Advances in Reliability, Safety and Security, Part 3 – Kołowrocki, Dąbrowska (eds.)
 ISBN 978-83-68136-15-9 (printed), ISBN 978-83-68136-02-9 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Probabilistic Approach Using SMP Tool For Systems Safety Of Road Vehicles

Stefan Kaalen[a,b], Mattias Nyberg[a,b], Ted Strandberg[c], Fredrik Warg[c], Adrian Westerberg[b]

[a]*KTH Royal Institute of Technology, Stockholm, Sweden*
[b]*Scania CV AB, Södertälje, Sweden*
[c]*RISE Research Institutes of Sweden, Borås, Sweden*

Abstract

Safety analysis on the level of a complete road vehicle can be an intricate task. Several methods and tools for safety analysis have been developed by the research community. One such tool developed to bridge the gap between research and industry is Semi-Markov Process (SMP) Tool. In this paper, two approaches for safety analysis utilizing SMP Tool are presented. The holistic approach starts out with a quantitative safety target on a vehicle level to then finally argue whether a proposed system design is safe enough. In the segmented approach, the idea is to follow the development steps of industrial standards, while utilizing SMP Tool for specific tasks within the standard. Specifically the standard ISO 26262 will be under most consideration. Both approaches are applied to a case study of a battery management system for an electrified truck. The segmented approach can avoid some difficulties arising when following ISO 26262 conventionally while keeping the advantage that the standard is utilized to find what qualitative tasks should be performed. The holistic approach has an advantage in that it considers the safety from a vehicle perspective. Moreover, all ambiguity issues in ISO 26262 are avoided.

Keywords: safety, ISO 26262, probability, SMP Tool, quantitative, road vehicles

1. Introduction

Systems are becoming increasingly complex in the automotive industry. This makes it difficult to analyze systems safety, which is often essential because of the harm these systems and their failures can cause the driver and other road users. Several methods and tools that can be used for safety analysis have been presented in academia, e.g. ORIS (Paolieri, 2019), PRISM (Hinton, 2006), and SHARPE (Trivedi, 2009). However, it is often difficult for such newer tools to get traction in the industry. This can be seen for example in the standard ISO 26262 for functional safety of Electrical and Electronical (E/E) systems for road vehicles (ISO, 2018) where the suggested methods are all traditional methods that have existed for half a century, such as Fault Tree Analysis (FTA) and Fault Modes and Effects Analysis (FMEA), and Markov processes.

In an attempt to bridge the gap between research and industry, a tool known as *Semi-Markov Process* (SMP) Tool for model-based reliability analysis has been presented in (Kaalen, 2021, 2022). The justification is that the modeling language used in SMP Tool is based on Matlab Stateflow, which is already widely used within the automotive industry. In SMP Tool, safety-critical systems described by models with underlying stochastic processes are analyzed to compute the *reliability*, i.e. the probability for reaching an undesired state. As stated in (Rausand, 2004), there exists conflicting goals to develop a modeling language that allow for sufficiently realistic models that are still simple enough to be handled from a mathematical perspective. As indicated by several previous case studies (Kaalen, 2021, 2022), these goals are better achieved with the modeling language in SMP Tool than in classical methods such as FTA or Markov processes since the language in SMP Tool allows for realistic representations of dynamic behaviors of systems, while the tool itself is powerful enough to compute the reliability of these models.

Previous work regarding SMP Tool (Kaalen 2021, 2022) has focused on developing the modeling language and how to compute the reliability from a mathematical perspective. In contrast, this paper aims to investigate SMP Tool in a greater context of safety engineering, specifically in the automotive industry. To this end, we consider two different approaches: a ***holistic approach*** and a ***segmented approach***.

The ***holistic approach*** disregards many aspects of safety standards and instead addresses the safety problem at its core: what is the highest tolerable rate of accidents being caused by the vehicle. This target is expressed in terms of a reliability over the lifetime of the vehicle. From this quantitative safety target on the vehicle level, a budget is created resulting in target reliabilities for different causes of accidents. Finally, one single model for each of these causes related to a system of interest is created and analyzed in SMP Tool to find if the system meets its reliability target. A related holistic view of safety engineering can be found in (Rausand, 2014). In Chapter 2 of (Rausand, 2014), assigning acceptance criteria is also started from the top system (vehicle) level and broken down to system levels. However, it is not specified how this criteria should be quantified. Moreover, once acceptance criteria are found on the system-level, how to assure that the system satisfies its criteria is managed differently than with the holistic approach in the present paper. Lacking powerful modeling languages with analysis tools such as SMP Tool, the criteria are in (Rausand, 2014) instead broken down further into discrete integrity levels on the safety mechanisms in the system, after which it has to be verified for each function in isolation that it satisfies its integrity level. However, often dependencies do exist between these safety mechanism and these dependencies may be lost in the process. Furthermore, when translating probabilistic acceptance criteria into discrete integrity levels, information is lost which may result in an over-engineered system design or even a system that it not safe enough to satisfy the top-level acceptance criteria.

The ***segmented approach*** aims to follow the workflow of the functional safety standard ISO 26262 but utilizes SMP Tool to go beyond the tasks in the standard. There are previous papers discussing tools to help with tasks in ISO 26262 (Chiang, 2022; Sinha, 2011). However, these tools provide support for performing the tasks conventionally while the use of SMP Tool allows to adapt these tasks to its more capable modeling language. This allows for system designs more accurately dimensioned for a required level of safety.

