Reliability Engineering and System Safety 130 (2014) 42–49

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Modeling automotive safety mechanisms: A Markovian approach

Abraham Cherfi [a,b], Michel Leeman [b], Florent Meurville [b], Antoine Rauzy [a,c,*]

[a] *LIX – Ecole Polytechnique, route de Saclay, 91128 Palaiseau cedex, France*
[b] *GEEDS Valeo, France*
[c] *Chaire Blériot-Fabre – Ecole Centrale de Paris, Grande Voie des Vignes, 92295 Châtenay-Malabry, France*

ARTICLE INFO

Article history:
Received 12 December 2013
Received in revised form
22 April 2014
Accepted 23 April 2014
Available online 2 May 2014

Keywords:
Automotive functional safety
ISO 26262
Safety mechanisms
Markov models

ABSTRACT

Cars embed a steadily increasing number of electric and electronic systems. One of the means at hand to enhance the safety of these systems is to reinforce them with so-called safety mechanisms. The ISO 26262 standard discusses at length how to estimate the contribution of these mechanisms to functional safety. These calculations rely however on fault tree models or ad-hoc formulas that are hard to check for completeness and validity. In this article, we propose generic Markov models for electric and electronic systems protected by first and second order safety mechanisms. These models are of a great help to clarify the behavior of these systems as well as to determine the domain of validity of simpler models such the above mentioned fault trees or ad-hoc formulas. Experimental results make it possible to have a better understanding of which parameters really matter in terms of safety.

1. Introduction

Cars embed a steadily increasing number of electric and electronic systems. In order to guaranty their functional safety, the ISO 26262 standard was published in November 2011 [1]. This standard defines a number of constraints and rules that the development of automotive electric and electronic systems must obey. One of the means at hand to enhance the safety of electric and electronic systems is to reinforce them with so-called safety mechanisms. Safety mechanisms are various types of devices that typically prevent spurious usages of the system, or warn the driver when something wrong happens.

The ISO 26262 standard discusses at length the use of these safety mechanisms and how to estimate their contribution to functional safety. To do so, it relies essentially on fault tree models or ad-hoc formula. Such models or formulas are indeed of interest for practitioners. But they are only approximations. Without a more explicit representation of failure scenarios to serve as a reference, it is hard to check them for completeness, to understand their domain of validity and to ensure their accuracy. Explicit models have been proposed by several authors for safety instrumented system described in the mother IEC 61508 Standard [2] (see e.g. [3,4]). In the case of the ISO 26262 standard, at least to our knowledge, this work has not been done yet.

The purpose of this article is therefore to fill this hole by proposing generic Markov models for electric and electronic systems reinforced by first order and possibly second order safety mechanisms. The interest of these models is twofold: first, they are of a great help to clarify the behavior of safety mechanisms; second, they make it possible to determine the domain of validity of simpler models such as fault trees or ad-hoc formulas of the standard.

The remainder of this article is organized as follows. First, we present two typical examples of safety mechanisms in Section 2. Then, we propose Markov models for these safety mechanisms in Section 3. We report numerical results obtained on these models in Section 4 and we discuss their significance. Finally, we review related works in Section 5.

2. Two typical examples of safety mechanisms

In this section, we present two representative examples of automotive systems embedding safety mechanisms.

2.1. Vehicle management unit for inversion

We shall first consider the case of a Vehicle Management Unit (VMU). In an electric vehicle, a VMU is responsible for commanding the electric motor inverter, among other functions. A VMU consists typically in a microcontroller which, given certain inputs (gas and brake pedal positions), sends a torque set-point to the

[*] Corresponding author.
E-mail addresses: abraham.cherfi@lix.polytechnique.fr (A. Cherfi), michel.leeman@valeo.com (M. Leeman), florent.meurville@valeo.com (F. Meurville), antoine.rauzy@ecp.fr (A. Rauzy).

http://dx.doi.org/10.1016/j.ress.2014.04.013
0951-8320/© 2014 Elsevier Ltd. All rights reserved.

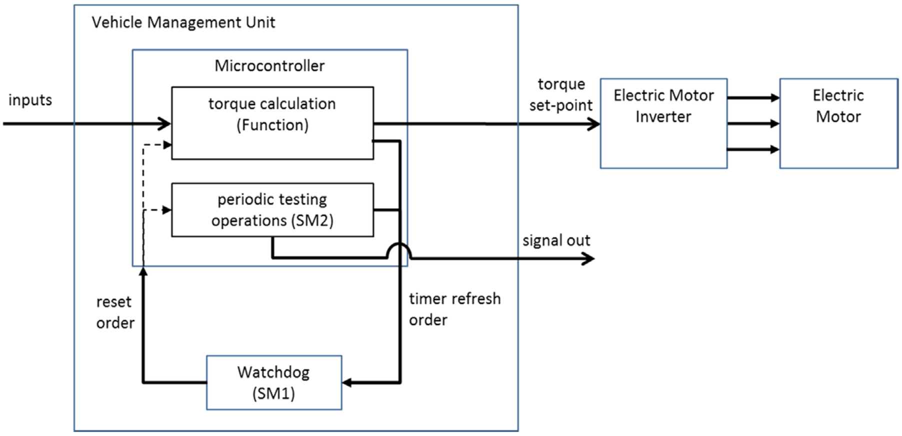

Fig. 1. Simplified functional representation of the vehicle management unit for inversion.

