Emergency Operation in the Power Supply Domain according to ISO 26262

Philipp Kilian¹, Oliver Koller², Patrick van Bergen¹, Carsten Gebauer³, Frederic Heidinger¹, Martin Dazer⁴
¹Cross-Domain Computing Solutions, Product Area Integrating Devices – Engineering Vehicle Systems (XC-AN/EPI1), Robert Bosch GmbH, 70499 Stuttgart, Germany
²Cross-Domain Computing Solutions, Product Area Integrating Devices – Senior Expert Powernet Strategy (XC-AN/PAl), Robert Bosch GmbH, 70499 Stuttgart, Germany
³Systems Engineering, Bosch Center of Competence Vehicle Safety (M/ENG-CVS), Robert Bosch GmbH, 71636 Ludwigsburg, Germany
⁴Institute of Machine Components, University of Stuttgart, 70569 Stuttgart, Germany

Corresponding author: Philipp Kilian (e-mail: philipp.kilian@de.bosch.com).

ABSTRACT The automotive industry is currently driven by the megatrends electrification, automated driving, and connectivity. To cope with these trends, new functionalities and electric and/or electronic (E/E) systems must be developed. Independent of the implementation of E/E systems, their power input shall be ensured by the power supply system as a shared resource. This leads to increased functional safety requirements for the power supply system, particularly regarding availability. Fault tolerance measures can be implemented to address a safety goal (SG) specifying a safety-related availability (SaRA) requirement. In this case, the functionality shall be provided even after the first fault. Emergency operation (EO) may be necessary to reach a defined safe state. The EO is still considered to be free from unreasonable risk even though the actual automotive safety integrity level (ASIL) capability of the item is lower than the initially specified ASIL rating for the hazard due to its timing restrictions. The definitions and examples provided in ISO 26262 focus on cold redundancy, whereby the backup system is not engaged during nominal operation. However, typical power supply architectures are implemented as warm redundancies. In this paper, EO in the context of ISO 26262 is evaluated in detail and mapped to an exemplary use case in the power supply domain.

INDEX TERMS Automotive Electronics, Automotive Engineering, Functional Safety, ISO 26262, Power Supplies, Reliability, Requirements Engineering, Vehicle Safety

I. INTRODUCTION

The relevance of safety applications within the automotive industry is continuously increasing, particularly driven by the megatrends electrification, automated driving, and connectivity. Generally, the ISO 26262 series of standards is applied to ensure the functional safety of safety-related E/E systems in the automotive industry. The power supply system is essential because it represents a shared resource for several safety-related E/E systems. Thereby, SaRA requirements are allocated to the power supply system, which cannot be realized using state-of-the-art fail-passive approaches.

To standardize the safety process and improve its applicability in the power supply domain, ISO 26262 concepts for EO are discussed in this paper.

A. ORGANIZATION OF THE ARTICLE

In Section I, the general aspects of functional safety in the context of the power supply domain are discussed, and different implementations of redundancy are distinguished. In Section II, EO is discussed in the context of ISO 26262, focusing on cold redundancy. In Section III, EO is applied to an exemplary power supply architecture that implements cold redundancy. Furthermore, an outlook is presented on how these definitions can be adapted to warm redundancy.

B. OBJECTIVE

Currently, there is no standard approach in the automotive industry to apply EO to fault-tolerant power supply systems. To fill this gap, EO, as defined in the second edition of ISO 26262, is discussed in detail and mapped to the power supply domain. Among others, the focus is on the general characteristics of EO, the definition of possible safe states, and
the maximum permissible duration of an EO. In addition, an approach for coping with transient faults in the context of EO is presented.

C. POWER SUPPLY SYSTEM IMPLEMENTING SAFETY RELATED AVAILABILITY REQUIREMENTS

Power supply systems are within the scope of ISO 26262 and must be functional safety compliant for homologations since 2022 [1], [2]. The relevance of failures in power supply systems and the continuously rising functional safety requirements have been discussed in previous publications [1], [3]. Power supply systems are considered as shared resources because they affect several other elements in the case of a malfunction [3].

The main tasks of the power supply system are to provide a safe power feed and power distribution [1]. Additionally, freedom from interference shall be ensured to enable ISO 26262-compliant coexistence between the different elements of the E/E system [4]. Thus, cascading faults between elements, which are implemented with different integrity levels regarding their capability to prevent interference with the power supply, are avoided [1], [3]. Otherwise, faults caused by elements with lower safety integrity potentially “directly or indirectly, violate any safety requirement” [4] of elements with higher integrity levels. This requirement applies to all elements that potentially affect the availability of the power supply, such as loads, wiring harness, energy sources and energy storages.

A widely discussed safety-related E/E system that allocates functional safety requirements to a power supply system is the steering entity [1], [3]. Within this paper, the steering entity comprises the item “electrical power steering” (EPS) and the item “power supply system” as introduced in [3]. In Table I, an exemplary use case for manual driving is introduced based on [1]. If the steering assist functionality is unavailable for longer than the fault tolerant time interval of the EPS (FTTI_{EPS}) of 100 ms, a potentially hazardous event occurs. Because a loss of steering functionality can lead to a hazardous situation while driving, a SaRA requirement for the steering entity is specified regarding its steering-assist functionality. Thus, the SaRA requirement is allocated to the power supply system. If the availability of a function is safety-related, it depends mainly on the vehicle operating state (VOS) [3], [5]. Therefore, the following safety requirements are applicable only for specific VOSs.

The FTTI_{EPS} of 100 ms on the EPS shall be adapted to the power supply system. Among others, this exemplarily leads to an FTTI_{PS} of 100 µs for the power supply system according to [3], which is considered in the following. Because the FTTI is a “relevant attribute for safety goals” [6] and thus, defined on item level, it shall be refined for the element level as maximum fault handling time interval (FHTI_{max}) to “support the functional safety concept” [6].

### Table I

| Hazard | Sudden loss of steering assist |
|--------|-------------------------------|
| Exposure | Everyday driving situation |
| Control-liability | Steering force support makes it easier if corrections are required. Normally, controllable, 90 % or more of all drivers or other traffic participants are usually able to avoid harm. |
| Severity | Depends on impact velocity: S3: > 40 km/h; S2: > 20 km/h; S1: > 0 km/h (ISO 26262-3, Table B.1) |
| Safety Goal | Prevent sudden loss of steering assist |
| HW metrics | PMH_{EPS}^*: < 100 FIT; SPF_{EPS}^* ≥ 97 %; LFM_{EPS}^* ≥ 80 % |

*Probabilistic metric for random hardware failures; *Single-point fault metric; ‘Latent-fault metric

In this study, it is explicitly differentiated between the FHTI_{max} – as a requirement – and the fault handling time interval (FHTI) – as an actual characteristic of a safety mechanism (SM) – according to [1].

D. COLD REDUNDANCY VS. WARM REDUNDANCY

In general, fault tolerance measures to ensure SaRA requirements are implemented by using redundancy. Redundancy may also be mandatory for homologations due to technical regulations [7]. Thereby, the performance of the backup system during fault-free operation can be integrated into the nominal mode in different ways, e.g., cold, warm, or hot redundancy [8].