The outline of the paper is as follows. First, in Sec. 2, preliminaries are presented. Then, in Sec. 3, an industrial case study from the heavy-vehicle manufacturer Scania is presented. In Sec. 4 and 5, the holistic and segmented approaches are presented and exemplified on the case study. Finally, in Sec. 6, key findings are emphasized and discussed together with possibilities of extending the segmented approach beyond ISO 26262.

2. Preliminaries

2.1. SMP Tool

SMP Tool is a MATLAB application for analysis of stochastic and time-dependent models. The supported modelling language, called Stochastic StateFlow (SSF), is an extension of a safe subset of Stateflow, with syntax and semantics defined in (Kaalen, 2022). SMP tool supports transient and sensitivity analysis of SSF models through computation of the reliability. Transient analysis of an SSF model finds the reliability while sensitivity analysis indicates to which parameters in the model the reliability is most sensitive. SMP Tool implements two solver methods. Firstly, a Monte Carlo simulation solver that gives statistical bounds on the failure probability, i.e. $1 - reliability$. Secondly, an analytical solver that gives an upper bound on the failure probability.

SSF models are a variant of statecharts with hierarchy and parallelism. A minimalistic SSF model is illustrated in Figure 1. States are represented by boxes with the state name in the left upper corner. States with dashed edges, e.g. `S1`, are parallel states which are active concurrently with their siblings if their parent is active. For states with solid edges, e.g. `S4`, only one sibling is active if their parent is active. Initially the states marked by an arrow from a blue dot is active if its parent is active, e.g. `S2` and `S4`. States marked with `down_state`, e.g. `S5`, represent system failure and are thereby identifies the target of the reliability computation.

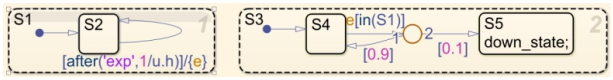

Fig. 1. Minimalistic SSF Model.

Transitions between states, e.g. the transition from `S2`, are represented by arrows with transition labels of the form `condition_events[guard]/{broadcast_event}`, e.g. `[after('exp', 1/u.h)]/{e}`. For a transition to be taken, any of the condition events, if such exists, must be broadcasted, and the guard must be true. If a transition is taken, the broadcast event is broadcasted allowing further transitions to be taken.

Guards have two basic forms. Firstly `in(state)` which is true if `state` is active. Secondly `after(distribution,parameters)` which is true if a time sampled from the distribution and parameters has passed since the source state was entered. Guards may also contain the connectives `~` (not), `&&` (and) and `||` (or).

Finally, transitions with probability branching, e.g. the transition with `S4` as source, are represented by arrows with transition labels of the form described above to a circle from which arrows with transition labels of the form `[probability]/{broadcast_event}` go to each destination state. One destination state is chosen according to the `probability` and then the event `broadcast_event` is broadcasted.

2.2 ISO 26262

ISO 26262 is a functional safety standard addressing safety-related systems in road vehicles that include electrical and/or electronic (E/E) elements (ISO, 2018). The objective of the standard is to achieve *absence of unreasonable risk caused by malfunctioning behavior* in those E/E elements. This is done by applying safety measures throughout the product lifecycle. The standard is organized around a V development model prescribing different measures in each phase. This model is illustrated in Figure 2 with the encircled numbers indicating different parts of the standard. Measures can be both process-oriented (e.g., using appropriate reviews and analyses, and ensuring a well-working safety culture) or product-based (e.g., introducing redundancy and diagnostics where needed). A key activity in the concept phase is to make a Hazard Analysis and Risk Assessment (HARA), resulting in a set of safety goals (top level safety requirements) each with an assigned Automotive Safety Integrity Level (ASIL) from A to D. Higher integrity levels indicate higher risk and consequently more rigorous safety measures to achieve the required risk reduction. A safety goal can be assigned Quality Management (QM) instead of an ASIL if the integrity is considered lower than the ASIL scale.

3. Case study

A case study based on a system from Scania will now be presented. The case study considers a *Battery Management System* (BMS). The system consists of a battery in which a short circuit can lead to venting of harmful gases affecting the health of the driver. In the worst case this can become life threatening. The cause of the short circuit can be external, e.g. improper charge control or inverter failure. The cause can also be internal due to a leakage of fluid in the thermal management system of the battery. To protect from short circuit, the battery is equipped with a *pyro fuse*, i.e. an explosive charge in the high-voltage circuit that is triggered by an ignition signal. For a more detailed explanation of the system, we use Figure 3a, representing a high-level model of the system and its components. For each component, the figure contains boxes representing a failure-related state (**F**), a diagnosis (**D**), and behavior (**B**). Arrows show causal dependencies, and (**-r**) means that the corresponding diagnosis or behavior can cause the system to be repaired. Below, each part of this model is described further.

From Figure 3a, we can see that the aspects of the pyro fuse, relevant for venting, is a failure and a diagnosis. The arrow from failure to diagnosis shows that when a failure appear, a diagnosis may detect it. When the diagnosis detects a failure, the whole system will be repaired. For external systems, the only aspect considered is a possible failure, i.e. improper charge control or inverter failures.

a) b)

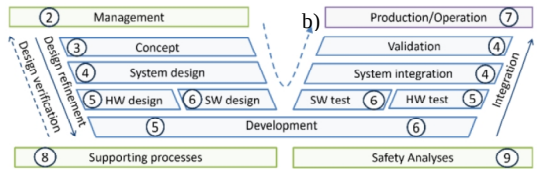

Fig. 2. ISO 26262 V-model development lifecycle.