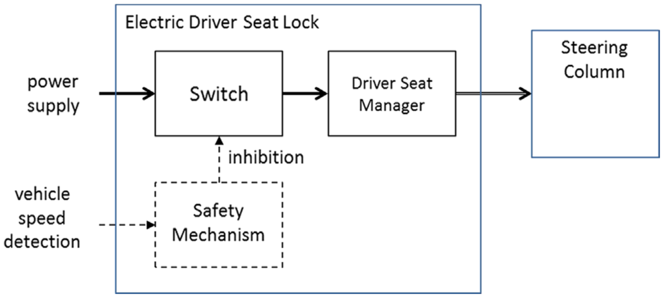

Fig. 2. Functional representation of an electric driver seat control.

inverter that in turn commands the electric motor (traction and regenerative braking), as illustrated Fig. 1.

Such a VMU is a critical function: if the microcontroller gets stuck in a loop and continuously sends a command higher (or lower) than expected, it could lead to unintended vehicle acceleration or braking.

In order to prevent such hazards, a watchdog is added which is in charge of bringing the system to a safe state in case the microcontroller is detected to be stuck. The watchdog is an electronic component that is used to detect and recover from microcontroller malfunctions. The microcontroller refreshes regularly the watchdog in order to prevent him from timing out. If it gets stuck in a loop, the watchdog cannot be reset, so the watchdog times out and sends a reboot order to the microcontroller.

Such a watchdog is a first order safety mechanism based on error detection.

As a physical component, the watchdog may fail (although the reliability of the watchdog is much higher than the one of the microcontroller). Also, the watchdog is able to detect only certain kind of errors of the microcontroller: typically, it is not able to detect memory corruption problems.

In order to ensure that the watchdog is working, the microcontroller tests the watchdog at each vehicle start. The role of this second order mechanism is to warn the driver in a case of a problem with the watchdog. It may itself fail and is itself not able to catch all of the problems of the watchdog.

As the torque calculation function and the second order safety mechanism function are never executed in parallel, their failures are considered as independent (and are independent from watchdog failures).

The above example is representative of safety mechanisms based on error detection as embedded for instance in electric steering column controller, electric braking, several types of microcontrollers protected with watchdogs and more generally command-control systems.

2.2. *Electric driver seat controls*

Another type of safety mechanism is used in Electric Driver Seat Controls (EDSC). An EDSC allows the driver to tune his seat position. A spurious tuning action while the vehicle is running (over a certain speed, e.g. 10 km/h) can indeed cause an accident, for instance because the driver is no longer able to reach the brake pedal or because he gets suddenly pushed onto the steering wheel.

In order to prevent this from happening, the system embeds a mechanism in charge of turning off the power supply of the EDSC when the vehicle is running (see Fig. 2). This first order mechanism is therefore based on inhibition. As previously, it is in general completed with a second order one in charge of testing it at each vehicle start (obviously, it cannot be tested while the vehicle is running).

The above mechanism is representative of safety mechanisms based on inhibition, as embedded for instance in electric steering column lock, automatic doors opening systems and more generally all systems that must be inhibited when the speed of the vehicle gets above a give threshold.

2.3. *Discussion*

The majority of automotive first order safety mechanisms can be actually categorized in either of the two categories presented above:

- Most of them are based on error detection. The idea is to switch the system into a safe state when an error is detected. These safety mechanisms are usually made of two elements: the detection device and the actuation device.
- Some of them inhibit the system they protect when the vehicle is in a state where the failure of the system is potentially dangerous.

As a failure of the first order safety mechanism has in general no direct influence of the system it controls, it can hardly be perceived by the driver. A second order safety mechanism is thus often added in order to check periodically the availability of the first one, typically when the engine is turned on or the vehicle starts to move. The role of such a second order mechanism is to warn the driver.

The improvement in vehicle safety provided by first and second order safety mechanisms can be measured by means of indicators such as the Probabilistic Metric for random Hardware Failures (PMHF).

The target value for the PMHF (and more generally for the reliability of the system) is determined by the so-called

Automotive Safety Integrity Level (ASIL). The ASIL consists of an aggregation of three parameters: the severity (quotation of the consequences of the function failure), the controllability (quotation of the driver control over the situation and its ability to limit the consequences) and the exposure (quotation of the frequency of the situation where the dangerous hazard could happen) [1]. These indicators are estimated prior to and thus independently of any probabilistic calculation regarding the system. Safety mechanisms such as those presented above have obviously nothing to do with severity. They are somehow potentially related to the two other parameters, but in a different way depending on the type of the considered safety mechanism.

Safety mechanisms based on inhibition aim only at reducing the probability of a certain event to happen, e.g. a spurious tuning action of the driver seat while the vehicle is running, i.e. they reduce the probability that something bad happen in case of exposure to a dangerous situation. The Markov models presented in the sequel can be used to measure as accurately as possible the probability of such an event to occur with and without safety mechanisms.

Safety mechanisms based on error detection are related to both the controllability of the system (for they put the vehicle into a safe state in case of a failure of the function) and the exposure (for they reduce the probability of a dangerous event to occur in case of exposure), as exemplified by the watchdog for vehicle management unit presented above. Although the Markov models presented in the sequel aim primarily at assessing as accurately as possible the probability of a dangerous event to occur with and without safety mechanisms, they provide also some information about the controllability (via the probability to be in a safe state).

