Comparison of Analytical Formulas of PFH and PMHF Calculation for M-out-of-N Redundancy Architecture

Elena Rogova[1], Christian Nowak[2], Matthias Ramold[3], Udo Steininger[4]

TÜV SÜD Rail GmbH, Germany.
[1]E-mail: elena.rogova@tuev-sued.de
[2]E-mail: christian.nowak@tuev-sued.de
[3]E-mail: matthias.ramold@tuev-sued.de
[4]E-mail: udo.steininger@tuev-sued.de

The international functional safety standard for road vehicles ISO 26262 proposes to use probabilistic metric for random hardware failures (PMHF) as a quantitative way to estimate probability of random hardware failures violating the safety goal. The example of calculation of PMHF is presented in ISO 26262. However, the standard does not contain an analytical formula of PMHF calculation for M-out-of-N redundancy architecture. This formula can find an important application in drive-by-wire systems where the question of redundancy and calculation of probabilistic metrics of redundant architectures is especially relevant. In this paper the formula of PMHF calculation for M-out-of-N redundancy architecture has been developed and compared with the formula of average frequency of dangerous failures per hour (PFH) which is defined in the international functional safety standard IEC 61508 for safety systems in high- and continuous demand mode. Comparative analysis presented in this paper, demonstrates that PFH and PMHF formulas give similar results for different case studies. These case studies are investigated by considering different types of failures defined in IEC 61508 and in ISO 26262.

Keywords: PMHF, PFH, redundancy, ISO 26262, IEC 61508, drive-by-wire.

1. Introduction

The standard ISO 26262 (2018) presents the requirements in functional safety for road vehicles. The origin of this standard is the international functional safety standard IEC 61508. IEC 61508 can be classified as a "probabilistic" standard, where calculation of probability of failure on demand (PFD) or average frequency of dangerous failures per hour (PFH) is required for safety systems (IEC 61508, 2010). In comparison, the standard ISO 26262 does not strictly require probabilistic calculations and provides a choice between two methods: 1) calculation of PMHF (Probabilistic Metric for random Hardware Failures), and 2) method of evaluation of each cause of safety goal violation (ISO 26262-5, 2018).

IEC 61508 and ISO 26262 ask for calculation of different probabilistic values which involve different types of failures. Therefore, it is interesting to conduct a comparative analysis of PFH and PMHF formulas for different types of failures and to clarify similarities and differences. For conducting comparative analysis of PFH and PMHF, the new analytical formulas of PMHF calculation for M-out-of-N (MooN) redundancy architecture have been proposed in this paper due to the lack of such formulas in ISO 26262.

The literature research shows some attempts to obtain PMHF formulas for redundant systems. However, these works focus mainly on the case study for redundancy architecture with two channels (Kleyner and Knoell, 2018), (Sakurai, 2018). There are different works that present quantitative techniques for estimation of PMHF. Mainly, PMHF calculation is conducted by using fault tree analysis as presented by Das and Taylor (2017).

There are a few reasons of lack of an analytical formula of PMHF calculation for M-out-of-N redundancy architecture:

(i) Redundant systems are not commonly in use in conventional automotive systems;
(ii) Comparing to IEC 61508, ISO 26262 uses other types of faults and failures. It is difficult to take into account all possible scenarios in one analytical formula of PMHF for MooN redundancy architecture.

This paper does not have a goal to develop a generalized formula of PMHF calculations: it mainly focuses on understanding the differences and similarities between PFH in the concept of IEC 61508 and PMHF in the concept of ISO 26262, and development of a simplified PMHF formula for MooN redundancy architecture with identical channels.

