reduced. Table 2 specifies the modified control action table for the brake pedal command based on our proposed methodology as an example.

Each row in the table 2 should be evaluated to determine whether it is hazardous as defined by the system-level hazards. We can notice that, there are some combinations which cannot be hazardous; therefore it should be neglected from the table. This process will continue to combine other potential states which are related to specified control action. Consequently, the safety constraints will be refined and documented.

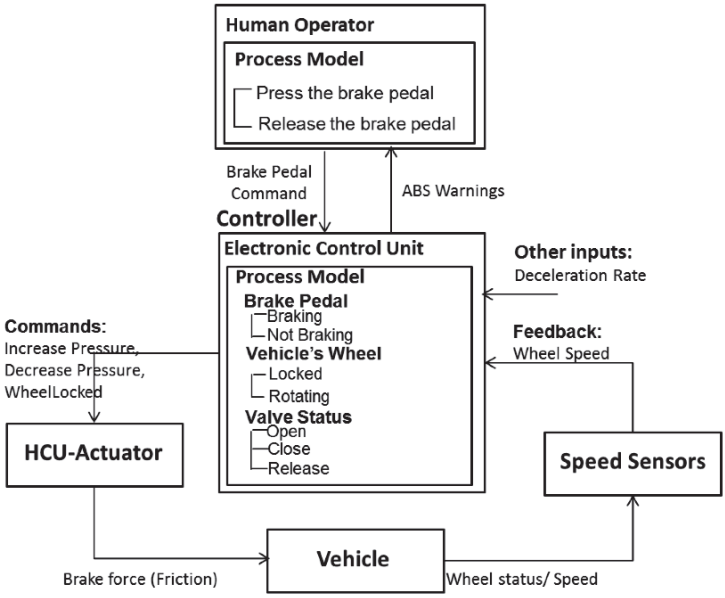

Figure 4: Control structure of the ABS with the process model of the electronic control unit

5 Discussion

To determine the usefulness of our proposed methodology to support safety analyst during STPA, we compared the results which are achieved by STPA (Table 1) with our results in Table 2. As we can see in Table 1, each control action has been analysed in four ways, which consider only the timing information of the control action (i.e. not given, too short, too late, too early, out of sequence-wrong timing). There is no systematic way to let the safety analyst know how to evaluate each control action and determine which can lead to a hazardous state and it is not clear how he or she can perform it. That means the safety analyst's professional knowledge and experience play a critical role in this step to evaluate the control actions. In most cases, the control actions in the control loop can depend on a number of relevant factors such as system states, human behaviour and environment conditions which have effects on determining the safety of the control action. Therefore, it is important to have a modelling method that allows considering all relevant factors. The FSM can visualise the actual behaviour of the system and can be used to examine the hazardous behaviour. We used FSM to examine each control action in the loop to detect hazardous situations based on the potential combinations of system states that are relevant. It is important to note that we do not consider the human behaviour and environment conditions (e.g. road surface) in our example, we only consider the system operating modes (states) that are relevant to control actions.

Many systems may exhibit behaviour much more complex. Thereby, in the evaluation process of control actions, it will be hard to determine unsafe control actions and it may

Table 2: The control action table for the *brake pedal command* based on the potential combination of system states

Control Action	Wheel Status	Wheel Speed	Valve Status	Hazardous?
Brake pedal command	Locked	slow	open	Yes
Brake pedal command	Locked	fast	open	Yes
Brake pedal command	Locked	slow	close	No
Brake pedal command	Locked	fast	close	No
Brake pedal command	rotating	slow	open	Yes
Brake pedal command	rotating	fast	open	Yes
Brake pedal command	rotating	slow	close	No
Brake pedal command	rotating	fast	close	No

take more time and effort. Moreover, the control loop of the system may have one or more controllers which control one process. Therefore, it is possible to find the different kind of control actions in the control loop such as conflict control actions or overload control actions or dependent control actions. In this case, the safety of such control actions will rely on the multiple controllers' behaviours. We found STPA does not provide a description on how to detect the hazardous situations among multiple controllers.

Consequently, the benefits which can be gained by integrating FSM during STPA are, first to model the complex system behaviour. Even though FSM of complex system will become more complex, it provides an understandable notation of dynamic behaviour and states of complex systems. A second benefit is to prove the consistency, correctness and completeness of the STPA analysis based on FSM by using model checking [EK00, DAC99, TS03]. Model checking is an efficient verification technique for models expressed as finite state machines. Model checking can help the safety analyst to automatically check if the FSM of system has the desired properties. We believe that model checking can be helpful in evaluating control actions based on our proposed methodology.