3. Generic Markov models

To have a clear understanding of the behavior of electric and electronic systems in the presence of failures (including those of safety mechanisms), the best method is probably to design state/transition models for these systems. It is often the case that Markovian hypotheses are verified or at least are a good approximation for calculation purposes so that these models can be turned into Markov chains in a straightforward way.

In this section, we shall propose Markov chains for systems of each of the two above categories. These Markov chains are generic in the sense that one has just to adjust values of parameters (such as failure rates, coverage rates…) to assess the safety of a particular system. Markov chains presented hereafter can be subsequently embedded into larger Markov models or approximated either by means of fault tree constructs or by ad-hoc formulas. They serve as a reference.

3.1. Case of a hardware block protected by a first order safety mechanism based on error detection

Let us consider first the case of a Hardware block HB protected by a first order safety mechanism SM1 based on error detection. The generic Markov chain for this system is given in Fig. 3.

Such a system fails in a dangerous state if both the hardware block and the safety mechanism fail, no matter in which order. Therefore, the Markov chain encodes basically three failure scenarios.

In the initial state (1), both the hardware block and the safety mechanism are working. The failure rates λ_{HB} for the hardware block and λ_{SM1} are assumed to be constant over the time (no ageing effect). If the hardware block fails first, the system goes to state 2, where the safety mechanism detects or not this failure instantaneously. As a graphical convention, we denote instantaneous states and their outgoing probabilities by dashed lines, as on the figure. The probability not to detect the failure is 1-DC1, where DC1 stands for the diagnostic coverage of the safety mechanism. In the state (2), if the failure of the hard block is not detected the system goes to the failure state (5) (first failure scenario). Otherwise, it goes to the safe state (3). In this state, the mean time before the vehicle is taken to the garage is T_M, i.e. the repair rate of the hardware block is $\mu_V = 1/T_M$. Now, if the safety mechanism fails before the vehicle is repaired, then the system goes to the failure state (5) (second failure scenario). Otherwise it goes back to the initial state (1).

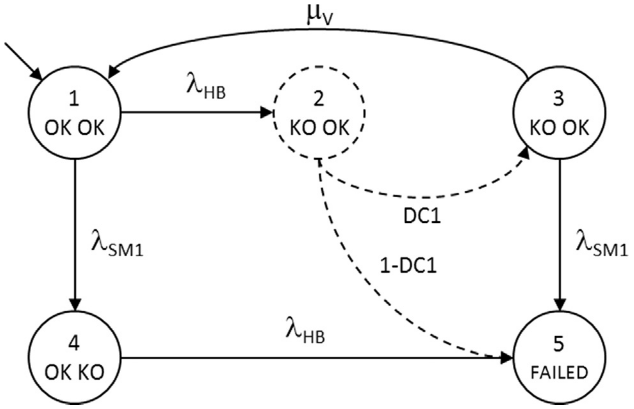

Fig. 3. Generic Markov chain for a hardware block protected by a first order safety mechanism based on error detection.

Finally, if, in the initial state, the safety mechanism fails before the hardware block fails, then the system goes to state (4). In this state, we have nothing to do but to wait until the hardware block fails to go into the failure state (5) (third failure scenario).

Note that since there is no mean to detect a failure of the safety mechanism, there is no mean to repair it neither. Moreover, we assume that neither the hardware block nor the safety mechanism is inspected during periodic maintenances of the vehicle. This hypothesis is realistic, although pessimistic.

3.2. Case of a hardware block protected by first order mechanism based on error detection and a second order safety mechanism

We shall consider now the case of a hardware block HB protected with a first order safety mechanism SM1 based on error detection which is itself tested by a second order safety mechanism each time the vehicle starts. The generic Markov chain for such a system is given in Fig. 4.

This model extends the previous one. The second order mechanism has its own failure rate λ_{SM2} as well as its own diagnostic coverage DC2. Note that it is assumed that when the vehicle is taken to the garage, it is fully repaired and is as good as new after this repair.

In the initial state (0), the hardware block HB and the two safety mechanisms SM1 and SM2 are assumed to work correctly. Now there are three possibilities:

- The second order mechanism fails first. In that case, according to our hypotheses, we are exactly in the same situation as if there was no second order mechanism. So the model obeys the same pattern as previously. We kept actually the same numbering of states 1–5 to emphasize this point.
- The hardware block fails first. This situation is also very similar to the previous one, for the second order mechanism plays no specific role in the subsequent scenarios. State 0, 6 and 7 are therefore symmetric to states 1, 2 and 3. The only difference stands in the availability of the second order mechanism.