The difference between cold, warm, and hot redundancies was discussed in detail in [3]. For the purpose of this study, the definitions of cold and warm redundancies according to Birolini were considered [8]:

1) Cold redundancy: “Redundant elements are subjected to no load until they become operating; load sharing is possible for operating elements, but not considered in the case of independent elements, and the failure rate in reserve (standby) state is assumed to be zero”;

2) Warm redundancy: “Redundant elements are subjected to a lower load until they become operating; load sharing is possible, but not considered in the case of independent elements”; failure rate “is between active and standby”

In the case of cold redundancy, actions such as activating or switching to the backup system are required. In contrast, no action to activate the backup is necessary if warm redundancy is implemented because the backup system is already active during nominal operation.

II. EMERGENCY OPERATION IN CONTEXT OF THE ISO 26262

In this section, EO is introduced as defined in ISO 26262. Among others, the focus is on the general characteristics of EO, definition of possible safe states, and maximum permissible duration of EO. Additionally, transient faults are discussed in the context of EO.
A. FAULT TOLERANCE TO ACHIEVE SAFETY-RELATED AVAILABILITY

SaRa requirements can be addressed by several safety measures, see [3], [5], or [9] for more details:
1) Fault avoidance: Faults shall be avoided through proper processes and/or dedicated measures. Thus, no failure shall occur at all.
2) Fault forecasting: Faults occurrence is predicted, and a hazard is prevented by not entering a safety-relevant VOS or leaving it before a failure occurs.
3) Fault tolerance: Faults occur, but specified functionality is provided “even in the presence of one or more faults” [5]. The function can be fully or partially maintained due to redundancy, typically with a reduced ASIL capability.

To achieve a certain ASIL capability, the safety requirements shall be fulfilled for systematic and random hardware faults. However, in the case of fault tolerance, the functionality is typically provided with a lower ASIL capability after the loss of the main system compared with the ASIL rating of the initial possible hazard:
1) Systematic faults: If ASIL decomposition is applied, at least one of the redundant systems only prevents and/or controls systematic faults with an ASIL lower than the hazard’s ASIL rating [3].
2) Random hardware faults: Redundancy enables lower requirements for random HW faults for each redundant system. After the loss of the main system, the stand-alone backup system typically does not comply with the initial target values for random HW faults.

The implementation of redundancy is typically driven by the safety requirements concerning random hardware faults. However, this has a negative impact on system costs, packaging, and weight [3]. In the following, the focus is mainly on systems with fault tolerance measures, whereby EO can be supported.

B. DEFINITION OF EMERGENCY OPERATION

Within ISO 26262, EO is defined as “operating mode of an item, for providing safety after the reaction to a fault until the transition to a safe state is achieved” [6]. This is applied if a “safe state
1) cannot be directly reached, or
2) cannot be timely reached, or
3) cannot be maintained after the detection of a fault” [6].

“Timely” is defined more precisely in ISO 26262-4:2018, 6.4.2.2, and ISO 26262-10:2018, 4.4.2.2, where FTTI is stated as time criteria. In general, EO shall be “initiated prior to the end of the FTTI and is maintained until the safe state is reached prior to the end of the emergency operation tolerance time interval” [5] (EOTTI). Therefore, a fault in the main system, which could potentially violate an SG directly, shall be detected, and a transition to EO shall be completed within the FTTI, i.e. to switch to the backup system. EOTTI is defined as “specified time-span during which [EO] can be maintained without an unreasonable level of risk“ [6]. If a safe state is reached within EOTTI, the SG is met; if not, the “cumulated risk becomes unacceptable” [5].

In general, the item is considered free from unreasonable risk during EO “even though the ASIL capability of the item is lower than the ASIL rating of the possible hazard” [5]. More precisely, the ASIL capability of an item after a fault is lower than the initially specified ASIL rating for the SG. As described in Section II-A, this may be the case after loss of the main system. If only fault avoidance measures are applied, no EO can be entered. EO can only be considered free from unreasonable risk because “the operating time in this state is limited, such that it is unlikely that an additional fault occurs which leads to a violation of the [SG]” [5]. Therefore, EO is only a timely limited state, that can be considered safe. However, the EO itself is not considered to be a safe state. EO is a temporary operating mode that enables a safe transition to a safe state, whereas a safe state is generally not limited in time. An SM is implemented to prevent entering possible VOSs in which the ASIL rating of the possible hazards exceeds the remaining ASIL capability after reaching a safe state [5]. According to ISO 26262-10:2018, 12.2.4.2 Note 6, this SM is implemented with the initial ASIL rating [5].

The EO is designed in a way that a further sufficiently independent fault, which would result in an SG violation in combination with the already occurred fault, is sufficiently unlikely during this limited time. Thus, the probability of fault occurrence during EO is considered as part of the derivation of the EOTTI. The EO, and therefore the EOTTI, begins as soon as the transition to the backup system is completed. The actual “time-span during which [EO] is maintained” [6] is defined as emergency operation time interval (EOTI). EOTI shall not be longer than EOTTI [6]. Therefore, the most relevant properties of EO are:
1) EO shall be restricted in time to avoid unreasonable risk.
2) EO is entered if the occurrence of a hazardous event is prevented, but a safe state cannot be reached within the FTTI.
3) EO shall be triggered within FTTI.
4) EO starts after the completion of the immediate fault reaction, which is required to prevent the occurrence of a hazardous event, i.e. as soon as switching to the backup is completed.
5) EO starts as soon as the specified functionality is available again. However, from the occurrence of a fault until the start of EO, i.e. during FHTI, the specified functionality may not be available.
6) EO is maintained during EOTI, whereby the ASIL capability of the item is lower than the ASIL rating for the possible hazard.
7) EO relies solely on the backup system. Thus, during EOTI, a fault in the backup potentially leads directly to a violation of an SG.
8) EO is only a temporary operating mode without an unreasonable risk of a further fault until a safe state is reached within EOTTI. Thus, it can be considered safe.

C. DEFINITION OF SAFE STATES

In ISO 26262-10:2018, 12.2.4.2, two potential safe states are described [5]:

1) Safe state 1: “[VOS] in which the specified functionality is no longer needed for safety reasons”, i.e. permanently switching off the specified functionality until the item is repaired.

2) Safe state 2: “possible [VOSs] are limited in such a way that the ASIL rating of the hazardous events which can occur in the limited [VOSs] is equal to or lower than the ASIL capability of the remaining system”, i.e. providing the specified functionality without time restrictions for the limited VOS until the item is repaired.

To achieve safe state 1, the item “maintains the specified functionality after occurrence of a fault” [5] until the specified functionality is permanently switched off within EOTTI. During this time span, the “functionality is kept operating” [5] without a VOS limitation. The time being in a VOS without a SaRA requirement during EO, e.g., the vehicle standstill, is also considered as part of EOTI because a fault may occur and manifest during this time. Thus, the SG may be violated as soon as a VOS with a SaRA requirement is entered if it is not handled properly by prevention of (re-) entering a safety-relevant VOS with a SaRA requirement after the second fault occurred. After finally reaching a safe state within the EOTTI, the functionality is kept unavailable until the item is repaired.