According to our proposed methodology, the safety analyst have to determine the possibilities combinations of states which are related to the control action and investigate how the system behaves in presence of different types of hazardous control actions. For this purpose, the safety analyst will use FSM to determine these relevant combinations. In fact, formal methods, such as FSM, are accepted best, if verification can be automated. Model checkers can do this for the finite state machines. For these reasons, we plan as future work to use model checkers in our proposed methodology for proving the corresponding correctness properties of finite-state machines and use existing commercial modelling tool such as Simulink [DH04] for simulating and analysing multidomain dynamic systems. Finally, in this paper, we identified important research challenges that need to be resolved to

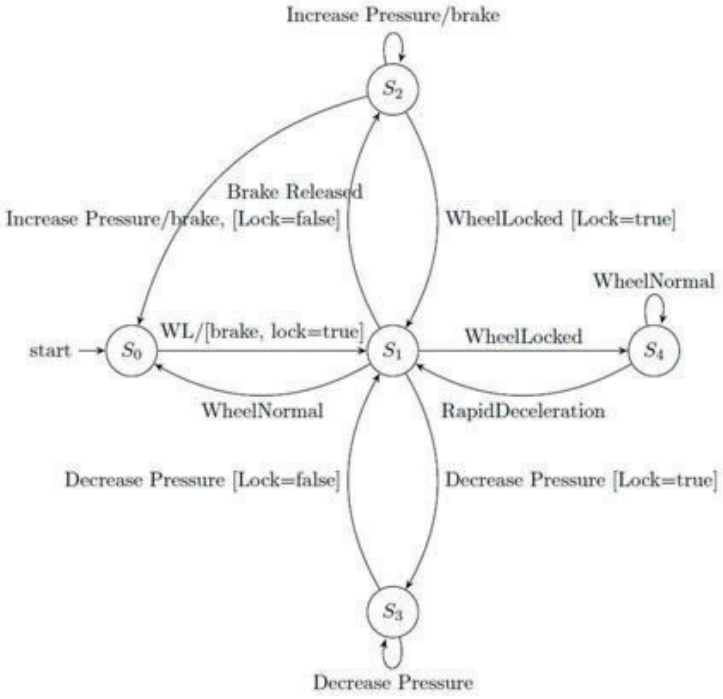

Figure 5: Finite state machine of ECU controller in the ABS system.
Where: *S0 = inactive (brake not pressed), S1=handellock, S2= applyBreakPedal, S3= pressureReduction, S4= MonitorDeceleration and WL= WheelLocked.*

make the hazard analysis with STPA practical.

6 Related Work

There a large body of existing work about integrating formal methods with hazard analysis techniques. Here we discuss some of the most closely related methodologies and tools which are used.

Thomas [Tho12] presents a formal mathematical structure underlying STPA and describes a procedure for systematically performing an STPA analysis based on the formal structure. He also presents a method for using the result of the hazard analysis to generate formal safety-critical, model-based system and software requirements. He points out that he is working on exploring potential ways in which similar kinds of detailed procedures can be created to assist the safety analyst during STPA step two.

Ariss et al. [EAXW11], present an approach for integrating fault-tree-based safety analysis

into statechart-based functional modelling. Their resultant model from the integration shows how the system behaves when a failure condition occurs and acts as the basis model to ensure safety through requirements validations.

The work of Fan et al. [FGZZ11] is closely related to the topic of safety analysis for complex systems based on the finite state machine theory. They introduced a formal modelling method based on finite state machines and proposed a safety analysis and assessment method of complex system based formal model. They did not show how to use finite state machine with any hazard analysis techniques.

Using formal methods during safety analysis would be a useful way in which the dynamic behaviour of complex system is presented. Therefore, our proposed solution aims to integrate FSM during the third step of STPA to visualise the relations between system states and control actions identified by STPA to help a safety analyst to examine the control actions based on system states whether it can lead to hazardous state.

More past work has been a large amount of work in the integration of FSM with traditional hazards analysis techniques such as FTA and FMEA which address only the component failure. Our proposed methodology is based on STPA which creates a set of scenarios that can lead to a hazard, is the same as FTA but STPA includes a set of potential scenarios in which no failures occur but the problems arise due to unsafe and unintended interactions among the system components.

7 Conclusion

In this paper, a solution is proposed to assist in evaluating the control actions identified during STPA step two based on the system states using formal method. We integrated state machine analysis with STPA to provide a suitable notation of arguments between states of system and control actions. The proposed solution uses the result of STPA to notate the relations between system states and control actions. We selected the anti-lock braking system as an illustrative example. By applying STPA to ABS, we determined the control actions, process model and state variables of our example. Next, we constructed an FSM of the controller with state variables and examined each potentially hazardous control action by examining each potential combination of relevant system states. These combinations are related to the system-level hazards identified by STPA step one. Finally, the control action table as well as safety constraints are refined and updated. The scalability of our methodology largely depends on the scalability of STPA and finite state machine. STPA has been successfully applied to different systems with a wide range of complexity in different areas such as Space Shuttle Operations [OHD+08] and the Darlington Shutdown System [Son12]. The finite state machines also have been widely used in different areas for representing the dynamic behaviour of systems.