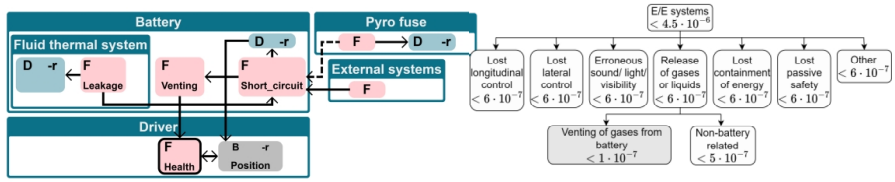

Fig. 3. (a) High-level model of BMS; (b) Breakdown of safety target from vehicle level to system level for BMS.

Within the battery, the fluid thermal system has the possibility of a ***leakage*** failure, and there is diagnosis of this leakage. Besides this, the battery has two types of failures, firstly ***short circuit***, which can cause the second type ***venting***, and this causal dependency is shown by the arrow between the two failures. There is also diagnosis of short circuit. As shown by all arrows leading into the short circuit box, the short circuit depends on three other failures. That is, it can be caused by a leakage or by an external failure. The dashed arrow shows that the pyro fuse can prevent a short circuit. Finally, the driver is modelled by a failure and a behavior. By failure here, we mean ***health*** of the driver. The behavior is essentially the ***position*** of the driver: inside or outside the cabin. The health depends on the position and venting, e.g. venting while driver is in the cabin affects the health, but not when the driver is outside the truck. The position depends on a ***warning*** from the diagnosis of the short circuit, urging the driver to escape from the cabin. The position also depends on the health, i.e. the driver may choose to leave the cabin due to perceiving symptoms of the gas.

4. Holistic approach

In the ***holistic approach***, a quantitative target of the lowest tolerable reliability of a vehicle, is specified. This ***safety target*** on a vehicle level can be determined with several different sources in mind, e.g. historical accident data and legal requirements (European Commission, 2022). The vehicle level safety target is then budgeted into safety targets on a lower level from different causes such that if all the lower-level targets are met, the safety target for the whole vehicle is met. In cases without dependencies originating from common-cause or cascading failures, this is straight-forward. If dependencies exist, this can be solved by SMP Tool in a similar manner to what will be discussed in Section 5.3.

In order to argue that a system is safe enough, one SSF model is built for each lower level safety target relevant to the system. By analyzing each of these models in SMP Tool, it is found if the suggested system design is safe. The parameters, such as failure rates and diagnostic coverages, in the model then become requirements for the system. In Sec. 6, it is discussed how these requirements can be utilized to indicate e.g. which process steps should be considered when creating the software for a particular subsystem by studying ISO 26262.

Clearly, this holistic approach disregards many aspects of safety standards such as defining ASILs. However, by taking the problem of safety to its core: What is the highest tolerable rate of accidents caused by a vehicle, safety is addressed in a straight-forward fashion.

4.1. Holistic approach exemplified

Here the BMS case study is utilized to exemplify the holistic approach. Specifically, one potential cause of fatalities is considered: ***Venting of gases from the battery***. It is assumed that fatalities can only occur if the gases reach a fatal concentration in the cabin while the driver is present. Based on accident data, it is assumed that the top level safety target for the vehicle over the lifetime is given by the probability $4.5 \cdot 10^{-6}$ of a fatal accident caused by Electrical or Electronical (E/E) systems. Notably, the choice of looking at accident data in order to find a target value on a vehicle level is supported by for example the recently released EU regulation for development of automated driving system (European Commission, 2022).

It is now assumed that a breakdown from the top level has found that the lower level safety target connected to the cause stated above is budgeted to be $1 \cdot 10^{-7}$ over the vehicle lifetime. An example of how this breakdown may look is presented in a fault tree-like structure in Figure 3b. All safety targets in the figure should be read as e.g. “Fatal accident caused by [Release of gases or liquids]”. The target values for the lower levels have been chosen such that the sum of probabilities of the lower level targets equals the parent safety target.

The idea is now to create an SSF model of how the proposed system design may cause fatalities to assure that the lower level safety target is satisfied. The high level model of the system in Figure 3a is refined into an SSF model with the same structure, illustrated in Figure 4. As an example, consider the state `Pyro_fuse_availability` in the SSF model, corresponding to the failure block **F** of the pyro fuse in Figure 3a. When a failure of the pyro fuse occurs, a transition from the state `Pyro_fuse_working` to `Pyro_fuse_broken` is triggered. As is explained in Section 2.1, the transition is triggered after a time given by an exponential distribution with rate `FR_pyro` and the event `pyro_breaks` is broadcasted which will affect `Pyro_diagnosis`.

After analyzing the SSF model using SMP Tool 3.6.0 it was found that the probability of failure is $2 \cdot 10^{-7}$. While near, this clearly does not meet the specified target and a decision must now be made whether to rethink the complete design, or to adjust the subsystem requirements within the model represented by the parameters.

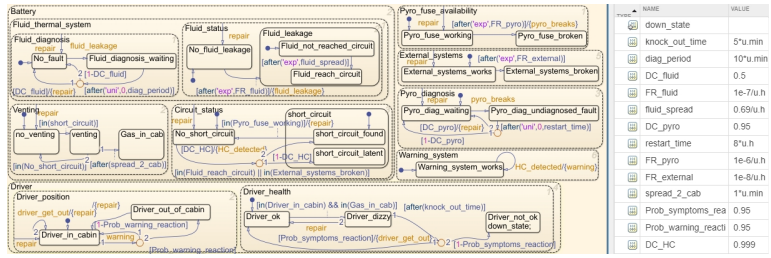

Fig. 4. SSF model for applying the holistic approach to the BMS case study.