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0185-cd

2. IEC 61508 and ISO 26262: different types of failures

As was mentioned in the Introduction, IEC 61508 and ISO 26262 define different types of failures. For instance, IEC 61508 defines: dangerous, safe, no effect and no part failures. Dangerous failures (D) are divided into dangerous detected (DD) and dangerous undetected (DU). Detected failures are failures that are detected by the diagnostics with a certain diagnostic coverage. Undetected failures are failures which cannot be detected by a diagnostic system:

$$\lambda_{DD} = DC\lambda_D, \quad (1)$$

$$\lambda_{DU} = (1 - DC)\lambda_D$$

Failures which are taken into account in formulas of calculation of PFD and PFH in IEC 61508 are considered to be random failures. Contribution of common cause failures is included in PFH and PFD formulas by using a common cause (beta) factor. Some systematic failures are quantified through the modelling of common cause failures (Lundteigen and Rausand, 2007). In the formula of PMHF in ISO 26262, only random hardware failures are considered: systematic and common cause failures are not estimated quantitatively. Random hardware failures are divided into a few groups: single-point failures (SPF), residual failures (RF), multiple-point failures (MPF), dual-point failures (DPF) - partial case of MPF. These failures can be classified into dangerous undetected and dangerous in terms of IEC 61508, as presented in Fig.1:

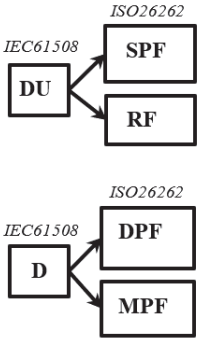

Fig.1. Classification of dangerous failures in ISO 26262 and in IEC 61508.

Safe faults are not considered in the analysis because as defined in ISO 26262, their "occurrence will not significantly increase the probability of violation of a safety goal" (ISO 26262-1, 2018).

In the classification proposed in Fig.1, SPF and RF are always undetected failures. There are no safety mechanisms to detect SPF. RF is a portion of a random hardware fault which is not controlled by a safety mechanism (ISO 26262-1, 2018). DPF and MPF can be detected by a safety mechanism ("sm"). However, if multiple-point fault is not detected, it is called latent fault (LF). Therefore, SPF and RF are always undetected failures, and DPF and MPF can contain both – detected and undetected part.

If the nature of single point and residual failures is clear and similar to the nature of dangerous undetected failures in the concept of IEC 61508, multiple-point failures (MPF) and dual-point failures (DPF) do not have analogues in IEC 61508. As explained in ISO 26262-1, multiple-point failure is a "failure, resulting from the combination of several independent hardware faults, which leads directly to the violation of a safety goal" (ISO 26262-1, 2018). DPF is a partial case of MPF of order 2.

It is interesting to consider a system which consists of a mission block ("m") and a safety mechanism ("sm"). Both "m" and "sm" can fail. If a mission block will fail, safety mechanism will detect a failure and prevent violation of a safety goal. However, if safety mechanism fails first, there is no direct violation of a safety goal, but there is a loss of diagnostic. In this case it is difficult to make a comparison, which type of fault it is in terms of IEC 61508. The most conservative answer is a dangerous undetected fault due to a fault of "sm". However, it is not completely correct because the mission block itself did not fail, it just lost its diagnostic. Due to these differences in terminology and nature of faults and failures in concept of IEC 61508 and ISO 26262, comparative analysis of PFH and PMHF formulas is ambiguous and can be conducted only for the case studies.

3. PMHF formula for M-out-of-N redundancy architecture

As stated in ISO 26262, PMHF shall be expressed in terms of average probability of failure per hour over the operational lifetime (ISO 26262-5, 2018) as presented in Eq. (2):

$$PMHF = \frac{P_{avg}}{T_{Lifetime}} \quad (2)$$

For obtaining the PMHF formula for M-out-of-N redundancy architecture let us assume that there are only dangerous hardware failures (without distinction between SPF, RF, DPF and MPF). Assuming that 0 or 1 dangerous group failure can occur during $T_{Lifetime}$, M-out-of-N system will fail

with probability presented in Eq. (3), which represents also a mean number of group failures (Rogova et al., 2017):

