Using State Transition Diagrams for Safety Quantification within the Automotive Industry

Stefan Kaalen, Mattias Nyberg, Olle Mattsson

Using State Transition Diagrams for Safety Quantification within the Automotive Industry

1st Stefan Kaalen
Dept. of machine design
Royal institute of technology (KTH)
Stockholm, Sweden
kaalen@kth.se, 0000-0001-7972-8843

2nd Mattias Nyberg
Dept. of machine design
Royal institute of technology (KTH)
Stockholm, Sweden
matny@kth.se

3rd Olle Mattsson
Dept. of System Safety Architecture
Scania CV AB
Stockholm, Sweden
olle.mattsson@scania.se

***Abstract*—One method suggested in functional safety standards for quantitative analysis of systems is Markov processes of which Semi-Markov processes (SMPs) is an extension allowing more accurate models of the systems of interest. The paper suggests state transition diagrams modeled in Stateflow for modeling systems as SMPs since it will ease the adoption of the method in the automotive industry. Compared to the method of fault trees, which is frequently applied in industry today, SMPs have a significant advantage for some systems given their ability to explicitly model time-dependent aspects of the system. SMP-tool is suggested as a tool support for quantitative analysis of state transition diagrams modeled in Stateflow.**

I. Introduction

This paper argues for a *state-diagram* approach based on *stochastic processes* for safety quantification of safety-critical systems containing timed aspects. This method is for certain situations preferable to *Fault Tree Analysis* (FTA), which is probably the most widely used approach in the industry today. Although the discussion is focused on safety, the results are applicable to quantification of any critical property, such as other dependability attributes.

In the automotive industry, systems are growing more and more safety-critical and complex, a transformation that increases even further with the development of autonomous vehicles. Therefore, performing quantitative safety analysis of safety-critical systems is more important than ever [1], [2]. In these systems, proving the highest levels of safety through pure testing becomes unfeasible given the high amount of testing that would be needed. Furthermore, without an extensive pre-analysis, unacceptable numbers of system failure can occur during the road testing endangering human lives in the process. The alternative to testing is to estimate the level of safety using some type of model of the system.

Several different methods for performing model-based quantitative analysis are suggested in the functional safety standard ISO26262 and its mother standard IEC61508 [1], [2]: fault trees, Markov processes, reliability block diagrams, and Petri nets. Of the four methods, Markov processes and Petri nets are the most feasible to incorporate timed aspects [10] which are often present in complex safety-critical systems and these will therefore be investigated further below. However, though standard fault trees lacks support for explicit modeling of important timed aspects [8], they are often used in the industry today.

The probably most well-known method for modeling timed probabilistic properties is Markov processes, which is also the only one mentioned in ISO26262 [2]. While Markov processes allow for easy computation, they can often not accurately describe real-world systems. The main reason for this is that they lack explicit modeling of non-exponential times until events occur. Semi-Markov Processes (SMPs) generalize Markov processes to allow non-exponential times, and consequently enable more accurate descriptions of real-world systems. The present paper therefore argues for the use of models of semi-Markov processes, in favor of models of Markov processes, in order to capture the underlying system more accurately.

Petri nets [4] with probabilistic delays of transitions (here referred to as stochastic Petri nets) is a more general and powerful modeling formalism than Markov processes. Their quantitative analysis is performed on the underlying stochastic processes and can thereby be seen as a method of visualizing stochastic processes such as Markov processes or SMPs. However, while stochastic Petri nets have been around for a long time, they have still not received any major spread in the automotive industry, perhaps since they are experienced as too intricate. The present paper therefore argues for the use of *state transition diagrams* for the modeling of stochastic processes. The argument for this is that state transition diagrams, in tools such as Simulink Stateflow, are already widely used in the industry.