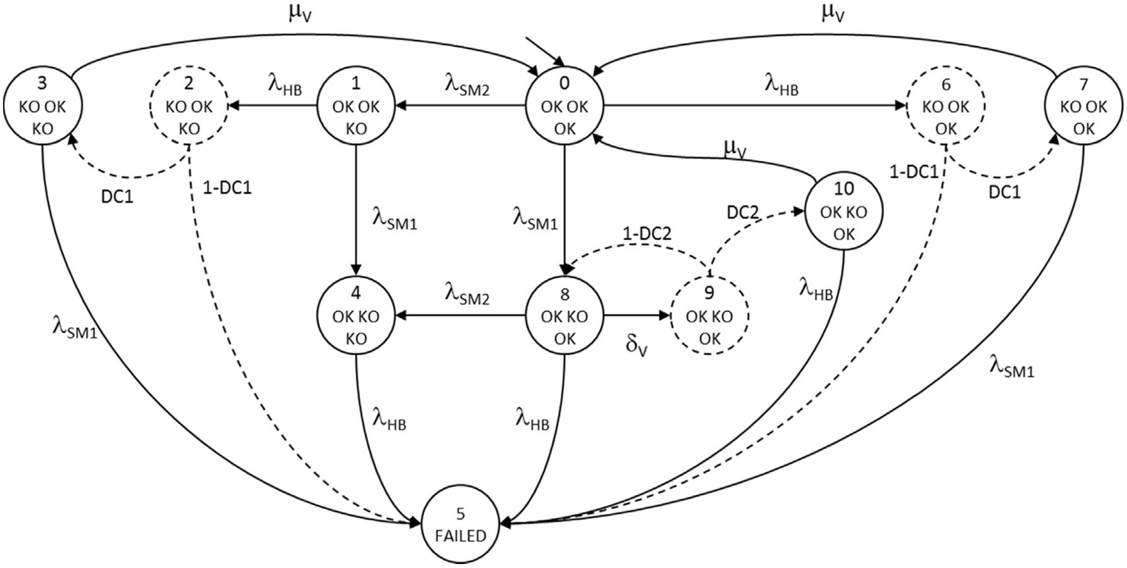

Fig. 4. Generic Markov chain for a hardware block protected by a first order safety mechanism based on error detection and a second order safety mechanism.

- The interesting scenarios are therefore those where the first safety mechanism fails first, i.e. the system goes to state 8. We shall now develop these scenarios.

In state 8, we are in the situation where the first order safety mechanism failure is unnoticed. Here again there is a race condition amongst three possibilities:

- The hardware block fails first, including before the current journey ends. In that case, the whole system fails (state 5).
- The second order safety mechanism fails first. In that case, we can make the pessimistic assumption that the driver did not notice the warning before this failure. So, we are back to the situation where there is no second order safety mechanism (and the first order one is failed), i.e. to state 4.
- The current journey ends before both the hardware block and the second order mechanism fail (state 9). We can assume that the mean time before the journey ends is T_J so that the transition rate between states 8 and 9 is $\delta_V = 1/T_J$. Now at the next start of the vehicle, the second order mechanism tests the first order one with a probability DC2 of successful detection. If the detection is successful (state 10) then either the driver takes the vehicle to the garage before the hardware block fails (in which case the system goes back to the initial state 0) or the hardware block fails first (in which case the whole system fails, i.e. goes to state 5). If the second order mechanism does not detect the failure of the first order one, then we have to wait for another start of the vehicle to make the test again (so the system goes back to state 8)

It is worth to note that the model described here is quite different from those proposed for safety instrumented systems in Refs. [3,4]. The difference stands mainly in assumptions about the maintenance policy. As already pointed out, the designer of an automotive electric and electronic system has no control on maintenance. So, he has to make pessimistic hypotheses about what the driver will (reasonably) do.

3.3. Case of a hardware block protected by a first order safety mechanism based on inhibition and a second order safety mechanism

We shall now consider the case of a hardware block HB protected with a first order safety mechanism SM1 that inhibits the hardware block functionality, itself periodically tested by a second order safety mechanism SM2. The generic Markov chain for such a system is given in Fig. 5. As the reader has immediately noticed, this model is embedded in the previous one. The reason is that if the hardware block fails before the first order safety mechanism, then there is nothing to inhibit and the system is safe (but of course not available).

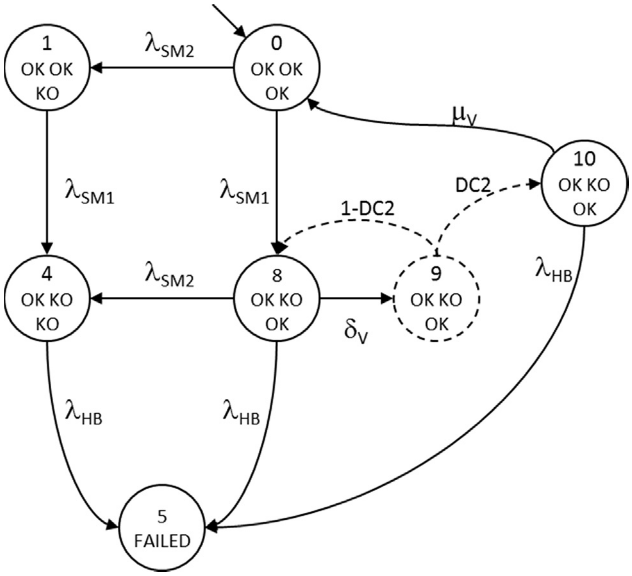

Fig. 5. Generic Markov chain for a hardware block protected by a first order safety mechanism based on inhibition and a second order safety mechanism.

Note also that there is no detection device and therefore no diagnostic coverage for the first order safety mechanism.

4. Experimental study

Once the modeling of prototypical electric and electronic systems was established on the solid ground of the Markov chains presented in the previous section, we were in position to study the sensitivity of their safety to the variations of their reliability parameters. This section reports experiments we made on the model pictured in Fig. 4, which is the most general one. To do so, we used the XMRK tool developed by one of the authors [5].

4.1. Realistic values of the parameters

In practice, mission times, transition rates and diagnostic coverage's are by no means arbitrary. They vary within bounds from one system to the other but this variation is rather limited.