To achieve safe state 2, the item “maintains the specified functionality after occurrence of a fault” [5] until the limited VOS are reached “within an allowable time interval” [5], i.e. EOTTI. Within safe state 2, the vehicle function “is kept to the limited [VOS] without time limitation” [5] by the backup system. Thus, the vehicle function is provided after EO as well. Depending on the SG, one of the most obvious measures to limit the VOSs is, e.g., to limit vehicle speed. The SM implemented to restrict possible VOS inherits the initial ASIL of the SG according to ISO 26262-10:2018, 12.2.4.2 Note 6 [5]. Once the item is repaired, “possible [VOSs] will return to unlimited” [5].

In its most generic way, the basic characteristics of how the safe states shall be achieved are equal [5]:

1) “item maintains the specified functionality after occurrence of a fault” and thus, the “functionality is kept operating” until the end of EOTTI, i.e. until a safe state is reached – without VOS limitation;

2) “item reaches the safe state”, i.e. ASIL rating of the possible hazard is not greater than the remaining ASIL capability of the item.

For safe state 1, the vehicle function is permanently switched off; however, for safe state 2, the vehicle function is kept operating afterwards. In both cases, the remaining possible VOSs are restricted such that the remaining ASIL rating of the possible hazard is not greater than the ASIL capability of the item. Whereas, for safe state 1, the possible VOSs are limited in such a way that no SaRA requirement is specified at all for those VOSs; for safe state 2, the possible VOSs are limited in such a way that the resulting SaRA requirements are reduced regarding their integrity and thus adapted to the remaining ASIL capability of the backup system. Therefore, safe state 1 can be interpreted as special application of safe state 2. In practical applications, it may be easier to maintain safe state 1 than safe state 2. Nevertheless, the SM implemented to maintain the vehicle standstill, i.e. to restrict possible VOSs, is implemented with the initial ASIL rating according to ISO 26262-10:2018, 12.2.4.2 Note 6 [5]. In general, a system comprising multiple redundancies can include subsequent EOs.

If the item is repaired within the EOTTI, none of the described safe states are applicable. In this case, the possible VOSs are neither restricted until nor after repair. The initial ASIL capability is restored, by repairing the item. [5].

D. QUANTITATIVE DERIVATION OF EMERGENCY OPERATION TOLERANCE TIME INTERVAL

To derive the EOTTI, the probability of fault occurrence during the EO shall be considered. Thus, the EO is designed such that a further sufficiently independent fault, which would result in an SG violation, is sufficiently unlikely during this limited time. In general, the probability that a failure occurs within a defined time interval $[0 \ldots t]$ is defined as unreliability $F(t)$ [10]. For random hardware faults an exponential distribution with a constant failure rate $\lambda$ is typically assumed [5], [10], [11]. The resulting unreliability can be calculated using (1). If the focus is only on small failure rates – which is typically the case for E/E systems – the approximations in the subsequent equations can be used. According to [5] and [10], the failure rate can be considered small if $\lambda \cdot t < 0.1$.

$$F(t) = \int_0^t f(\tau) \, d\tau = 1 - e^{-\lambda \cdot t} \cong \lambda \cdot t. \quad (1)$$

The unreliability $F(t)$ is monotonically increasing “since for each time or interval a positive value is added – the observed failure frequency” [10]. $f(t)$ is the derivation of the unreliability $F(t)$ and is defined as the failure density function [11]. For random hardware faults – considering an exponential distribution and constant failure rate – it is calculated using (2) [5], [10], [11]:

$$f(t) = \lambda \cdot e^{-\lambda \cdot t} \cong \lambda. \quad (2)$$

However, in the context of functional safety, the input to calculate the probability that a failure occurs within a defined time interval may not be the failure rate of an individual component, which is typically the case in reliability analysis. The input may also be an average probability per hour over a
defined time interval considering the effect of the implemented SMs – in the following referred to as $\lambda_{\text{avg}}$ – which is generally not the case for $F(t)$. Even though the probability per hour over a defined time interval of the item $\lambda_{\text{avg}}$ and the failure rate $\lambda$ share the same unit, i.e. failures in time (FIT), they are different values [5]. 1 FIT corresponds to one failure per one billion operational hours, i.e. 1 FIT = $10^{-9}$ 1/h.

The probability per hour over a lifetime is defined as PMHF [12]. The resulting probability that a failure occurs within a certain time interval $POF(t)$ can be calculated according to (3) for random hardware faults, analogous to (1):

$$POF(t) = 1 - e^{-\lambda_{\text{avg}} t} \approx \lambda_{\text{avg}} \cdot t. \quad (3)$$

The probability that a failure occurs within the lifetime $T_{\text{life}}$ – considering only small failure rates – is calculated using (4):

$$POF(T_{\text{life}}) = \text{PMHF} \cdot T_{\text{life}}. \quad (4)$$

Two different first-order approximations based on random hardware faults are provided in ISO 26262 to derive and/or calculate EOTTI. In the following sections, both equations are explained and compared.

1) RESIDUAL RISK CAUSED BY REDUNDANT SYSTEMS
The residual risk of an SG violation for both redundant systems combined shall be lower than the defined PMHF target, e.g. according to ISO 26262-5:2018 Table 6. For SGs rated with ASIL B or ASIL C, the PMHF target is set to 100 FIT, and the PMHF target for a SG rated with ASIL D is set to 10 FIT [12]. To ensure that the residual risk is below the PMHF target, the EOTTI shall be derived based on the equation used to calculate the PMHF. The PMHF can be calculated by applying certain patterns, see ISO 26262-10:2018, 8.3.2.4 for a detailed description [5]. In the example provided in ISO 26262, the item comprises the intended functionality (IF) and two SMs (SM1 and SM2). Thereby, faults in the IF are detected, mitigated, and notified to the driver by SM1. In addition, faults in SM1 are detected, mitigated, and notified to the driver by SM2:

1) Pattern 1: “fault in SM1 is not mitigated by SM2”;
2) Pattern 2: “fault in SM1 is mitigated and notified by SM2”;
3) Pattern 3: “fault in IF is detected, mitigated, and notified to the driver by SM1. In addition, faults in SM1 are detected, mitigated, and notified to the driver by SM2:
4) Pattern 4: “fault in IF is mitigated and notified by SM1”.

The resulting PMHF can be calculated according to (5):

$$PMHF = \lambda_{\text{SPF}} + \lambda_{\text{RF}}$$

Pattern 1

$+ 0.5 \cdot \lambda_{\text{SM1,DPF,latent}} \cdot \lambda_{\text{IF,DPF}} \cdot T_{\text{life}}$

Pattern 2

$+ \lambda_{\text{SM1,DPF,Detected}} \cdot \lambda_{\text{IF,DPF}} \cdot T_{\text{Service}}$

Pattern 3

$+ 0.5 \cdot \lambda_{\text{IF,DPF,latent}} \cdot \lambda_{\text{SM1,DPF}} \cdot T_{\text{life}}$

Pattern 4

$+ \lambda_{\text{IF,DPF,Detected}} \cdot \lambda_{\text{SM1,DPF}} \cdot T_{\text{Service}}, (5)$

The relevant variables are summarized in Table II [5].

For clarity and ease of comprehension, the following assumptions are made to simplify (5):

1) No SPF is assumed;
2) If a fault in the IF is controlled by SM1, it is always notified to the driver, i.e. $\lambda_{\text{IF,DPF,Detected}} = \lambda_{\text{IF,DPF}}$ and $\lambda_{\text{IF,DPF,Latent}} = 0$;
3) SM2 is neglected, i.e. $\lambda_{\text{SM1,DPF,latent}} = \lambda_{\text{SM1,DPF}}$ and $\lambda_{\text{SM1,DPF,Detected}} = 0$.