To summarize, the industry is in need of a powerful modeling formalism to support model-based safety analysis. It is also important that this formalism is easy to use and understand. A way of achieving this would be to base the modeling formalism on methods and tools already widely spread in the industry, such as state transition diagrams and Stateflow. However, an issue is that Stateflow lacks support for explicit analysis of models with probabilistic aspects. While the analysis phase is problematic, probability can be easily incorporated in the modeling phase in Stateflow as will be seen later. In order to aid the industry in analysing these models,

The authors acknowledge the following agencies and projects for general and financial support: the European H2020 - ECSEL PRYSTINE project and Vinnova FFI, through the AVerT project, and the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by Knut and Alice Wallenberg Foundation.

the present paper proposes *SMP-tool* [5], [6] which can be downloaded for free from [9]. SMP-tool is a tool support for modeling state transition diagrams of SMPs in Stateflow and performing quantitative analysis, such as computing the reliability of the models. Through SMP-tools numerical engine the large computation time that can occur using Monte-Carlo simulation is avoided.

The outline of the paper is as follows: In Sec. 2, SMP-tool is presented. Then, in Sec. 3, a simple redundant steering system is presented and modeled with state transition diagrams of SMPs. it is also analyzed using SMP-tool to highlight the advantages of SMPs over other techniques such as fault trees and Markov processes. Finally, in Sec. 4, it is discussed how state transition diagrams of SMPs can be used in practise.

II. SMP-TOOL

SMP-tool has previously been presented in [5] and [6] as a tool for performing steady-state, transient, and sensitivity analyses of SMPs modeled as state transition diagrams. There is support for these analyses as long as all transitions have a time to occurrence belonging to the class of expolynomial distributions, containing the exponential, degenerate, and uniform distribution. Furthermore, in SMP-tool 2.0, support for analysis of hierarchical-SMPs has been added.

Stateflow, within Matlab and more specifically the Simulink product family, provides a graphical language for state transition diagrams and is widely used within the automotive industry. Based on this, the tool support given by SMP-tool is based on models specified in Stateflow. However, in order to include all stochastic behaviour of SMP-models, the models used by SMP-tool do, while they are specified in Stateflow, differ in some aspects from the models that can be analyzed directly in Stateflow. The main user interface for creating models for SMP-tool is the standard modeling Stateflow GUI shown in Fig. 3. The main user interface in SMP-tool for the analysis of models is illustrated in Fig. 1. By simply opening a model to be analyzed, or creating a new model through the "file"-menu, a transient analysis can be performed for any specified time by simply pressing the button "Run transient analysis".

III. CASE STUDY

In this section, a simple redundant steering system, which is based on a real system from the heavy vehicle manufacturer Scania, will be presented. This will be followed by an attempt to analyze the system utilizing both fault trees, Markov processes and SMPs.

A. Redundant steering system

In the redundant steering system considered, the steering can be performed by either a Primary System (PS) or a Secondary System (SS) that takes over in the event of a system failure in the primary system. The two systems both have an exponentially distributed time to failure with a failure rate of λ_{PS} and λ_{SS} respectively. Furthermore, each of the subsystems have diagnostic procedures in place to detect a system failure; a system failure in PS is detected with the probability (has a diagnostic coverage of) DC_{PS} and a system failure in the SS is detected with the probability DC_{SS}. It is assumed that the vehicle undergoes a maintenance every 30 days. If a failure in any of the subsystems has been detected, the subsystem will be repaired during the maintenance. The case study has been somewhat simplified with assumptions to fit the paper format. The assumptions does for example include that the driver will not actively take the vehicle to the workshop any sooner than planned if there is a system failure in either PS or SS. In order to build quantitative models, some assumptions on the system are made. Firstly, it is assumed that everything works initially in the lifetime of the system. Secondly, it is assumed that $\lambda_{PS} = \lambda_{SS} = 10^{-6}$ and that $DC_{PS} = DC_{SS} = 0.99$.

B. Fault tree

Fig. 2 visualizes one of several possible attempts to model the redundant steering system with a fault tree. In the fault tree, the events EV1 and EV10 have an event probability that is compensated by the repair of the corresponding subsystem. The model has been built in Isograph Reliability Workbench.