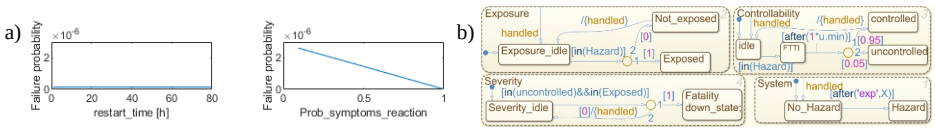

Fig. 5. (a) Result of sensitivity analysis of two parameters in BMS; (b) HARA SSF model of BMS.

Table 1. (a) Use of SMP Tool in ISO 26262 safety activities; (b) Conversion table from hazard rates to ASIL classes.

Activity	Part-Section
Hazard Analysis and Risk Assessment (HARA)	3-6
Safety analysis instead of e.g. fault tree analysis	5-7, 6-7, 9-8
Requirements decomposition/refinement	5-7, 6-7, 9-5
Calculation of hardware metrics	5-8, 5-9
Supporting impact analysis of changes	8-8

ASIL / QM	Highest tolerable hazard rate
ASIL D	$[1 \cdot 10^{-10}, 8 \cdot 10^{-9}]h^{-1}$
ASIL C	$(8 \cdot 10^{-9}, 2 \cdot 10^{-8}]h^{-1}$
ASIL B	$(2 \cdot 10^{-8}, 2 \cdot 10^{-7}]h^{-1}$
ASIL A	$(2 \cdot 10^{-7}, 1 \cdot 10^{-5}]h^{-1}$
QM	$(1 \cdot 10^{-5}, 1]h^{-1}$

Given that the result was close to the target, simply adjusting the subsystem requirements is now investigated. A sensitivity analysis is run in SMP Tool to see to which extent each parameter affects the probability of failure. Figure 5a illustrates the analysis result for two of the parameters where the right parameter clearly impacts the probability of failure while the left one has negligible impact. The sensitivity analysis yields that the parameters that the reliability of the model is most sensitive to are: the failure rate that the battery leaks fluid, `FR_fluid`, the probability of the driver reacting to symptoms of the gas, `Prob_symptoms_reaction`, and the diagnostic coverage of detecting high current, `DC_HC`. Based on this, these three parameters are investigated first. The probability of the driver reacting to the symptoms of the gas cannot be adjusted by the system design. Moreover, the diagnostic coverage of detecting high current is already very high. However, for the failure rate that the battery leaks fluid, it is considered that by utilizing a different material, it can be lowered to $5 \cdot 10^{-8}/h$. By analyzing the SSF model again with this changed parameter, it is found that the new probability of a failure yielded by SMP Tool is below the target of $1 \cdot 10^{-7}$. This means that this new model reached an acceptable level of safety. The system design is thereby acceptable given that all requirements given by the parameters in the model are satisfied.

5. Segmented approach

The *segmented approach* follows a different strategy than the holistic approach. Rather than creating a budget from the vehicle level and building and analyzing one SSF model per relevant safety target, this approach more closely adheres to the safety standard ISO 26262. SMP Tool is utilized as a supporting tool when performing some of the tasks required by the standard. Table 1a provides a non-exhaustive list of activities in ISO26262 where SMP Tool can be used. Specifically, three of these areas will be investigated further: the HARA, requirements decomposition, and the calculation of hardware metrics.

5.1. Translate tolerable hazard rate to ASIL

Since SMP Tool is probabilistic, integrity levels yielded by the tool is in the form of probabilities or rates. On the other hand, ISO 26262 handles integrity levels by discrete ASIL classes. Therefore, a table translating the highest tolerable hazard rate yielded by SMP Tool into an ASIL class is here developed. When the highest tolerable hazard rate has been identified, this number is simply compared with this table to find the ASIL of the corresponding hazardous event and safety goal. For the remainder of the paper, a heavy truck developed for a

lifetime of 45000 hours is considered. Moreover, we assume that over the vehicle lifetime, the highest tolerable probability for a malfunctioning E/E system causing a fatal accident is $4.5 \cdot 10^{-6}$.

The translation is developed with the help of the tables in Annex B in Part 3 of (ISO, 2018) where probability intervals are assigned to different levels of *severity*, *exposure*, and *controllability*. Moreover, since the probability intervals for severity in ISO 26262 are expressed in terms of the Abbreviated Injury Scale (AIS), another table converting this scale to intervals of probability, is also needed. Such a table is illustrated in (Wilde, 2019) and will here be utilized. Each of the mentioned tables with probability intervals can be utilized in several ways. To avoid overlap between ASIL classes, the chosen approach is to compute the mean of each probability interval and multiply these to yield a how likely it is that the hazard cause an accident. It can then be computed with a simple model in SMP Tool what the highest tolerable hazard rate is to not exceed the tolerable probability $4.5 \cdot 10^{-6}$ of a fatal accident caused by any E/E system . Since the probabilities varies by orders of magnitude, a logarithmic mean is chosen to give a more intuitive understanding of *being in between* two probabilities. Noteworthy, since several different combinations of severity, exposure, and controllability can be translated to the same ASIL in ISO 26262, most ASIL classes are given several different values for the highest tolerable hazard rates. We let the lowest and highest of these values create an interval of highest tolerable hazard rates corresponding to each ASIL.