The considered lifetime of a vehicle is about 10,000 driving hours. This corresponds to an average of 15 years or 400 thousand kilometers (660 h of driving per year, with an average speed of 40 km/h). We performed most of the calculations for this value. In this section, we present results up to 20,000 h lifetime to give the reader more insight about how the indicators evolve.

The failure rate of hardware blocks (λ_{HB}) stands typically between 10^{-6} and 10^{-7} failures per hour. The failure rates of first and second order safety mechanisms (λ_{SM1} and λ_{SM2}) stand typically between 10^{-6} and 10^{-8} failures per hour. We made most of the experiments around these values which corresponds to the failure rates ranges of the majority of the automotive components extracted from IEC 62380 [12].

ISO 26262 annex D clarifies the evaluation of diagnostic coverage of safety mechanisms. Different tables are proposed in order to identify the type of safety mechanism that allows the detection of specific element failures. It also associates to each of those combinations the expected diagnostic coverage value, which represents the effectiveness of a safety mechanism with respect to the different failures modes [1]. The diagnostic coverage is typically sorted into three ranks: Low (60%), Medium (90%) and High (99%). However, these values can be adapted based on the analysis of the component or with the expert judgment in order to take into account specific characteristics such as specific implementations constraints or specific test periodicity. Also, a 100% diagnostic coverage can be considered if it can be justified. In practice, as it relies on the expert judgment, it's very unlikely to have a diagnostic coverage percentage with more than one or two decimal digits (e.g. 99.5%, 99.95%).

The mean journey time ($T_J = 1/\delta_V$) is of course more difficult to estimate. It is usually taken as to be 1 h. We made it vary from this value to larger values to take into account a large variety of situations.

Similarly, the mean time before the vehicle is taken to the garage when a warning is raised ($T_M = 1/\mu_V$) depends dramatically on the driver. We made it vary also from 1 h (i.e. the journey mean time) to the lifetime of the vehicle. Here again the ISO26262 standard provides typical values (Part 5, requirement 9.4.2.3, note 2) of the average time to vehicle repair, depending on the fault type:

- 200 vehicle trips for reduction of comfort features;
- 50 vehicle trips for reduction of driving support features;
- 20 vehicle trips for amber warning lights or impacts on driving behavior; and
- one vehicle trip for red warning lights.

The time taken for repair is usually not considered (except to evaluate hazards that can expose maintenance personnel).

Table 1 summarizes realistic variations of the values of parameters.

In the case of the Vehicle Management Unit presented Section 2.1, the per hour failure rate of the hardware block, i.e. the torque calculation part of the microcontroller has an estimated value of 0.4E-6. This estimation results from the weighting of failure probabilities and rates of different constituent of the microcontroller. The per hour failure rate of the watchdog is estimated at 5.0E-8. The diagnostic coverage of the watchdog is estimated from its capacity to detect different failure modes of the microcontroller and the proportion of failures of each mode. For a simple watchdog it would be around 60%, for a more elaborated watchdog (so-called window watchdog) it would be around 90%. The per hour failure rate and diagnostic coverage of the second order mechanism are estimated respectively at 0.4E-6 and 60%.

Table 1
Typical values of parameters.

	Lower bound	Higher bound		Lower bound	Higher bound
λ_{HB}	1E-07	1E-06	λ_{SM2}	1E-08	1E-06
λ_{SM1}	1E-08	1E-06	DC2	0%	100%
DC1	0%	100%	$T_M = 1/\mu_V$	1	10,000
$T_J = 1/\delta_V$	1	10			

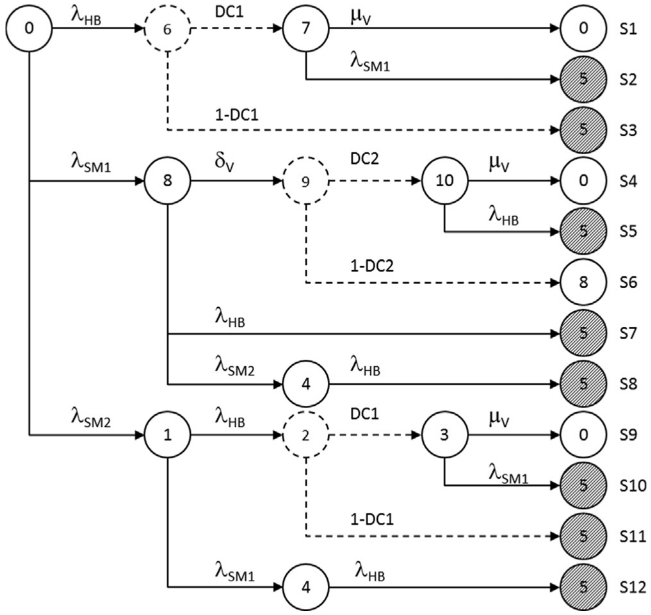

Fig. 6. Unfolded view of the Markov chain representing hardware block protected with a first and second order mechanisms based on error detection.

4.2. Most influential parameters

According to numbers given in Table 1, the hardware block and both safety mechanisms are reliable with respect to the expected mission time of vehicle. As a consequence, scenarios involving more than one or two failures of these components are extremely improbable. Although the Markov chain pictured Fig. 4 encodes an infinite number of failure sequences, only the shortest ones are of real interest. Fig. 6 presents an unfolded (tree-like) view of this Markov chain. Sequences that go back to an already visited state are not expanded so to keep only shortest sequences.