C. Semi-Markov Process

The same system will now be modeled as an SMP with a state transition diagram. The result is visualized in Fig. 3. The first stage in building a state transition diagram of an SMP through SMP-tool is to identify the states the system can be in. The states should be chosen so that the system is always in exactly one of the states. This concept of states is corresponding to the built-in standard states in Stateflow and the six states chosen for creating the model of the redundant steering system are visualized in Fig. 3.

The next step is to add the transitions that can occur between states. When a state, i, is entered, assume that for each event that will cause a transition from state i to some other state, a timer is started. Connected to each of these timers is a Cumulative Distribution Function (CDF) that, by drawing a sample, provides the time the timer starts counting down from. Each of these timers start counting down in the same pace when state i is entered and when the first one reaches zero, the corresponding state transition occurs. Furthermore, each transition t may have several possible target states, each possible target state j is assigned a probability that a transition t will lead to the next state being state j. For each transition, these probabilities should add up to 1. To model this, the transitions, modeled by the default transitions of Stateflow, may have a Stateflow junction as target from which several default transitions origins, one for each possible target state. Each default transition with a state as origin is labelled with the CDF of the corresponding timer, while each default transition with a junction as origin is labelled by the probability that the corresponding target state will be the outcome of a transition through the junction. For the redundant steering, junctions are utilized to model the diagnostic coverage.

The last things to add to the model is which state(s) should be considered as *down state(s)* (states corresponding to system failure), and what probability each state have of being the first

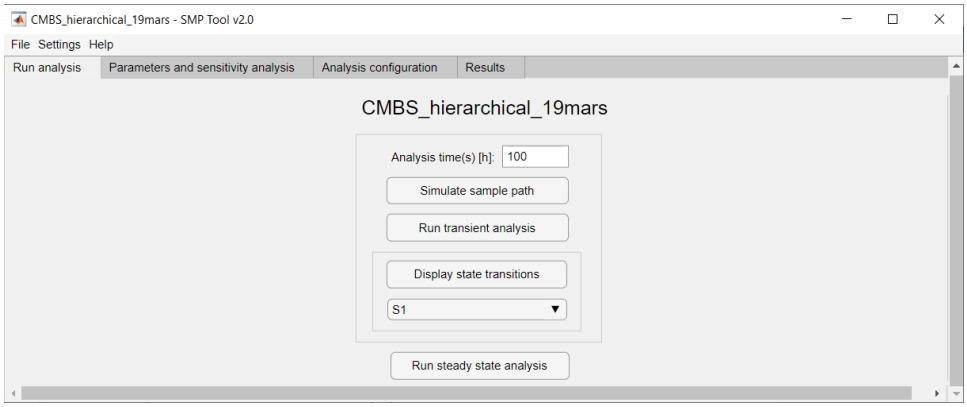

Fig. 1. Main user interface of SMP-tool.

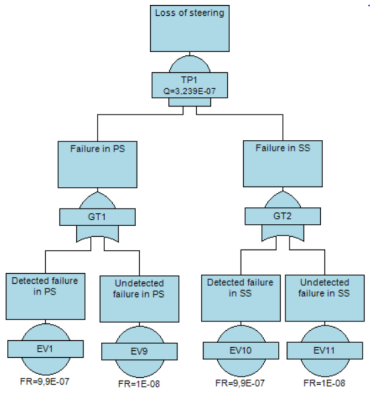

Fig. 2. Attempted fault tree breakdown of redundant steering

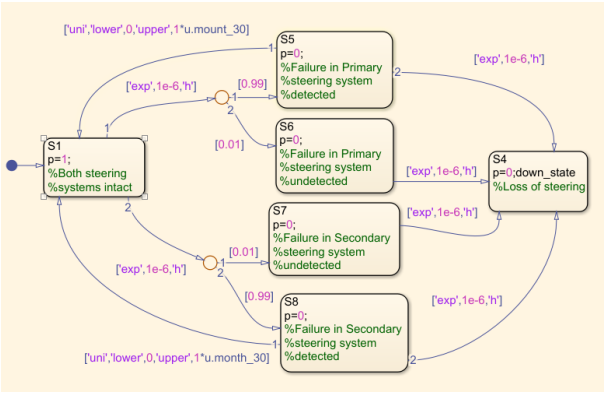

Fig. 3. State transition diagram modeled in Stateflow of the redundant steering system.

state of the process. To make a state a down state, simply mark the state with "down_state". To assign a probability, s, that a state i is the initial state of the process, simply mark the state with "p=s;". Fig. 3 illustrate a resulting state transition diagram after modeling the redundant steering system as an SMP.