As an example of how to create this table, we consider the combination of S3, E4, and C2 that is one of the combinations corresponding to ASIL C in ISO 26262. Severity class S3 corresponds to a probability between 0.1 and 1 of reaching AIS 5 or 6. Through the tables in (ISO, 2018) and (Wilde, 2019) and the logarithmic mean, this yields the probability 0.39 of reaching an AIS level that has a probability of 0.74 for fatalities if the driver cannot avoid an incident caused by the hazard and the vehicle is in a situation where the hazard is dangerous. Similarly, exposure class E4 yields the probability 0.39 that the vehicle is in a situation where the hazard is dangerous, and controllability class C2 yields the probability 0.039 that harm can be avoided by driver interaction. Analysis of a simple model in SMP Tool yields that the highest tolerable hazard rate is $2 \cdot 10^{-8}$, given that the probability of it leading to a fatal accident is $0.39 \cdot 0.74 \cdot 0.39 \cdot 0.039 = 0.004$.

Once a preliminary table is found, small conservative adjustments are made of the limits between ASIL classes to achieve complete coverage of rates without any overlap. QM is also added and ASIL A is extended to include rates of as high as 10^{-5} since it is estimated that this extension will not result in assignment of too low integrity levels. All of this finally yields Table 1b translating highest tolerable hazard rates to ASIL classes. As an example, we can see in the table that the hazard rate $2 \cdot 10^{-8}$ calculated in the example above constitutes the upper limit of highest tolerable hazard rates corresponding to ASIL C.

5.2. HARA

The BMS system will now be utilized to exemplify the segmented approach. Specifically, the HARA, requirements decomposition, and the calculation of hardware metrics presented in Table 1a is exemplified.

We begin with the concept phase and specifically the HARA. We here assume that we are early in the development process of the BMS system and currently do not have a detailed proposed design. Furthermore, given that identifying hazards, hazardous events, and safety goals is a qualitative exercise, we assume this has already been done and the task remaining is to assign ASILs to these safety goals. The idea when doing this with SMP Tool is to identify the greatest tolerable hazard rate for each hazard after which this rate is translated into an ASIL through Table 1b.

The hazard under consideration is defined as H1: *battery venting harmful gas into the cabin*. This hazard give rise to the hazardous event HE1: *battery venting lethal amount of harmful gas when a person is present in the cabin*. The ASIL for this hazardous event can now be found through the model presented in Figure 5b together with Table 1b. It is here estimated that, 95% of all drivers will be able to control the situation, i.e. leave the driver cabin before turning unconscious. The reasoning behind this is that while the gas is odor-and colorless, symptoms such as headache, nausea, and dizziness portrays in advance of loss of consciousness. Moreover, the exposure is estimated to be 100% since during the operating time of the vehicle, the time spent without a driver in the cabin is seen as negligible. Finally, if the driver does not leave the cabin in one minute after gas is being vented it is estimated that the gas will cause a fatality 100% of the time.

The parameter marked X in the model represents the rate at which the hazard happens in the system. The idea is now to vary X to find the highest hazard rate that yields a probability of fatality lower than the tolerable limit of $4.5 \cdot 10^{-6}$ yielded from accident data. Note that here the target probability $4.5 \cdot 10^{-6}$ is not broken down as in the holistic approach since this would yield a different conversion table between ASIL classes and rates for each system in a vehicle. It is found that the worst tolerable rate for the hazard is $2 \cdot 10^{-9}$. Looking at Table 1b it is clear that this yields ASIL D for the hazardous event. The same ASIL is then assigned to the safety goal SG1: *Battery shall not vent a lethal amount of gas into the driver cabin while a person is in the cabin*, corresponding

with this hazardous event. Notably, this is the same ASIL class as the one reached in (Khoury, 2021) for the hazardous event of fire and smoke reaching the driver compartment while driving at high speed. Note that with the same probability of controllability, exposure, and severity as presented in Figure 5b, a conventional HARA in accordance with ISO 26262 would following the tables in Annex B in Part 3 of ISO 26262 result in the lower integrity level: ASIL C. The main reason behind this difference is the crudeness of the classes of controllability, exposure, and severity in ISO 26262. In our example, the exposure and severity is not only in the highest classes but also in the upmost end of the corresponding intervals.

5.3. Requirements Decomposition

We will now remain in the concept phase and assume that we have the same safety goal as in the HARA SG1: *Battery shall not vent a lethal amount of gas into the driver cabin while a person is in the cabin* that has now been assigned ASIL D. To move forward with SMP Tool we do however need a probability rather than an integrity level. We find this probability by first identifying a tolerable rate of occurrence of the hazard corresponding to the safety goal. Two alternative ways this rate can be found are: 1) the ASIL of the safety goal can be translated through Table 1b or, 2) if SMP Tool was used for the HARA, the highest tolerable hazard rate found there can be used. If the table is used, the lowest rate for that ASIL should be utilized in order to be conservative. We will here move forward with alternative 2) and the rate $2 \cdot 10^{-9}/h$ found in the HARA in Section 5.2. This rate corresponds to the probability of $9 \cdot 10^{-5}$ of H1 occurring over the lifetime 45000 h of the vehicle.