Fig. 6 makes clear that all of the failure sequences involve the failure of the hardware block. Therefore, its failure rate is an influential parameter. To illustrate this point, we calculated the probability of failure of the system for different values of λ_{HB} (λ_{HB}=1.00E-6, 0.80E-6, 0.60E-6, 0.40E-6, and 0.20E-6 h^{-1}) and fixed values of the other parameters: λ_{SM1}=1.00E-6 h^{-1}, DC1=99%, λ_{SM2}=1.00E-6 h^{-1}, DC2=99%, T_J=1 h, and T_M=10 h. We made these calculations from 0 h to 20,000 h by step of 100 h. Values of the failure probability of the system are plotted Fig. 7. This figure shows that the dependence of the failure probability w.r.t. the failure rate of the hardware block is quasi-linear. We observed such

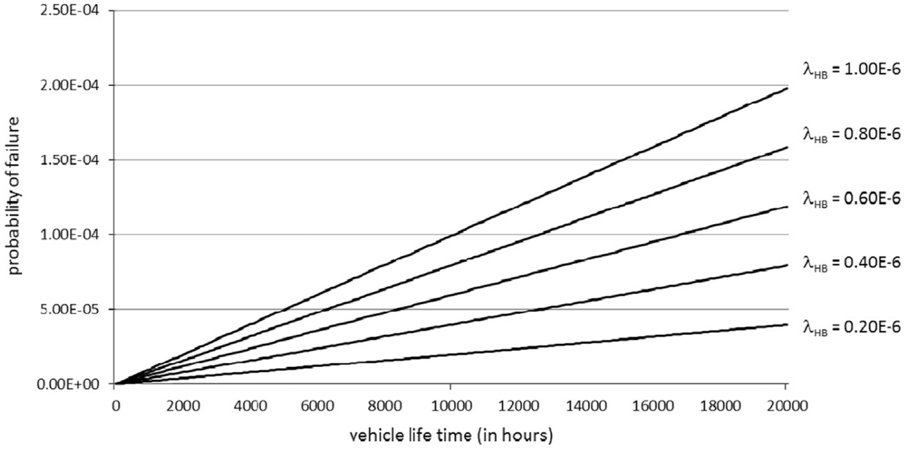

Fig. 7. Variations, mutatis mutandis, of the failure probability with respect to the failure rate λ_{HB} of the hardware block (with $\lambda_{SM1}=1.00E\text{-}6\ h^{-1}$, DC1 = 99%, $\lambda_{SM2}=1.00E\text{-}6\ h^{-1}$, DC2 = 99%, $T_J=1$ h, $T_M=10$ h).

Table 2
Quotient of the probability of failure divided by λ_{HB} for different mission times.

	Vehicle life time (h)			
	5000	10,000	15,000	20,000
λ_{HB}				
1.00E-6	49.89	99.54	148.97	198.19
0.80E-6	49.89	99.54	148.97	198.19
0.60E-6	49.89	99.54	148.97	198.19
0.40E-6	49.89	99.54	148.97	198.19
0.20E-6	49.89	99.54	148.97	198.19

a quasi-linear dependence for other realistic values of the other parameters.

Table 2 gives the quotient of the failure probability by λ_{HB} for different times (and different values of λ_{HB}). These numbers confirm our quasi-linearity hypothesis.

We performed similar experiments to determine the influence of the diagnostic coverage DC1 of the first order mechanism on the failure probability. We let DC1 vary (DC1 = 95%, 96%, 97%, 98%, 99%) while the other parameters are fixed ($\lambda_{HB}=1.00E\text{-}6$, $\lambda_{SM1}=1.00E\text{-}6$, $\lambda_{SM2}=1.00E\text{-}6$, DC2 = 99%, $T_J=1$ h, $T_M=10$ h) and we computed the failure probability from 0 h to 20,000 h by step of 100 h (although this value is twice higher than the vehicle lifetime, it allows a better visualization and interpretation of the different behaviors). Results are plotted Fig. 7. This figure shows clearly the direct influence of this parameter on the failure probability. Again, similar results are obtained for different values of the other parameters.

4.3. Influence of other parameters

We established so far that both the failure rate of the hardware block and the diagnostic coverage of the first order mechanism have a direct and quasi-linear influence on the failure probability of the whole system. What about the other parameters?

Fig. 6 makes clear that sequences S9, S10, S11 and 12 are obtained respectively by prefixing sequences S1, S2, S3 and S7 with a failure of the second order mechanism (λ_{SM2}) and that sequence S8 is obtained from sequence S7 by inserting a failure of the second order mechanism in between the failure of the first order mechanism one and the failure of the hardware block. Moreover, the failure of the second order mechanism occurs only in sequences S8, S9, S10, S11 and S12.

As a consequence, the failure rate of the second order mechanism cannot greatly influence the probability of failure of the system.

There are two possibilities here: either we consider a perfect or nearly perfect diagnostic coverage of the first order mechanism, or we consider an imperfect (although possibly quite good) one.

If the diagnostic coverage is not perfect, it turns out that the other parameters have a minor role in the determination of the failure probability. The failure probability comes almost exclusively from the scenario: failure of hardware block (state 0 to state 6), non-detection of this failure (state 6 to state 5). As an illustration consider the four following extreme cases (see Fig. 8).