$$\Pr\left(V\left(T_{Lifetime}\right) \geq N-M+1\right) = \sum_{j=N-M+1}^{N} \Pr\left(V\left(T_{Lifetime}\right) = j\right) \quad (3)$$

where $V(T_{Lifetime})$ is a certain number of channels that will fail during the operational lifetime interval. This number is binomially distributed (Rausand, 2014) and can be expressed as following:

$$P_j = \Pr\left(V\left(T_{Lifetime}\right) = j\right) = \binom{N}{j}\left(1 - e^{-\lambda_D T_{Lifetime}}\right)^j \cdot \left(e^{-\lambda_D T_{Lifetime}}\right)^{N-j} \quad (4)$$

Taking into account that MooN architecture will have a dangerous group failure if at least *N-M+1* of the N channels will have dangerous faults during $T_{Lifetime}$, Eq. (5) can be obtained:

$$\mathrm{PMHF}^{MooN} = \frac{P_{avg}}{T_{Lifetime}} = \frac{1}{T_{Lifetime}} \cdot \sum_{j=N-M+1}^{N} \binom{N}{j}\left(1 - e^{-\lambda_D T_{Lifetime}}\right)^j \cdot \left(e^{-\lambda_D T_{Lifetime}}\right)^{N-j} \quad (5)$$

Applying a set of approximations (Rogova et al., 2017), for small $\lambda_D T_{Lifetime}$:

$$\left(\lambda_D T_{Lifetime}\right)^{j+1} \ll \left(\lambda_D T_{Lifetime}\right)^j \text{ for all } j \geq 1 \quad (6)$$

This gives:

$$\mathrm{PMHF}^{MooN} = \frac{1}{T_{Lifetime}} \cdot \sum_{j=N-M+1}^{N} \Pr\left(V\left(T_{Lifetime}\right) = j\right) \approx \frac{\Pr\left(V\left(T_{Lifetime}\right)=N-M+1\right)}{T_{Lifetime}} \quad (7)$$

To further simplify, the following approximations are introduced:

$$1 - e^{-\lambda_D T_{Lifetime}} \approx \lambda_D T_{Lifetime}$$
$$e^{-\lambda_D T_{Lifetime}} \approx 1 \quad (8)$$

Therefore, PMHF for MooN redundancy architecture:

$$\mathrm{PMHF}^{MooN} = \binom{N}{N-M+1} \cdot \lambda_D{}^{(N-M+1)} \cdot T_{Lifetime}^{N-M} \quad (9)$$

Corresponding PFH formula can be presented as follows (Rogova et al., 2017):

$$\mathrm{PFH}^{MooN} = \binom{N}{N-M+1} \cdot \lambda_D{}^{(N-M+1)} \cdot \tau^{N-M} \quad (10)$$

where τ is a proof test interval in case of regular proof testing.

Eq. (9) is similar to Eq. (10) if the following conditions are met for both PFH and PMHF formulas:

(i) failure rate of all dangerous failures is λ_D (without distinguishing between DD and DU in the concept of IEC 61508, and between SPF, RF, DPF and MPF in the concept of ISO 26262);
(ii) proof test interval τ in PFH formula is equivalent to the operational lifetime interval $T_{Lifetime}$ in PMHF formula;
(iii) system is non-repairable;
(iv) channels are identical and independent.

Table 1 presents PMHF values for different MooN architectures obtained by using Eq. (9):

Table 1. PMHF formulas for several MooN architectures.