The idea is now to decompose our safety goal into two functional safety requirements: R1: *Battery shall not vent harmful gas*, and R2: *If battery vents harmful gas, the driver shall be warned at least one minute before a lethal amount of gas is in the driver cabin*. In the decomposition, it is also assumed that 95% of the drivers will react properly to a warning. Note that, while the probability happens to be the same, this does not represent the same quantity as the probability 0.95 considered in the controllability of the HARA which represents the probability of the driver escaping without a warning present. The question is now: which ASIL can be attributed to each of these two new requirements? To answer this, an SSF model with both the sub-requirements as well as the assumption on the driver is created. Since Table 1.b contains probabilities per hour and not on demand probabilities, we for R2 ask the question: which failure rate can the warning-subsystem have. Implicitly, this failure rate yields the probability that the warning system gives a warning when it should. The model is presented in Figure 6, where Z and Y represent the rates of the requirements we wish to find and translate into ASILs. The idea is to find a combination of Z and Y ensuring that the total probability of gas being released in conjunction with that harm is not avoided by the safety mechanism, is below the probability $9 \cdot 10^{-5}$ of H1 occurring without the safety mechanism in the system. Through this, the probability that R1 and R2 are violated is never higher than the probability that SG1 is violated.

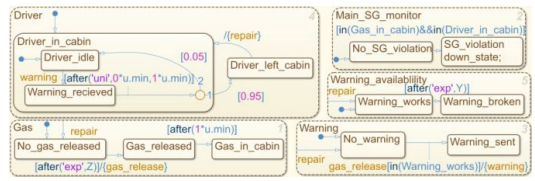

Fig. 6. SSF model to determine ASILs for decomposed requirements in the BMS case study.

It can now be realized that we have two variables: Z and Y and more than one answer can therefore be found. This reflects the fact that there are several ways we can attribute rates to the sub-requirements and still meet the requirement of the overarching safety goal. Two examples are now given for how to, by analyzing the model, find a combination of ASIL levels that can be attributed to the sub-requirements. In the first example, it is found that by setting the highest tolerable rate for the hazard corresponding to R1 to $2 \cdot 10^{-8}$, corresponding to highest rate of ASIL C, the worst tolerable failure rate for the warning system in order to satisfy the target probability of $9 \cdot 10^{-5}$ is $2 \cdot 10^{-6}$, corresponding to ASIL A. One acceptable decomposition is thereby R1: ASIL C and R2: ASIL A. Note that using the upper rate in Table 1b, i.e. $2 \cdot 10^{-8}$ in ASIL C, for R1 is conservative in the sense that no hazard rates chosen from the table satisfying R1: ASIL C and R2: ASIL A will violate the target probability of $9 \cdot 10^{-5}$. In the second example, it is attempted to set R1 to ASIL B. By letting Z take the value of $2 \cdot 10^{-7}$ it is found that the target probability cannot be met, regardless of the rate of R2. This is interpreted as that R1 may not be lower than ASIL C. This is notable since a traditional requirement decomposition from an ASIL D safety goal would according to ISO 26262 allow ASIL B for each of the requirements. The decomposition into ASIL C and ASIL A above can now be continued by breaking down either of requirements R1 or R2 further.

5.4. Calculation of Hardware Metrics

The hardware design phase is now entered with the calculation of hardware metrics discussed in part 5 of ISO 26262. Consider the safety goal presented earlier SG1: ***Battery shall not vent a lethal amount of gas into the driver cabin while a person is in the cabin*** with ASIL D. According to tabulated values in (ISO, 2018), this yields that the probability of violating the safety goal due to random hardware failures should be less than $10^{-8}/h$ or $4.5 \cdot 10^{-4}$ over the lifetime of the vehicle. According to the standard, a quantitative analysis of the suggested system design should be performed to assure that this probability is not exceeded. This analysis will be performed utilizing SMP Tool. While the purpose is to analyze that the system is safe from a hardware perspective, there are no restrictions in the standard on involving components of the system that is also affected by the software. With this in mind, the model in Figure 4, used for the holistic approach, can be reutilized here.

According to the standard (ISO 26262:2018-5, Section 9.4.2), the best estimate of the failure rates for hardware components should be used within the model. It is assumed that the parameters currently in the model represents these best estimates. Moreover, the fact that the driver may leave the cabin after feeling symptoms of the gas has already been considered in the HARA where the ASIL of the safety goal was assigned. This same information should now not again be utilized in order to assist in reaching the random hardware failure target values. The part named `Driver_status` in the model thereby have to be adjusted for this. The result is that the state `Driver_dizzy` is removed and that only the transition with the guard: `in(Driver_in_cabin) && in(Gas_in_cabin)` remains, only now with `Driver_not_ok` as destination state. By analyzing the model in SMP Tool it is found that the probability of violating the safety goal because of a random hardware failure is $3 \cdot 10^{-6}$ over the lifetime of the vehicle. This is clearly below the target and the design is therefore acceptable.

6. Discussion

We now discuss the advantages and disadvantages of the two approaches.

6.1. Holistic Approach

A strength with the holistic approach is that safety is considered from a vehicle perspective. By breaking down safety targets from the vehicle level to a system level, safety analysis on vehicle level can be realized by satisfying the quantitative safety targets on system level. By circumventing ISO 26262, ambiguity problems of the standard as exemplified in Sec. 6.2 are also avoided. The standard leaves itself open for interpretation and this may in the worst case cause two different users to reach two incompatible conclusions about the safety of a proposed system design. The holistic approach also has the advantage that one single model is utilized to assess all aspects of safety. This simplifies managing changes to the system. Another advantage of the holistic approach is that discussions about what should and what should not be included in the scope of the analysis is avoided. For example, when there is a fault of the battery it is not certain this should be viewed as an E/E fault rather than an electrochemical fault. Similarly, it is not always easy to draw the line of what is a functional safety problem and what rather relates to safety of the intended functionality of the system. By circumventing ISO 26262, this distinction does not have to be made within the holistic approach but all aspects of safety can be included in the same model.