Based on these assumptions, Patterns 2 and 3 have no impact on the PMHF and can be neglected in the derivation of EOTTI.

Within the remaining Pattern 4, $T_{\text{service}}$ can also be interpreted as the time until a vehicle function is permanently switched-off after the first fault – if it is no longer needed for safety reasons – instead of repairing the item as described in the definition above. In this case, the definition of $T_{\text{service}}$ is similar to that of EOTTI. In its most general manner, $T_{\text{service}}$ and EOTTI can be interpreted as the actual time interval where a detected multiple point fault (MPF) can be present in a system causing an SG violation in combination with a further independent MPF. Therefore, $T_{\text{service}}$, and EOTTI are considered to be equivalent in the following equations. In general, SMs implemented to transition to safe state 1 or safe state 2 after a first fault shall handle the MPF within the EOTTI. Hence, (5) can be adapted to (6) by replacing $T_{\text{service}}$ with $T_{\text{EOTTI}}$ in the actual PMHF with the PMHF target value, i.e. $\lambda_{\text{avg,target}}$, see also ISO 26262-10:2018, 12.3.1.2 [5]:

$$T_{\text{EOTTI}} \leq (\lambda_{\text{avg,target}} - \lambda_{\text{SPF}} - \lambda_{\text{RF}})$$

$$-0.5 \cdot \lambda_{\text{SM1,DPF,Latent}} \cdot \lambda_{\text{IF,DPF}} \cdot T_{\text{life}}$$

$$-0.5 \cdot \lambda_{\text{IF,DPF,Latent}} \cdot \lambda_{\text{SM1,DPF}} \cdot T_{\text{life}}$$

$$/(\lambda_{\text{IF,DPF,Detected}} \cdot \lambda_{\text{IF,DPF}} + \lambda_{\text{IF,DPF,Detected}} \cdot \lambda_{\text{SM1,DPF}}). \quad (6)$$

A more detailed equation may need to be derived for a specific architecture to calculate the PMHF and thus, to calculate EOTTI, e.g. by considering multiple redundancies and cyclic diagnostics with different time bases. The intention of this methodology is to derive the EOTTI based on the PMHF calculation – independent of the actual equation used to calculate the PMHF. Therefore, EOTTI can also be derived, e.g., based on an FTA.

Considering the assumptions introduced previously, (6) can be simplified as (7):

$$T_{\text{EOTTI}} \leq (\lambda_{\text{avg,target}} - \lambda_{\text{RF}})$$

$$-0.5 \cdot \lambda_{\text{SM1,DPF,Latent}} \cdot \lambda_{\text{IF,DPF}} \cdot T_{\text{life}}$$

$$/(\lambda_{\text{IF,DPF,Detected}} \cdot \lambda_{\text{SM1,DPF}}). \quad (7)$$

### Table II

| Variable | Explanation |
|----------|-------------|
| $\lambda_{\text{SPF}}$ | “single point failure rate” |
| $\lambda_{\text{RF}}$ | “residual failure rate” |
| $\lambda_{\text{SM1,DPF,Detected}}$ | “dual point failure rate for X” |
| $\lambda_{\text{SM1,DPF,Latent}}$ | X’s “detected and notified dual point failure rate” |
| $\lambda_{\text{SM1,DPF,Detected}}$ | X’s “latent dual point failure rate (mitigated but not notified)” |
| $T_{\text{life}}$ | “vehicle lifetime” |
| $T_{\text{Service}}$ | “expected time to repair after notification provided to driver” |
If the resulting $T_{EOTTI}$ is negative, the PMHF target is already exceeded by the RFs and Pattern 1. This could be an indication of an insufficient design. If safe state 2 is targeted, the PMHF shall be proven for this safe state based on the remaining system. If the remaining system comprises redundant elements, an additional EOTTI can be calculated to transition from the limited VOSs to, e.g., an operating state without any SaRA requirements.

In Fig. 1, the impacts of RFs, Pattern 1, and Pattern 4 on the overall PMHF are illustrated. In this example, $T_{service} = T_{EOTTI} = 975$ h (see Section III-B) is assumed. Each line represents the probability of failure resulting from a pattern or the RFs. The $P_{RF}(t)$ resulting from the RFs is the main contributor to this example (see Fig. 1, black dotted line). It increases linearly over time due to the approximated equation (3), i.e.:

$$P_{RF}(t) = PMHF_{RF,i} \cdot t = \lambda_{RF} \cdot t.$$  

The average probability per hour over time resulting from the RFs is constant $= \lambda_{RF}$ in general. The average probability of failure per hour over a certain time interval is represented by the slope of the relevant straight line from the probability of failure at the beginning to the probability that a failure occurs at the end of the interval of interest. The resulting $P_{RF}(t)$ of Pattern 1 increases quadratically over time, see (9) and Fig. 1 point-virgule line:

$$P_{RF}(t) = PMHF_{RF,i} \cdot t = 0.5 \cdot \lambda_{SM1,DPF,latent} \cdot \lambda_{IF,DPF} \cdot t \cdot t.$$  

To evaluate the resulting $P_{RF}(t)$ from Pattern 4, the following intervals are differentiated:

$$P_{RF}(t) = PMHF_{RF,i} \cdot t = \lambda_{IF,DPF, detected} \cdot \lambda_{SM1,DPF} \cdot t \cdot t \text{ if } t \leq T_{EOTTI}$$

$$= \lambda_{IF,DPF,detected} \cdot \lambda_{SM1,DPF} \cdot T_{EOTTI} \cdot t \text{ if } t > T_{EOTTI}.$$  

The resulting $P_{PMHF}(t)$ is the sum of the three individual $P_{RF}(t)$, $P_{PR}(t)$, and $P_{RF}(t)$. The average probability per hour over the lifetime, i.e. the PMHF, is represented by the slope of a straight line from $P_{PMHF}(0) = 0$ to $P_{PMHF}(T_{life})$. The PMHF shall be lower than the PMHF target. The longer $T_{service}$ respectively $T_{EOTTI}$, the higher the final PMHF due to the higher slope resulting from $P_{RF}(t)_{P4}$.

In contrast to Birolini, it is not recommended to consider the failure rate in the reserve state as zero for cold redundancy [8]. During the time in the reserve state, a fault may occur and manifest anyway – increasing the risk of an SG violation. Thus, the MPFs in the backup system shall be considered in Patterns 1 and 2. This potentially necessitates the implementation SMs to prevent faults from being latent. Nevertheless, the mission profile during the reserve state may differ from that during the operation of the backup system, which potentially results in different failure rates for the two different operating phases.

2) RESIDUAL RISK CAUSED BY THE BACKUP SYSTEM

The second equation for calculating the EOTTI is stated in ISO 26262-10:2018, 12.3.1.1 [5]:

$$T_{EOTTI} \leq T_{life} \cdot \frac{\lambda_{avg.target}}{\lambda_{avg.degr}}$$

whereby [5]:

1) $\lambda_{avg.target}$:
   a. Safe state 1: target PMHF of “the initial ASIL is used”;
   b. Safe state 2: “target PMHF […] corresponding to the ASIL rating of the item after the occurrence of the fault or loss of redundancy”;

2) $\lambda_{avg.degr}$: “average probability per hour over [EOTTI] of a failure that results in a violation of the [SG]” [5] – caused by the remaining system after loss of redundancy.