7.1 Limitations

There are two main limitations of our methodology. The first is getting an appropriate finite state machine of real system. We have constructed the finite state machine of our example from various published sources. The second is a larger number of states of complex system that may forces the safety analyst to devote much of his effort and time to construct the potential combinations of relevant states to control action.

7.2 Future work

As future work, we aim to extend the scope and depth of analysis with the proposed methodology and try to identify systematic procedures for it. Future work is needed to further refine this method by applying it to other cases. Therefore, we aim to apply this methodology to both adaptive cruise control and anti-lock braking system which work together in a vehicle and investigate their interactions, control actions and causal factors as a single study object. In addition, we will work on comprehensive tool support which will be the starting point for the proposed methodology to be automated. Furthermore, we also aim to investigate applicability of STPA to security problems to identify and mitigate the threats that could emerge in systems.

References

[AP11] V.S. Alagar and K. Periyasamy. *Specification of Software Systems*. Texts in Computer Science. Springer, 2011.

[AZHS11] A. A. Aly, E. Zeidan, A. Hamed, and F. Salem. An Antilock-Braking Systems (ABS) Control: A Technical Review, Intelligent Control and Automation. In *An Antilock-Braking Systems (ABS) Control: A Technical Review, Intelligent Control and Automation*. Intelligent Control and Automation, August 2011.

[Cle12] Anti-lock Braking Systems. The Clemson University Vehicular Electronics Laboratory, 2012.

[DAC99] Matthew B. Dwyer, George S. Avrunin, and James C. Corbett. Patterns in property specifications for finite-state verification. In *Proceedings of the 21st international conference on Software engineering*, ICSE '99, pages 411–420, New York, NY, USA, 1999. ACM.

[DH04] J. Dabney and T.L. Harman. *Mastering Simulink*. Pearson/Prentice Hall, 2004.

[EAXW11] O. El Ariss, Dianxiang Xu, and W.E. Wong. Integrating Safety Analysis With Functional Modeling. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 41(4):610 –624, july 2011.

[EK00] G. Eleftherakis and P. Kefalas. Towards Model Checking of Finite State Machines Extended with Memory through Refinement. In *Towards Model Checking of Finite State Machines Extended with Memory through Refinement*. Springer-Verlag, 2000.

[Eri05] Clifton A. Ericson. *Hazard Analysis Techniques for System Safety*. Wiley, 2005.

[FGZZ11] Yichen Fan, Qi Gong, Jianguo Zhang, and Yuanzhen Zhu. Safety analysis for complex system based on the finite state machine theory. In *Reliability, Maintainability and Safety (ICRMS), 2011 9th International Conference on*, pages 594 –598, june 2011.

[Gmb07] Robert Bosch Gmbh. *Bosch Automotive Handbook*. Bosch Handbooks series. Bentley Pub, 2007.

[Lev04] Nancy G. Leveson. A Systems-Theoretic Approach to Safety in Software-Intensive Systems. *IEEE Transactions on Dependable and Secure Computing*, 1(1):66–86, 2004.

[Lev12] N.G. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety*. Engineering Systems. Mit Press, 2012.

[NRJA11] P.D. Nrusingh, D. Ranjan, C. Jayakar, and H. Arindam. Event Driven Programming for Embedded Systems- A Finite State Machine Based Approach. In *Event Driven Programming for Embedded Systems- A Finite State Machine Based Approach*. In: Proc. 6th International Conference on Systems, 2011.

[OHD+08] B.D. Owens, M.S. Herring, N. Dulac, N.G. Leveson, M.D. Ingham, and K.A. Weiss. Application of a Safety-Driven Design Methodology to an Outer Planet Exploration Mission. In *Aerospace Conference, 2008 IEEE*, pages 1 –24, march 2008.

[Son12] Y. Song. Applying System-Theoretic Accident Model and Process (STAMP) to Hazard Analysis. In *Applying System-Theoretic Accident Model and Process (STAMP) to Hazard Analysis*. McMaster University, 2012.

[Tho12] J. Thomas. Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis. In *Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis*. SAND2012-4080,Sandia National Labroratories., 2012.

[TS03] A. Thums and G. Schellhorn. Model checking FTA. In *FME 2003: Formal Methods, LNCS 2805*, pages 739–757. Springer-Verlag, 2003.