A limitation of the holistic approach is how to assure that requirements yielded by the parameters in the model are met. This in mainly an issue from a perspective of qualitative safety regarding the software, i.e. what tasks should be performed in order to argue that the software in the system has a high enough quality? However, by interpreting the parameters in the model as integrity levels of sub-systems and components, support can be found within ISO 26262 to identify which tasks are suitable to apply to the software in order to argue it is safe enough.

6.2. Segmented Approach

By following the lifecycle of ISO 26262, the segmented approach avoids the mentioned limitation of the holistic approach. In essence, the argument for safety is based upon compliance with the standard. SMP Tool is simply used to support this process. However, this support may prove highly useful in a twofold manner. Firstly, three tasks of the standard have been presented and all these tasks can be solved with SMP Tool. Moreover, the preliminary analysis in Table 1a indicates that even more tasks can be performed by SMP Tool. This is an advantage since only a single tool needs to be learnt for all these tasks which would otherwise need several different tools or methods. Secondly, the quantitative approach and support for temporal properties can yield

more accurate analyses and results than conventional solutions suggested in the standard such as FTA.

A clear case where we yield these more accurate results is in the HARA of the BMS where, by avoiding the crude classifications of severity, controllability, and exposure, a different ASIL level can be reached that arguably captures the actual integrity level of the safety goal better. Also, it was found that decomposing requirements and assigning ASILs is not always as simple as just using the predefined decomposition patterns in the standard. For example, it was found in the first decomposition in the BMS that a decomposition from ASIL D to two ASIL B requirements was not acceptable for the chosen safety goal. Finally, the support in SMP Tool for temporal properties provides an intuitive handling of ***Fault-Tolerant Time Intervals*** that according to ISO 26262 are important attributes of safety requirements.

While some ambiguities in ISO 26262 remain in the segmented approach, an example of an ambiguity that can be avoided is the choice between frequency and duration for exposure in the HARA. The standard provides two different methods for determining exposure: the percentage of operating time spent in the operational situation and how often the operational situation occurs. However, which method should be chosen is not always clear, and the exposure class may prove highly different depending on the choice. For example, a long haulage truck driving in reverse could be assigned E2 with the first method and E4 with the second method. Utilizing SMP Tool, this choice does not need to be made. In the BMS example, it was quite easy to handle the exposure since the driver is almost always in the cabin when the engine is on. However, in the example of the long haulage truck driving in reverse, this could simply be modelled with two states: `Driving_in_reverse` and `Not_driving_in_reverse`. An exponential rate can then be assigned based on vehicle data for how long operational time will pass between two times when driving in reverse. Moreover, a uniform distribution could be added for how long time is spent reversing each time. This model provides a quantitative description of driving in reverse without having to make a choice between the two methods of ISO 26262.

The limitations of the segmented approach originates from the fact that it is built around ISO 26262. Some ambiguities from the standard remain even if SMP Tool is used to support some tasks. Another problem is that, unlike the holistic approach, no consideration is made in the standard regarding budgeting a quantitative safety target of the vehicle over the safety goals. The result of this may be that the vehicle as a whole is not actually safe compared to historical accident data while the vehicle has been developed in compliance with the standard.

It should be noted that in the segmented approach, the scope of the paper was only to investigate how SMP Tool can be used to perform various activities in ISO 26262. However, there are more considerations for actually using the tool in compliance with the standard. The standard supports ***tailoring*** of activities in the lifecycle, which can be used to replace methods proposed in the standard with alternative methods such as we have done with SMP Tool. However, such tailoring needs to be documented in the ***safety plan*** with a well-founded rationale explaining why “the tailoring is appropriate and sufficient to achieve functional safety” (ISO 26262:2018-3, Sec. 6.4). Such a rationale could contain some of the issues discussed in this paper describing the advantage of using SMP Tool compared to traditional analysis methods. Moreover, the standard put requirements on tool qualification (ISO 26262-9:2018, Section 11), which states activities that should be performed for the qualification of the tool itself if it is to be used in compliance with ISO 26262. Noteworthy, this qualification can be helped by the fact that SMP Tool already implements two different computation engines that are to a high extent independent of each other.

6.3. Approaches in Relation to Each Other

The advantages and disadvantages of using each approach has been discussed under the assumptions that only one of the approaches is utilized. However, in reality there is no necessity to choose between one or the other when utilizing SMP-tool for safety analysis. For example, the parameters obtained by applying the holistic approach can be utilized to find technical safety requirements on the system design. Parts of ISO 26262 can thereafter be utilized with the help of SMP Tool to argue that these requirements are satisfied. Moreover, by following both the two approaches independently of each other, an increased belief in the safety case can be achieved. This idea is rooted in the theory that a safety case cannot be assigned the value ***true*** with absolute certainty but rather with a certain level of belief (Nešić, 2021).

6.4. Other Standards

The scope of the paper has, up until now, considered ISO 26262 covering functional safety of E/E systems in road vehicles. However, there are other safety standards for systems safety. Specifically, ISO 21448, and IEC 61508, of which ISO 26262 is an adaption, will now be discussed.