D. Markov process

Trying to model the same system with continuous-time Markov processes, it can be seen in Fig. 3 that issues arise when trying to describe the transitions corresponding to repairing a failed subsystem since they are most realistically modeled as non-exponential. Markov processes only allow for exponential distributions of the timers for each transition in the model. While attempts can be made to approximate non-exponential distributions as exponential distributions, the accuracy of the results differ highly on the system being studied and it is a difficult task to estimate how much the approximation affects the overall accuracy of the results.

E. Comparison of SMPs and fault trees

The modeling of the redundant steering system will here be compared between the proposed method of SMP-based state-transition diagrams and fault trees. For the redundant steering system, a failure of the secondary system must occur while a failure in the primary system is active, or vice versa, in order to cause an overall system failure. Given the presence of the diagnosis and possible repair of each of the subsystems, no fault tree based on the standard fault tree formalism could be found that completely capture the behavior of the model. In order to approximately compensate the event probabilities for the repair time in the fault tree analysis, the repair time is assumed to be exponential [7] (with the same mean as the original uniform distribution). In comparison, an SMP describing the model could easily be found modeled as a state transition diagram without approximations in Fig. 3. Estimating the effect of approximations, made in the modeling, on the analysis result is generally an intricate task. On the redundant steering case study with the parameters chosen as described earlier in this section, the unreliability was by the fault tree analysis found to be $5.1 \cdot 10^{-5}$ while it by SMP-tool was found to be $3.1 \cdot 10^{-5}$. A Monte-Carlo simulation of the system found the real value to have a 95% confidence interval of $[2.8 \cdot 10^{-5}, 3.6 \cdot 10^{-5}]$. This together with the result of analysing the fault tree result clearly indicates that the limited support of explicit modeling of timed aspects in fault trees leads to an analysis result that differs from the correct value. For this particular case, the result of the fault tree analysis still ended up in the same magnitude as the real value and could therefore be deemed acceptable. However, it is difficult to in advance estimate the impact that approximations in models will have on the result of analyses, and thereby difficult to verify models.

What is actually visualised in the model is also an important aspect. In the fault tree model, the dynamical course of events is not clear. The state transition diagram however needed only a few states and transitions to completely visualize the dynamics of the redundant steering system in a model that is still is easy to overlook and understand.

It should be noted that there are extensions of standard fault trees such as dynamic fault trees [10], which are better equipped for handling e.g. timed aspects of the systems. However, as the modeling possibilities increase the number of possible gates, the complexity of building a model of your system increases with it, which in the end increases the probability of creating an erroneous model. Furthermore, while the extensions are many, they are yet too see any wide spread in the automotive industry.

IV. Using state transition diagram modeling in safety engineering

It is possible to, through the use of SMPs modeled as state transition diagrams, find different configurations of subsystems that assures that the system satisfies a needed level of reliability. This way, the configuration that shows most promise from e.g. an economical or technological standpoint can be chosen for the system. Finding possible configurations is done by assigning different values of the CDF for each timer and the probabilities from each junction in the model. This way, different configurations satisfying the same level of reliability can be found. As an example: consider that the maximal allowed probability of loosing steering within the lifetime of the vehicle is $3.2 \cdot 10^{-5}$. One way of designing the systems and diagnosis procedure is as illustrated in Fig. 3: to have $\lambda_{PS} = \lambda_{SS} = 10^{-6}$ and $DC_{PS} = DC_{SS} = 0.99$. Another idea could be to instead make the secondary system have a higher failure rate, while the primary system has a lower failure rate or vice verse. It is also possible to look at how changing the proportion of failures that is caught by the diagnosis procedure, or the maintenance, affects the needed failure rate of each subsystem.