There is a contradiction in the introduction of the equation and description of $\lambda_{avg.target}$. On the one side, it is referred to the “probabilistic metric of violating the [SG] over the expected usage of the vehicle” [5], i.e. the ASIL of the initial hazard. On the other hand, it is referred to as “the ASIL rating of the item after the occurrence of the fault or loss of redundancy” [5]. Following the intention of (11), the PMHF-target value of the initial hazard shall be considered to balance the risk between nominal operation and EO. Thus, the target PMHF of “the initial ASIL is used” – independent of the chosen safe state.

The resulting EOTTI can be considered “as a property of the item state after the occurrence of the fault or loss of redundancy” [5]. Therefore, the equation focuses only on the state during EO. In this case, the “appropriateness of the $T_{EOTTI}$ is decided by comparing the probabilistic metric of violating the [SG] over the expected usage of the vehicle (PMHF $\times T_{life}$) to the probabilistic metric of violating the [SG] while operating without redundancy” [5], i.e. by comparing the maximum permissible probability that a
failure occurs over lifetime to the probability that a failure occurs during EO:

\[
PoF(T_{EOTTI}) \leq PoF(T_{life})
\]

\[
1 - e^{-\lambda_{avg,EOTTI}T_{EOTTI}} \leq 1 - e^{-\lambda_{avg.life}T_{life}}
\]

\[
\lambda_{avg,EOTTI} \cdot T_{EOTTI} \leq \lambda_{avg.life} \cdot T_{life}.
\]

(12)

where: \( \lambda_{avg,EOTTI} = \lambda_{avg,degr} \) and \( \lambda_{avg.life} = \lambda_{avg,target} \). Equation (11) can be adapted to the use case presented in ISO 26262-10:2018, 8.3.2.4 respectively Section II-D 1 resulting in [5]:

\[
T_{EOTTI} \leq T_{life} \cdot \frac{\lambda_{avg,target}}{\lambda_{SM1,DPF}}.
\]

(13)

A comparison of the probability that a failure occurs during the EO and the maximum permissible probability that a failure occurs over the lifetime is shown in Fig. 2. Even though the backup has a significantly higher average probability of failure per hour, the resulting probability that a failure occurs during EO can be limited by restricting time in this state. Therefore, it can be ensured that the residual risk of an SG violation during the time-limited EO is not greater than the probability that a failure occurs over the lifetime.

\[
\begin{align*}
&\text{FIGURE 2. Comparison of the probability that a failure occurs during EO} \\
&\text{and the maximum permissible probability that a failure occurs over lifetime}
\end{align*}
\]

In these equations, it is implicitly assumed that no fault in SM1, respectively the backup system in general, is present at the time the first fault occurs. This equation focuses solely on the operation after the first fault in the main system. In addition, no fault can occur until the backup system is activated, which is analogous to Birolini [8]. However, if a fault in the backup system can occur when it is not yet activated – in contrast to [8] – it shall be considered in the derivation of EOTTI. In this case, a fault in the backup system causing its unavailability may have already occurred during the fault detection in the main system and the transition to the backup system, i.e. FHTI. If such a fault occurs, SG violation is not prevented after completion of the transition to the backup system because the required functionality cannot be provided. Therefore, the probability that a failure occurs in the backup system during the FHTI is considered in the derivation of the EOTTI in addition to the probability that a failure occurs in the backup system during the subsequent EO. By doing so, (12) is adapted to (14):

\[
PoF(T_{FHTI}) + PoF(T_{EOTTI}) \leq PoF(T_{life}).
\]

(14)

If different averaged probability of failure per hour during FHTI – with no/reduced stress – and the subsequent EO shall be considered, (14) results in (15) for small failure rates and small average probability of failure per hour:

\[
T_{EOTTI} \leq \frac{T_{life} \cdot \lambda_{avg,target} - T_{FHTI} \cdot \lambda_{avg,degr,FHTI}}{\lambda_{avg,degr,EOTTI}}.
\]

(15)

whereby:

1) \( \lambda_{avg,FHTI} \): average probability per hour over FHTI;

2) \( \lambda_{avg,degr,EOTTI} \): average probability per hour over EOTTI.

If the actual required FHTI to detect a fault in the main system and transition to the backup system has not yet been determined, e.g., in the early development phases, it can be replaced conservatively by \( FHTI_{max} \) as the upper boundary. Depending on FHTI, the impact of \( T_{FHTI} \cdot \lambda_{avg,degr,FHTI} \) may be negligible. However, not considering this term is a non-conservative simplification.

3) COMPARISON OF CALCULATION METHODS

These two equations, typically, result in different EOTTIs [5]:

1) Equation (6): considering the probability that EO is triggered in the first place by evaluating the overall risk. The EOTTI depends on the system design during fault-free operations;

2) Equation (11) or (13): only focusing on the operation during EO by comparing the probability that a failure occurs during EO to the maximum permissible probability that a failure occurs over the lifetime of the target ASIL. EOTTI depends on the system design after a fault occurs.

The application of (11) is not mandatory for compliance with ISO 26262. Nevertheless, it can be considered to evaluate the design of the backup system and prevent too optimistic EOTTIs. However, the application of (6) respectively more general the derivation of EOTTI based on the PMHF calculation – independent of which equation or method is used – is required by ISO 26262 and thus, shall be considered for the design of the EO. The resulting EOTTI can be interpreted as a time interval in which the occurrence of two DPFs causing a dual-point failure and thus, an SG violation, is sufficiently unlikely with respect to the ASIL rating of the hazard.

A common misunderstanding in the automotive industry is, that EOTTI shall only be derived based on random hardware faults. Real-world issues typically relate to systematic faults. Generally, the conditional probability \( P \) that a second fault is of a systematic nature is deemed significantly higher than the conditional probability \( P \) that a second fault is a random hardware fault:
\[ P(\text{systematic fault}|2^{nd} \text{ fault}) \gg P(\text{random hardware fault}|2^{nd} \text{ fault}) \]  

Hence, optimizing EOTTI by just considering the risk resulting from random hardware faults may not be an appropriate approach. Because the probability of occurrence of a systematic fault typically cannot be predicted and quantified, the risk mitigation strategy for systematic faults is to keep the EOTTI as short as reasonably possible. Thereby, it is appropriate to consider the overall resulting risk from different minimal risk maneuvers and the correlated necessary EOTI to execute them. This is particularly relevant if both redundant systems cannot be considered to be fully independent. Thus, systematic effects may arise after the first fault, which additionally limit the EOTI. Those constrains can be identified in the dependent failure analysis and shall be taken into account for the design of EO to, e.g., avoid cascading faults. Therefore, the quantitatively derived EOTTI based on random hardware faults is only considered as the upper boundary of the EOTTI.