ISO 21448 (ISO, 2022) is a complement to ISO 26262. While ISO 26262 address functional safety, ISO 21448 address Safety Of The Intended Functionality, i.e. ***absence of unreasonable risk due to hazards resulting from the functional insufficiencies of the intended functionality or its implementation***, which is why the standard is often simply referred to as SOTIF. This is particularly relevant for components providing situational awareness

for advanced driver assistance or automated driving functions. An example is a radar for an automated/autonomous braking system. This radar will at times indicate obstacles that are not really present, i.e. ghost warnings, and it will at times miss an obstacle that is there. Such performance issues would be treated by applying ISO 21448 rather than ISO 26262. However, both safety standards are making use of similar analysis methods, and while applying SMP Tool in SOTIF is left for future work, we believe it would be useful in activities such as SOTIF HARA or evaluating quantitative targets when defining acceptance criteria. In some aspects, using SMP Tool in ISO 21448 might be more straight-forward than ISO 26262 since ISO 21448 provides more support for identifying quantitative targets on a vehicle level.

IEC 61508 (IEC, 2010) is a domain-independent functional safety standard for E/E systems. Since ISO 26262 is an adaption of IEC 61508, the tasks performed by SMP Tool in the segmented approach can also be done for IEC 61508. In fact, the utilization of SMP Tool is more straight forward considering IEC 61508. For example, IEC 61508 presents a conversion table between safety integrity levels and the frequency of failure of safety functions. A table such as Table 1b thereby does not need to be developed.

7. Conclusion

As the main contribution, two approaches for utilizing SMP Tool in safety engineering have been presented. The holistic approach utilizes a quantitative target on the vehicle to argue whether a system design is sufficiently safe. The segmented approach is instead based on following ISO 26262 but utilizing SMP Tool to support specific tasks during the system development. Regardless of the chosen approach, modeling safety with stochastic processes and computing the reliability through SMP Tool allows for more accurate dimensioning of system design to achieve a desired level of safety without introducing unnecessary redundancy or overengineered safety mechanism.

Each approach have the potential of increasing the level of model-based safety engineering in industry. The experience from working with the case study in the paper, as well as other industrial case studies, is that, by building SSF models, the understanding of the safety properties of the system is significantly increased.

ISO 26262 has been the standard under main consideration in the paper, but the results and discussion suggests that the approaches can be extended beyond the scope of ISO 26262 and beyond the domain of road vehicles.

Acknowledgements

For financial support the authors acknowledge Vinnova FFI through the SafeDim project ref. nr. 2020-05131.

References

Chiang, T., Mendoza, R.G., Mahmood, J., Paige, R.F. 2022. Towards the adoption of model based system safety engineering in the automotive industry. MODELS 22: Proc. 25th Int. Conf. Model Driven Engineering Languages and Systems: Companion Proceedings, 579-587.

European Commission. 2022. Commission Implementing regulation (EU) 2022/1426: laying down rules for the application of regulation ({EU}) 2019/2144 of the European Parliment and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles. Official Journal of the European Union 221, 1-64.

Hinton, A., Kwiatkowska, M., Norman, G., Parker, D. 2006. PRISM: A tool for automatic verification of probabilistic systems. Proc. 12th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS'06), 441-444

International Electrotechnical Commisson. 2010. IEC 61508:2010: Functional safety of elactical/electronic/programmable electronic safety-related systems.

International Organization for Standardization. 2018. ISO 26262:2018: Road Vehicles - Functional Safety, 2nd Ed.

International Organization for Standardization. 2022. ISO 21448:2022 Road Vehicles - Safety of the Intended Functionality.

Kaalen, S., Nyberg, M., Mattsson, O. 2021. Transient analysis of hierarchical semi-Markov process models with tool support in stateflow. Int. Conf. Quantitative Evaluation of Systems, 105-126.

Kaalen, S., Hampus, A., Nyberg, M., Mattsson, O. 2022. A Stochastic Extension of Stateflow. Proc. 2022 ACM/SPEC on Int. Conf. Performance Engineering. 211-222.

Khoury, N. 2021. ISO Functional Safety Requirement Types. www.btc-embedded.com/iso-26262-requirement-types/. Accessed 2024-04-16.

Nešić, D., Nyberg, M., Gallina, B. 2021. A probabilistic model of belief in safety cases. Safety Science 138, art. 105187.

Paolieri, M., Biagi, M., Carnevali, L., Vicario, E. 2021. The ORIS Tool: Quantitative Evaluation of Non-Markovian Systems. IEEE Transactions on Software Engineering 47(6), 1211-1225.

Rausand, M., Høyland, A. 2004. System Reliability Theory: Models, Statistical Methods, and Applications 2nd ed. Wiley. Hoboken

Rausand, M. 2014. Reliability of Safety-Critical Systems: Theory and Applications. Wiley. Hoboken.

Sinha, P. 2011. Architectural Design and Reliability Analysis of a Fail-Operational Brake-By-Wire System from ISO 26262 Perspectives. Reliability Engineering & System Safety 96(10), 1349-1359.

Trivedi, K. S., Sahner, R. 2009. SHARPE at the age of twenty two. ACM SIGMETRICS Performance Evaluation Review 36(4), 52-57.

Wilde, K., Tilsen, A., Burzynski, S., Witkowski, W. 2019. On estimation of occupant safety in vehicular crashes into roadside obstacles using non-linear dynamic analysis. In MATEC Web of Conferences 285, art. 00022.