MooN	*PMHF*
1oo1	λ_D
1oo2	$\lambda^2_D \cdot T_{Lifetime}$
2oo2	$2\lambda_D$
1oo3	$\lambda^3_D \cdot T^2_{Lifetime}$
2oo3	$3\lambda^2_D \cdot T_{Lifetime}$
3oo3	$3\lambda_D$

It is important to understand, which failures are included in λ_D. In terms of IEC 61508, λ_D in obtained PMHF formula (Eq.9) includes both – dangerous detected DD and dangerous undetected DU failures. In terms of ISO 26262, λ_D in the formula includes dangerous undetected failures (SPF and RF) and dangerous detected failures with undetected part (DPF or MPF). However, if redundancy architecture MooN is not 1oo1 (one single channel), SPF+RF→0. SPF and RF are failures which directly (by themselves) lead to the violation of a safety goal and not controlled by any safety mechanism (ISO 26262-1, 2018). In case of redundancy, failure of one channel by itself cannot violate a safety goal: it is necessary to have a combination of faults from the other channels. Therefore, contribution from SPF and RF can be neglected for MooN, if M>1.

3.1 *Case studies*

As was mentioned above, single-point and residual failures do not contribute to the PMHF value of MooN redundancy architecture if M>1. Therefore, 1oo1 system is excluded from the analysis in this section. Failure of MooN system is caused by multiple-point failures (dual-point failures in case of two channel redundancy architecture). In this section two case studies are considered. Fig.2 represents these case studies on the example of redundancy architecture with two channels (1oo2).

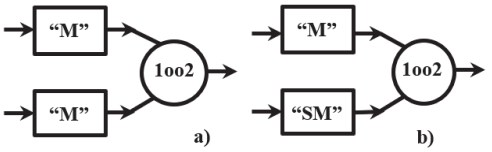

Fig. 2. 1oo2 architectures with MPF.

Let us consider the first case study (a) when MooN system (M>1), does not have any safety mechanisms (Fig. 2a). In this case, each channel is considered as a "mission block" which performs a mission function. Therefore, Eq. (9) can be presented as follows:

$$\mathrm{PMHF}^{MooN} = \binom{N}{N-M+1} \cdot \lambda_{m,MPF}{}^{(N-M+1)} \cdot T_{Lifetime}^{N-M} \quad (11)$$

where $\lambda_{m,MPF}$ is a multiple-point failure rate of the mission block "m".

The case study (b) considers the MooN architecture (M>1) where one channel contains a mission block, and the other channels are safety mechanisms. This is presented on Fig. 2b on the example of 1oo2 architecture where safety mechanism has a redundant mission function. Taking into account the limitations of our model (identical channels), failure rates of a mission block and safety mechanisms are the same and equal to:

$$\lambda_{m,MPF} = \lambda_{sm,MPF} = \lambda_{MPF} = \lambda_D \quad (12)$$

Therefore, PMHF formula obtained for this case study will be the same as presented in Eq. (11). It is important to mention, that detected multiple-point failure rate of the safety mechanism "sm" is neglected here.

A PMHF formula for two channel redundancy architecture with different channels was obtained by Sakurai (Sakurai, 2018). Generalized PMHF formula for MooN redundancy architecture with non-identical channels will be very elaborate. Eq. (13) presents the PMHF formula for two channel redundancy architecture with non-identical channels. In addition to the primary safety mechanism (which performs a redundant mission function), Sakurai considers also secondary safety mechanisms (for prevention of latent faults) (Sakurai, 2018). In this section the formula developed by Sakurai is adapted for the case study presented in Fig. 2b, bearing in mind that it does not have secondary safety mechanisms for "M" and "SM":

$$\mathrm{PMHF}^{1oo2} = \frac{1}{2} \cdot \lambda_{m,MPF}\lambda_{sm,MPF} \cdot T_{Lifetime} + \frac{1}{2} \cdot \lambda_{m,MPF}\lambda_{sm,MPF} \cdot T_{Lifetime} \quad (13)$$

Taking into account that for identical channels failure rates are equal, as presented in Eq. (12), Eq. (13) can be transformed to Eq. (14), which presents the value of PMHF for 1oo2 architecture with identical channels:

$$\mathrm{PMHF}^{1oo2} = \lambda_D^2 \, T_{Lifetime} \quad (14)$$

PMHF value presented in Eq. (14) is equal to the value obtained by Eq. (9) for 1oo2 architecture with identical channels (see Table 1 for 1oo2).