In order to assist in finding these configurations, SMP-tool has a built-in *sensitivity analysis* that can be utilized not only to find suitable configurations, but also to find possible aspects of the system that has low impact of the overall safety. This way the company can both save money and focus the workload on where it is most useful.

A question that often arises when looking at a state transition diagram of an SMP is: how can the probability distributions in the model be found? Four answers to this question will be presented here. Firstly, while the shape of some transitions may be given directly out of the context, such as the uniform transition in the redundant steering system, others that are found in the sensitivity analysis can be seen as requirements of the subsystems or components in order to satisfy a level of safety. For example, the failure rates of the primary and secondary steering systems in Fig. 3 can be considered to be requirements to be given to the suppliers delivering these subsystems. Secondly, the sensitivity analysis may show that the distribution of some timers barely affect the safety of the vehicle. The distributions of these timers can therefore be set almost arbitrarily. Thirdly, the probability distributions can be found through testing. By performing tests on components and subsystems, the number of test hours can often be made significantly lower than if tests are done on the whole system. Finally, in safety engineering, some assumptions are always made on the behaviour of the system. These assumptions are often conservative estimates, which can be fairly easy to find.

To avoid the problem of state-space explosion, models can be built on different abstraction levels of the vehicle and analyzed in isolation. An example from the case study could be to make two more detailed separate models describing the internal reliability of the primary and secondary steering systems respectively. This reliability can then be used as failure distributions in the model on the higher abstraction level.

V. Conclusion

When modeling systems with timed aspects, as is often the case with real-world embedded systems for automotive vehicles, modeling and analysis are easily performed through SMPs modeled as state transition diagrams. Unlike fault trees, which are often used in the industry, state transition diagrams with underlying SMPs have general support for explicit modeling of timed aspects of the systems of interest. SMPs should therefore be preferable over fault trees for modeling complex systems where timed aspects often occurs, an importance that will only grow with the development of autonomous vehicles

To make the industry adapt the methods, it is suggested to model the state transition diagrams in Simulink Stateflow, which is already used widely in the automotive industry. SMP-tool was presented to compute the reliability for a SMP modeled as a state transition diagram in Stateflow.

The paper has focused on safety, yet the result are equally valid for other dependability attributes.

References

[1] IEC: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (IEC61508), 2010.

[2] ISO, Road vehicles - functional safety (ISO26262), 2018.

[3] Kulkarni, V.G.: Modeling and analysis of stochastic systems. 3rd ed., Taylor & Francis Group, LLC. (2017).

[4] Trivedi, K.S., Bobbio, A.: Reliability and availability engineering: modeling, analysis, and applications, Cambridge university press (2017).

[5] Kaalen, S., Nyberg M., and Bondesson, C.: Tool-Supported Dependability Analysis of Semi-Markov Processes with Application to Autonomous Driving, in: 4th International Conference on System Reliability and Safety (ICSRS) 2019. pp. 126–135.

[6] Kaalen, S. and Nyberg, M.: Branching Transitions for Semi-Markov Processes with Application to Safety-Critical Systems, in: Model-Based Safety and Assessment 7th International Symposium (IMBSA) 2020, pp. 68–82. Lisbon, Portugal. Proceedings

[7] Rausand, M.: Reliability of safety-critical systems: theory and application, John Wiley & Sons (2014).

[8] Flammini, F. Iacono, M. Marrone, S., and Mazzocca N. : Using repairable fault trees for the evaluation of design choices for critical repaiable systems, in: Proceedings of the 9th IEEE International Symposium on High-Assurance Systems Engineering (HASE) 2005, pp. 163–172. Heidelberg, Germany.

[9] https://www.kth.se/itm/smptool Last accessed: 9 Aug 2021

[10] Ruijters, E., Stoelinga, M.: Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools, in: Computer Science Review, vol.15-16, pp.29–64, 2015.