- Case 1: both the first order and the second safety mechanisms are highly reliable ($\lambda_{SM1}=\lambda_{SM2}=1.0E\text{-}8$), the second order mechanism detects perfectly the failures of the first one (DC2 = 100%) and the driver takes immediately the vehicle to the garage when she is advised to do so ($T_M=1$ h).
- Case 2: Similar to case 1, but with a passive driver who never takes the vehicle to the garage ($T_M=20{,}000$ h).
- Case 3: the first order safety mechanism is only reasonably good ($\lambda_{SM1}=1.0E\text{-}6$) and the second order mechanism is ineffective (DC2 = 0, $T_J=20000$ h). The driver is active ($T_M=1$ h).
- Case 4: similar to case 3, but with a passive driver ($T_M=20{,}000$ h).

In all of the cases, we took $\lambda_{HB}=1.0E\text{-}6$.

As shown by Fig. 9, the probability of failure of the worst case (case 4) is less than three times as much as the probability of failure of the best one (case 1) after 20,000 h and only two times this probability after 10000 h (the expected life time of a vehicle).

If the first order safety mechanism is highly reliable ($\lambda_{SM1}=1.0E\text{-}8$), the driver behavior has not much influence. If it is only reasonably reliable ($\lambda_{SM1}=1.0E\text{-}6$), the driver behavior has some influence.

With a smaller value diagnostic coverage of the first order safety mechanism, e.g. DC1 = 90%, the differences between the above test cases are negligible. The situation is rather different in the case of a perfect or nearly perfect diagnostic coverage of the first order mechanism. First, the failure rate of the first order mechanism comes into the play, second the behavior of the driver has a great influence especially in the case the first order mechanism is highly reliable, as illustrated Table 3.

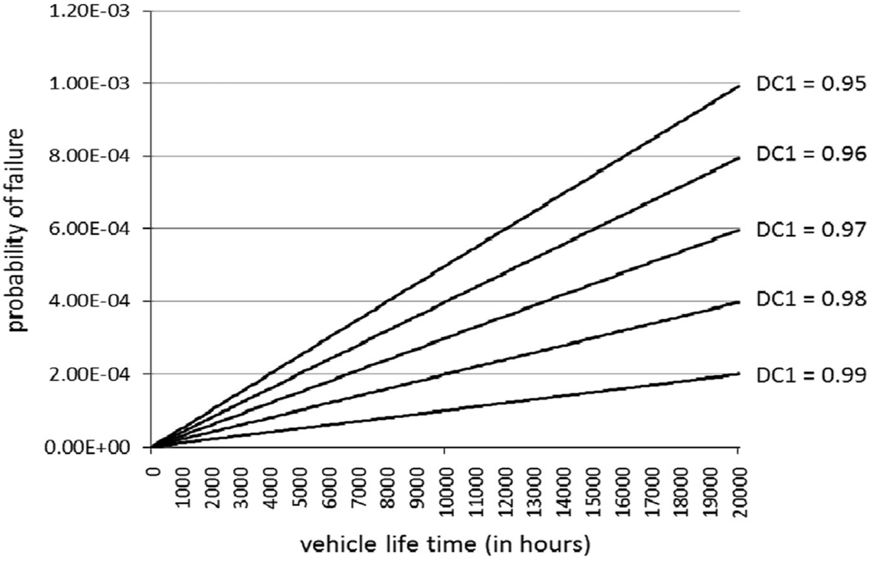

Fig. 8. Variations, mutatis mutandis, of the failure probability with respect to the diagnostic coverage DC1 of the first order safety mechanism.

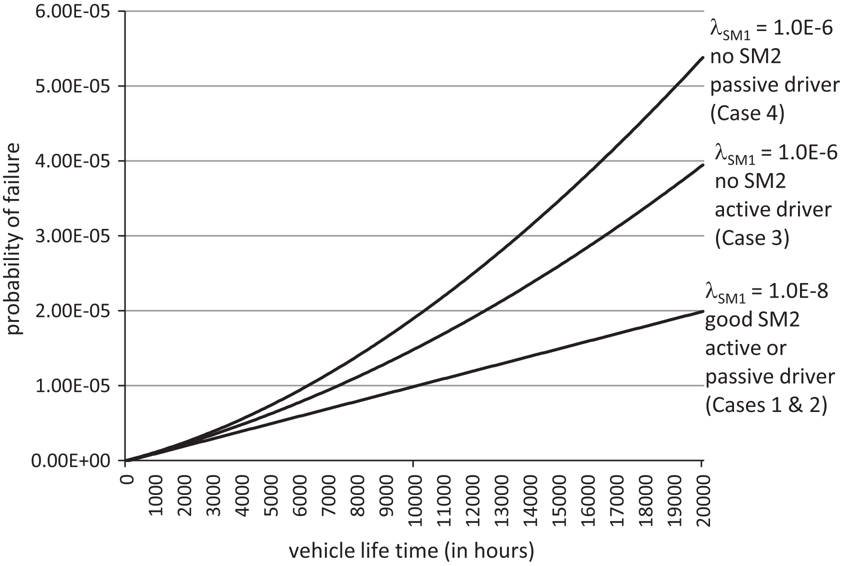

Fig. 9. Influence of other parameters (but λ_{HB}=1.0E-6) in case of an imperfect diagnostic coverage of the first order mechanism (DC1=99%).

Table 3
Influence of other parameters (but λ_{HB}=1.0E-6) in case of a perfect diagnostic coverage of the first order mechanism (DC1=100%).