The case study (b) represents a redundancy architecture with diagnostics. It is important to note that this case study, as well as case study (a), is not limited by two channels architecture presented on Fig. 2.

The main difference between considered architectures (a) and (b) is a diagnostics. Case study (a) does not have a diagnostics. The voter decides which channel(s) will be chosen to continue an operation (in case of a fail-operational system) or to shut down and to go to a safe state (in case of a fail-safe system), based on comparison of signals. For autonomous driving systems, shutdown is not an acceptable solution, and a system still needs to continue operation even after a fault occurs.

Case study (b) contains a diagnostics implemented in safety mechanism(s). Therefore, the voter can make a decision based on diagnostic information, and not only based on comparison of signals coming from channels like in the case study (a).

4. Conclusion

Comparative analysis of PFH and PMHF formulas has been conducted in this paper for different case studies. Equal results were proved in case of the lack of safety mechanisms (case study (a)). If a mission block and safety mechanisms with redundant mission function are implemented in a system with MooN architecture, case study (b) gives the same results as in the case study (a) in the assumption that safety mechanisms and mission block are equal. If safety mechanisms and mission block are different,

redundancy architecture MooN has different non-identical channels: in this case development of a generalized PMHF formula for MooN redundancy architecture is very elaborate. However, the results obtained in Eq. (13) for the architecture 1oo2 with different channels are equal to the results obtained by Eq. (9) in the assumption of identical channels in both formulas.

Therefore, comparative analysis presented on the examples of different case studies, demonstrates that PFH and PMHF formulas give similar results. The results of the analysis also show the importance of categorization of faults and failures for comparison of PFH and PMHF formulas. Common cause failures can be directly included in the calculation of PFH as a beta-factor while in ISO 26262 common cause failures can be estimated only qualitatively.

Developed PMHF formula for MooN redundancy architecture with identical channels is easy for use by engineers. Such a formula also allows to conduct a comparative analysis of PFH and PMHF. However, for more complicated architectures where obtained simplified PMHF formula cannot be applied, analytical methods such as fault tree analysis should be applied.

One of the topics for future research may include an extension of PMHF formula developed in this paper for MooN redundancy architecture, with inclusion of test of safety mechanisms with multiple-point fault detection interval, and consideration of non-identical channels.

The formulas and comparative analysis presented in this paper is a useful contribution to the reliability assessment of drive-by-wire systems which play significant role in automobiles with autonomous driving.

References

Das, N. and W. Taylor. (2016) Quantified Fault Tree Techniques for Calculating Hardware Fault Metrics According to ISO 26262. *IEEE Symposium on Product Compliance Engineering (ISPCE)*.

International Organization for Standardization (ISO). (2018). ISO 26262. Road vehicles - Functional safety, 2nd ed., Part 1, 5, 10.

International Electrotechnical Commission (IEC), (2010). IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems, 2nd ed, Part 1-7.

Kleyner, A. and R. Knoell. (2018) Calculating Probability Metric for Random Hardware Failures (PMHF) in the New Version of ISO 26262 Functional Safety - Methodology and Case Studies, *SAE Technical Paper*, 2018-01-0793.

Lundteigen, M.A. and M. Rausand. (2007) Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *JLPPI, 20-3*, 218-229.

Rausand, M. (2014) *Reliability of safety-critical systems theory and applications*. Hoboken, NJ: John Wiley & Sons.

Rogova, E., G. Lodewijks, and M.A. Lundteigen. (2017) Analytical formulas of average probability of failure on demand and average frequency of dangerous failures per hour calculation for systems with nonconstant failure rates. *Proc IMechE Part O: J Risk and Reliability, 231-4,* 373-382.

Sakurai, A. (2018, April) Generalized Formula for the Calculation of a Probabilistic Metric for Random Hardware Failures in Redundant Systems, *In Compliance*.