E. TRANSIENT FAULTS CAUSING EMERGENCY OPERATION

Whereas previous definitions mainly focused on permanent faults, transient faults may also occur. However, no guidelines have been provided within ISO 26262 on how to deal with transient faults in the context of EO. Transient faults are defined as “fault that occurs once and subsequently disappears” [6]. If a transient fault causes a loss of the main system for longer than FHTI\textsubscript{max} respectively FTTI, a transition to the backup system shall be triggered to prevent an SG violation and thus, an EO is entered – similar to a permanent fault. A temporary operation under stressful environmental conditions outside the specification is considered as transient fault. If a temporary operation outside the specification occurs frequently, e.g., electromagnetic interference or extremely cold temperatures, it shall be considered as a systematic fault due to an insufficient specification. However, if this only occurs infrequently by a random combination of worst-case conditions, the EO may be used to argue for the absence of unreasonable level of risk. Basic premise: The backup system is sufficiently independent and is still operating.

If the transient fault disappears within EOTTI by itself, it may be feasible to switch back to the main system to limit the operation on the backup and thus, not force a transition to the previously mentioned safe states according to Section II-C. This can be considered a minimal risk condition in addition to the provided safe states. Because these transient faults are considered as systematic faults, they are typically not considered in quantitative evaluations based on random hardware faults.

The risk of a further sufficiently independent fault that violates the SG accumulates every time a temporary EO is present. The second fault that causes a loss of the backup system can be either permanent or transient. To prevent an unreasonable level of risk, the actual duration of every temporary EO, i.e. EOTI, is accumulated because the initially derived EOTTI – among others – is based on a comparison of the probability that a failure occurs during EO to the overall maximum permissible probability that a failure occurs over the lifetime. Before the sum of EOTI exceeds EOTTI, the transition to safe state 1 or safe state 2 shall be completed. Ensuring that the sum of the EOTIi is not greater than the initially derived EOTTI, the probability that a failure occurs in the backup system during EO respectively EOTTI is not greater than the permissible probability of failure occurring during EOTTI, i.e. PoF\textsubscript{permis}. PoF\textsubscript{permis} is based on the derived EOTTI – considering random hardware faults and systematic faults – and the PMHF target value. The behavior of the resulting probability that a failure occurs during EO is shown in Fig. 3. None of the three exemplary temporary EOTIi results in an unreasonable risk by itself because each EOTIi is shorter than EOTTI (see Fig. 3, black lines). However, the cumulated risk of all three EOTIi combined results in an unreasonable level of risk because the time duration relying on the backup exceeds the maximum permissible time, i.e. the sum of EOTIi, is longer than EOTTI and thus, the probability of a fault in the backup system is higher than permissible.

![FIGURE 3. Resulting probability that a failure occurs during EO](image)

Alternatively, instead of cumulating the time during EO, an event recorder may be implemented to count transitions to the backup system. By comparing the number of operation phases relying solely on the backup to a certain threshold, an indication of an unreasonable level of risk can be provided.

III. EMERGENCY OPERATION IN CASE OF COLD REDUNDANT POWER SUPPLY SYSTEMS

In this section, the previously discussed properties of EO are discussed for an exemplary power supply system implementing cold redundancy.

A. FUNCTIONAL SAFETY CONCEPT AND PRELIMINARY ARCHITECTURAL ASSUMPTIONS

In the early development phases, preliminary architectural assumptions can be used “to handle immature architectural
information” [13]. Two potential power supply architectures for complying with the SG introduced in Section I-C are shown in Fig. 4. In the following, the left architecture in Fig. 4 is considered as an exemplary power supply system implementing cold redundancy, whereas the right architecture provides an example for warm redundancy:

1) Topology 1: Implements a cold redundant power supply architecture. The main power supply comprises the power feeds by the DC/DC converter and the battery, whereas the backup power supply is ensured by the backup power storages. During nominal operation, the backup power storages are not actively stressed because it is disconnected from the main power supply system, and the corresponding safety-relevant loads are supplied from the main power supply – not from the backup power supply. In the case of a fault in the main power supply, e.g. an open circuit in the wiring to the EPS, switching to backup is required within FHTI\textsubscript{max}.

2) Topology 2: Implements a warm redundant power supply architecture based on the redundancy between the power feed by the DC/DC converter and the battery. Among others, a smart safety switch is implemented as a centralized safety measure to ensure sufficient independence between redundant power feeds [1]. For example, in the case of a fault leading to a loss of power feed by the DC/DC converter, e.g. short circuit to ground in an HV base load, the power supply of the EPS is instantly provided by the battery – depending on the design premises and the functional safety concept. Due to its advantages regarding scalability and costs, Topology 2 has a high level of market penetration. Therefore, the corresponding functional safety concepts are widely discussed in the automotive industry [1], [3], [14], [15]. However, this is not within the scope of the following sections because the definitions and examples provided in ISO 26262 regarding EO focus on cold redundancy. Thus, the cold redundant architecture is considered in the following for sake of simplicity, even if this architecture has only marginal significance to the automotive industry.

Analogous to the functional safety concept in [1], which focuses on a warm redundant architecture, the three generic safety requirements for power supply systems are applied to the main power supply and its backup: 1) ensuring safe power feed; 2) ensuring safe power distribution; and 3) ensuring freedom from interference [1]. Basic premise: Each power supply can provide sufficient power by itself. Decomposition can be applied to lower the ASIL for each power supply. In this case, sufficient independence between the two power supplies shall be demonstrated [5]. One possible option is to assign QM(C) integrity to the main power supply and ASIL C(C) to the backup power supply.

In addition, several requirements for the EPS shall be considered. This includes, but is not limited to:

1) Switching from the main power supply to backup in the case of a fault within the main power supply;
2) Ensure sufficient independence between main power supply and its backup;
3) EPS itself shall ensure a SaRA requirement with ASIL C. This study focused on the power supply system instead of the EPS itself. Thus, a detailed view on the EPS is not part of it.

In this example, it is assumed that an ASIL C-compliant safe power supply cannot be ensured by the main power supply or by the backup itself:

1) Main power supply: ensures neither an ASIL C-compliant safe power supply regarding systematic faults nor regarding random hardware faults. Due to the lack of freedom from interference measures, it achieves only a QM level regarding its systematic integrity.
2) Backup power supply: ensures an ASIL C-compliant safe power supply only regarding systematic faults but not regarding random hardware faults;

Thus, if a fault occurs in the main power supply and a safe state cannot be reached within FHTI\textsubscript{max} respectively FTTI, an EO can be used to argue the absence of unreasonable level of a risk during this limited time.

![Topology 1](image1)

![Topology 2](image2)

**FIGURE 4.** Preliminary architectural assumptions for power supply systems implementing either cold redundancy (left) or warm redundancy (right) to comply with the SG introduced in Table I
If any of the redundant systems by itself would comply with the initial ASIL rating for systematic faults as well as for random hardware faults, there is no need for an EO. This may also require complete independence between the main power supply and its backup, which is typically not the case in the power supply domain [3].

### B. EXEMPLARY FAULT SCENARIO

Within this section, the focus is on safe state 1, because the operation with only the backup storage is generally limited in time. If the main power supply is unavailable, the backup power storage cannot be recharged. Thus, the steering function shall be permanently switched-off within the EOTTI. This leads to the necessity to either reach a workshop within EOTTI or park the item in a minimal risk condition to enable towing to the next workshop.

The time dependencies discussed in Section II respectively the ISO 26262 are summarized in Fig. 5. The relevant time steps $t_i$ to $t_j$ in Fig. 5 are summarized in Table III according to ISO 26262-10:2018, 12.2.5.5 [5] and [1].