	Vehicle life time (h)			
	5000	10,000	15,000	20,000
λ_{SM1}=1.0E-8, T_M=1 h	1.49E-11	3.13E-11	5.02E-11	7.28E-11
λ_{SM1}=1.0E-8, T_M=20,000 h	2.22E-08	8.36E-08	1.76E-07	2.92E-07
λ_{SM1}=1.0E-6, T_M=1 h	1.25E-06	4.98E-06	1.12E-05	1.98E-05
λ_{SM1}=1.0E-6, T_M=20,000 h	2.40E-06	9.21E-06	2.00E-05	3.44E-05

4.4. Wrap-up

The large experimental study we performed showed that, within the bounds set up by the current technologies, the two most influential reliability parameters are the failure rate of the hardware block and the diagnostic coverage of the first order safety mechanism. In a case of a perfect diagnostic coverage of the first order mechanism, the failure rate of the first order mechanism and the driver behavior have a significant impact on the reliability of the system. In all of the cases, the reliability of the second order mechanism has only a minor influence.

5. Related works

As we said in the introduction, the design of Markov models for safety systems has been done for the type of systems the mother standard IEC 61508 [2] is dealing with (see e.g. [3,4]). Such a work has not been done yet for automotive safety mechanisms.

In their works, Zhang, Long and Sato [6] propose models for the representation of multi-channels safety related systems. The Markov models proposed in this paper take into account two kinds of failure: the self-detected ones and the undetected ones. This can be compared to the safety mechanisms diagnostic coverage in this paper. Their models also take into account a “down time” parameter which can be assimilated to the exposure time introduced in ISO 26262 and which is taken into account in our models.

In another article, Yoshimura, Sato and Suyama propose a Markov model to calculate the failure probability of a system without self-diagnostic by taking into account dynamic demand rates [7]. Holub and Borcsok enhanced this model by adding the support of the self-diagnostic allowing to distinguish the dangerous detected failures from the undetected ones [8].

In their study, Winkovich and Eckardt propose Markov models to evaluate the failure probability of the IEC 61508 related systems. The models proposed in this paper take into account block equipped with self-test mechanism, each of them characterized by a self-test period and a diagnostic coverage percentage. However, unlike our models, the proposed models do not take into account the possibility of self-test mechanisms failures [9].

6. Conclusion

In this article, we proposed Markov chains that model the behavior of a large class of automotive Electric and Electronic systems protected by first and possibly second order safety mechanisms. These Markov chains are generic in the sense that the analyst has just to set up the values of parameters such as failure rates and diagnostic coverage to assess a particular system. We report experiments we made to determine the most influential of these parameters.

These Markov chains can serve as reference models for the systems the ISO 26262 standards deal with. Together with our findings on the relative influence of the different parameters, they make it possible to propose approximate models, such as fault trees patterns or ad-hoc formulas. The determination of fault tree patterns is of a special interest for most of the analysts are familiar with this technology. We are currently working on this issue.

Another promising idea would be to combine the Markov chains we propose here with the ones modeling other components in order to model a whole automotive system (not only an individual electric and electronic system). Of course, the resulting Markov chain would be gigantic even for a relatively small number of components. It is however possible to generate partial Markov chains (typically from AltaRica descriptions, see e.g. [10]) that provide excellent approximations for the failure probability, as recently demonstrated in [11].

References

[1] ISO 26262. Road vehicles – Functional safety. Working Group ISO TC22 SC3; 2011.

[2] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems, parts 1–7. Geneva: International Electrotechnical Commission; 1998.

[3] Innal F F, Dutuit Y, Rauzy A, Signoret J-P. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. J Risk Reliab 2010;224:75–86 (July).

[4] Jin H, Lundteigen M-A, Rausand M. Reliability performance of safety instrumented systems: a common approach for both low- and high-demand mode of operation. Reliab Eng Syst Saf 2011;96:365–73.

[5] Rauzy. A. An experimental study on six algorithms to compute transient solutions of large Markov systems. Reliab Eng Syst Saf, 86. Elsevier; 2004; 105–115.

[6] Zhang T, Long W, Sato Y. Availability of systems with self-diagnostic components – applying Markov model to IEC 61508-6. Reliab Eng Syst Saf 2003;80:133–41.

[7] I Yoshimura, Y Sato K Suyama. Safety-Integrity Level model for safety-related systems in dynamic demand state. In: Proceedings of Asian International Workshop on Advanced Reliability Modeling, 2004; pp. 577–84.

[8] P Holub, J Borcsok. Advanced PFH calculations for safety integrity systems with high diagnostic. Symposium on Information, Communication and Automation Technologies; 2009.

[9] T. Winkovich, D. Eckardt. Reliability analysis of safety systems using Markov-chain modelling. In: Proceedings of the European Conference on Power Electronics and Applications, Dresden, Germany, 2005; pp 10–20. ISBN 90-75815-09-3.

[10] Boiteau M, Dutuit Y, Rauzy A, Signoret J-P. The AltaRica data-flow language in use: assessment of production availability of a multistates system. Reliab Eng Syst Saf 2006;91(7):747–55.

[11] P-A Brameret, A Rauzy, JM Roussel. Preliminary System Safety Analysis with Limited Markov Chain Generation. In: Proceedings of 4th IFAC Workshop on Dependable Control of Discrete Systems, DCDS 2013, York (Great Britain); September, 2013.

[12] IEC 62380. Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment. International Electronic Commission; 2004.