#### 3) EMERGENCY OPERATION

The power supply to the EPS is provided by the backup power supply after the transition is completed within the FHTI.

However, the remaining item’s ASIL capability does not comply with the ASIL of the initial hazard. Even if systematic faults are avoided with the initial ASIL, the target metrics regarding random hardware faults are not met by the backup system alone. To prevent an unreasonable risk, the transition time to safe state 1 is limited, as specified by the EOTTI. The EO, and thus EOTTI and EOTTI, begin after the backup system is activated. As of this point in time, the backup system is fully loaded.

In this example, the transition to the backup system is always signaled to the driver if it is successful, i.e. $\lambda_{DPF, detected} = \lambda_{DPF}$ and $\lambda_{DPF, latent} = 0$. Because the safe state shall be reached within the EOTTI, the actual time to transition to a safe state, i.e., EOTTI, shall not be greater than EOTTI. Thereby, a VOS without a SaRA requirement may be entered and left again during EOTTI. However, the safe state is entered once and maintained in the following.

#### TABLE III

| Time   | Explanation                                                                 |
|--------|-----------------------------------------------------------------------------|
| $t_1$  | “time when a fault manifests itself as a significant loss of the specified functionality” [5] |
| $t_2$  | “time when the fault is detected” [5], i.e. actual point in time when the fault is detected by a specified SM |
| $t_3$  | “time when the item completes changing its operation mode, end of the [FRTI]” [5], i.e. actual point in time when transition to EO by a specified SM is completed |
| $t_4$  | end of FHTI, i.e. latest point in time to handle the fault by a SM before a SG violation cannot be prevented any longer [1] |
| $t_5$  | end of [FHTI] [5], i.e. point in time when the SG violation potentially occurs if fault is not handled properly, e.g. due to diagnostic slip, or if no SM is applied at all |
| $t_6$  | “time when the item reaches the safe state” [5], i.e. actual point in time when the EO is completed |
| $t_7$  | “maximum allowable time to reach the safe state” [5], i.e. latest point in time until an unreasonable risk can be argued |

In this example, the safety relevance of the VOS depends only on vehicle speed. In the following sections, a specific fault scenario of the power supply system is explained in accordance with Fig. 5. It is assumed that a safe state cannot be reached within $FHTI_{max}$ respectively FTTI.

#### 1) NOMINAL OPERATION

The starting point of the investigation is a nominal operation without any fault. At a random point in time, a fault occurs in the main power supply.

#### 2) FUNCTIONALITY UNAVAILABLE

After the fault, the steering functionality is not available for the duration of the FHTI of the corresponding SM:

1) Fault detection: Within the fault detection time interval (FDTI), the fault is not detected, i.e. no information regarding the unavailability of the steering functionality is available. Latest after the FDTI expires, the fault is detected by an SM.

2) Fault reaction: Within the fault reaction time interval (FRTI), the EPS switches its power input to the backup power supply and enters the EO.

The sum of FDTI and FRTI is defined as FHTI.

#### FIGURE 5.

Timing properties according to ISO 26262 – combined with FHTI$_{max}$ definition – mapped to the VOSs in case of EO for cold redundancy.
4) FUNCTIONALITY DISABLED
As introduced at the beginning of this section, the focus of this example is on safe state 1. Thereby, the vehicle standstill can be considered as a safe state because no SaRa requirement is allocated from the SG “Prevent sudden loss of steering assist” to the power supply system at the vehicle standstill. The vehicle standstill shall not only be reached within EOTTI; additionally, it shall be maintained in this VOS after EOTTI, as long as the vehicle is not repaired.

Exceeding the EOTTI would result in an unreasonable level of risk because the time duration relying only on the backup system is inadmissible. At the end of the EOTTI, several safe states as a subset of safe state 1 are possible, e.g.:

1) Continuation of the journey after the EPS is faded out with a limited slope and thus permanently switched off within the EOTTI. In addition, the driver is notified about the unavailability of the EPS sufficiently early.

2) The item reaches the workshop within EOTTI and, continuation of the journey is prohibited. After repairing the power supply system, the item can be used again without restrictions.

3) The item is parked in a minimal risk condition within EOTTI and, continuation of the journey is prohibited. After towing the vehicle to a workshop and repairing the power supply system, the previously failed functionality can be used again without restrictions.

Regarding 1), the safe state definition may conflict with other SGs. For example, steering heavy may have to be avoided with ASIL A after a loss of assistance according to vehicle hazard No. 3 in [2].

C. EXEMPLARY DERIVATION OF EOTTI BASED ON RANDOM HARDWARE FAULTS
As introduced in Section II-D, two equations are provided in ISO 26262 to derive a first-order approximation of the maximum EOTTI based on random hardware faults. To derive the EOTTI for the example provided in Section II-A, the following assumptions and mappings are made:

1) IF: is represented by the main power supply T.30_q;
2) SM1: composed of a switching mechanism to activate the backup system and the backup system itself;
3) SM2: not considered – no SM is considered to prevent a fault from being latent in SM1;
4) Active switching: Information is available as soon as the transition to the backup system is completed, i.e. \( \lambda_{IF,DPF,Detected} = \lambda_{IF,DPF} \) and \( \lambda_{IF,DPF,Latent} = 0 \);
5) Target safe state: safe state 1 – vehicle in standstill, where the availability of the functionality is no longer safety relevant;
6) \( T_{Life} = 8000 \) h.

In Table IV, exemplary failure rates of these components are shown. For simplification, the availability of the EPS itself is not considered in this evaluation.

| TABLE IV |
| --- |
| **Exemplary Failure Rates for the Architecture Shown in Fig. 4** |
| Component name | IF Main supply | SM1 Switching | Backup supply |
| --- | --- | --- | --- |
| Failure rate [FIT] | 10000 | 100 | 1000 |
| FM | safe | FM1 | safe | FM2 | safe | FM3 |
| FMC \( w.r.t. \) violation of SG | - | yes | - | no | - | No |
| SPF/RF [FIT] | - | 70 | - | - | - | - |
| DPF* [FIT] | - | 6930 | - | 20 | - | 800 |
| DPF\( \text{latent} \) [FIT] | - | 0 | - | 20 | - | 800 |
| DPF\( \text{detected} \) [FIT] | - | 6930 | - | 0 | - | 0 |

*failure mode; †failure mode coverage; ‡dual point fault

As explained in Section II-D 1), the backup system may fail even if it has not yet been activated. In this example, the averaged probability of failure per hour of SM1 in passive mode, during the transition to the backup system and during EO is assumed to be constant and equal for all VOSs, as shown in Table IV. According to (7), this results in:

\[ T_{EOTTI(7)} \leq 1279 \text{ h}, \]  

Additionally, (15) is applied while considering \( \lambda_{SM1,DFP} := \lambda_{avg,degr,FIT} = \lambda_{avg,degr,EOTTI} \) and the worst-case boundary condition \( T_{FIT} := T_{FIT\text{max}} = 100 \mu \text{s} \). This results in:

\[ T_{EOTTI(11)} \leq 975 \text{ h}, \]  

In this example, the shortest calculated \( T_{EOTTI} \) is considered according to the conservative approach provided in ISO 26262-10:2018, 12.3.1.2, although the application of (11) is not required by the standard, i.e. \( T_{EOTTI} \leq 975 \) h is set as the upper boundary. This typically needs to be refined due to other systematic boundaries, e.g. the capacity of the backup power storage – depending on its size – and in order to adequately reduce the risk due to systematic faults as explained in Section II-D 3).

The resulting PMHF can be calculated according to (5) considering the actual time in the EO. In the worst-case scenario, the full budget of \( T_{EOTTI} \) is required to achieve a safe state, i.e. \( T_{EO} = T_{EOTTI} = 975 \) h. Analogous to the assumptions in Section II-D 1) Pattern 2 and Pattern 3 have no impact on the PMHF for this example. The residual failure rate is calculated as \( \lambda_{RF} = \left(1 - FC_{SM1}\right) \lambda_{IF} \). Considering the aforementioned assumptions, this results in (19):

\[ PMHF = \lambda_{RF} \]

Pattern 1 \[ + 0.5 \cdot \lambda_{SM1,DPF,Latent} \cdot \lambda_{IF,DFP} \cdot T_{Life} \]
Pattern 4 \[ + \lambda_{IF,DFP,Detected} \cdot \lambda_{SM1,DFP} \cdot T_{EOTTI(11)} \approx 98 \text{ FIT}. \]  

For sake of completeness, the single-point fault metric (SPFM) and the latent fault metric (LFM) is evaluated as well.
– according to ISO 26262-5:2018, Annex C. Thereby, \( \sum_{SR,HW} \lambda_X \) represents the “sum of \( \lambda_X \) of the safety-related hardware elements of the item to be considered for the metrics” [12]:

\[
SPFM = 1 - \frac{\sum_{SR,HW} (\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW} \lambda_{SR}} = 99.4\%,
\]

\[
LFM = 1 - \frac{\sum_{SR,HW} (\lambda_{MPF,latent} - \lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW} (\lambda_{SR} - \lambda_{SPF} + \lambda_{RF})} = 92.6\%.
\]

Thus, the item can be considered as ASIL C-compliant as far as the residual risk due to random hardware faults is concerned.

D. TRANSFER OF RESULTS TO THE CONTEXT OF WARM REDUNDANCY

The examples and definitions in ISO 26262 in the context of an SG specifying an SaRA requirement and EO focus on cold redundancy, where the focus is on the loss of the main system. While guidelines and requirements concerning random hardware faults in the intended functionality and in the backup are provided – driven by the HW-metrics – no guidelines and only ambiguous requirements are provided regarding the required systematic integrity for handling faults in the backup. Two high-level interpretations of ISO 26262 may be argued to cover this case:

1) Interpretation 1: No EO is present after a fault in the backup system, since no active fault reaction is necessary to avoid a SG violation. Instead, SMs only to prevent faults from being latent may be applied. Those SMs can be implemented with reduced ASIL capability according to ISO 26262-4:2018, 6.4.2.5. However, this way of argumentation contrasts to the common interpretation that if the “ASIL capability of the item is lower than the initially specified ASIL rating of the hazard” [5], an EO is present. This may lead to an asymmetry in the required ASIL capability of the SM to handle a fault in the main system compared with the backup system.

2) Interpretation 2: EO is present after fault in the backup system since the actual “ASIL capability of the item is lower than the initially specified ASIL rating of the hazard” [5] after loss of redundancy. Thus, SMs may need to be implemented with the initial specified ASIL to ensure a transition to safe state within EOTTI and to restrict possible VOS after EOTTI according to ISO 26262-10:2018, 12.2.4.2 Note 6 [5].

IV. CONCLUSION

To standardize the safety process and improve its applicability in the power supply domain, one of the remaining challenges is the application of emergency operation to fault-tolerant power supply systems. This study contributes to further standardization of functional safety in the power supply domain by applying EO to an exemplary use case.

If a fault in the main system potentially violates an SG and a safe state cannot be reached within the maximum fault handling time interval, the backup system can be activated in a fault tolerant item to prevent an SG violation. If the actual ASIL capability of the backup system itself is lower than the initially specified ASIL rating for the hazard, an emergency operation is entered. The emergency operation is still considered to be free from unreasonable risk due to its timing restrictions. The definitions and examples provided in ISO 26262 in the context of emergency operation focus on cold redundancies. In this study, the most fundamental properties of emergency operation according to ISO 26262 are elaborated. A major point is the derivation of the maximum permissible emergency operation tolerance time interval. These definitions are mapped to exemplary power supply architectures. However, fault-tolerant items based on warm redundancy are of particular interest for the power supply domain, as they represent the preferred implementation in the market. Besides the HW-metric targets, no guidelines and only ambiguous requirements are provided in ISO 26262 for this use case. To fill this gap, an outlook for future research activities is provided.

ACKNOWLEDGMENT

Thanks to Armin Köhler, David Linden, Florian Cramme, Markus Wörz and Dr. Tobias Traub for inspiring discussions about the applicability of the provided definitions and interpretations. Additionally, we want to thank Dr. Steffen Krüger, chairman of the working group VDA 450, and all members of the VDA 450 for their valuable discussions and their contribution towards further standardization of power supply systems.

REFERENCES

[1] P. Kilian et al., “Principle Guidelines for Safe Power Supply Systems Development,” in IEEE Access, vol. 9, pp. 107751-107766, 2021, doi: 10.1109/ACCESS.2021.3100711
[2] GB 17675-2021, “Steering system of motor vehicles. Basic Requirements,” 2021.
[3] P. Kilian et al., “Safety-Related Availability in the Power Supply Domain,” in IEEE Access, to be published
[4] ISO 26262-10:2018(E), “Road vehicles – Functional safety – Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses,” 2018.
[5] ISO 26262-10:2018(E), “Road vehicles – Functional safety – Part 10: Guidelines on ISO 26262,” 2018.
[6] ISO 26262-1:2018(E), “Road vehicles – Functional safety – Part 1: Vocabulary,” 2018.
[7] ECE R 13-H, “Regulation No 13-H of the Economic Commission for Europe of the United Nations (UNECE) — Uniform provisions concerning the approval of passenger cars with regard to braking,”, 2015.
[8] A. Birolini, “Reliability Engineering: Theory and Practice,” 2nd ed. New York, NY, USA: Springer, 2017 DOI 10.1007/978-3-662-54209-5
[9] C. Gebauer, “Fail operational and ISO 26262 2nd edition,” presented at the safetronic. 2018, Stuttgart, Germany, Nov. 13-14, 2018.
[10] F. Edler, M. Soden, R. Hankammer, “Fehlverhaltenanalyse in Theorie und Praxis - Grundlagen und Anwendung der Methode”, 2015, München/Berlin
[11] B. Bertsche, “Reliability in Automotive and Mechanical Engineering,” Berlin: Springer, 2008, DOI 10.1007/978-3-540-34282-3.
[12] ISO 26262-5:2018(E), “Road vehicles – Functional safety – Part 5: Product development at the hardware level,” 2018
[13] ISO 26262-3:2018(E), “Road vehicles – Functional safety – Part 3: Concept phase,” 2018.
[14] VDA 450, “VDA Empfehlung für einen Mindestsicherheitsstandard der Energieversorgung und deren Elemente im Rahmen der ISO-26262,” draft, 2021.
[15] A. Koehler and B. Bertsche, “An approach of fail operational power supply for next generation vehicle powernet architectures,” in Proc. 30th Eur. Saf. Rel. Conf. 15th Probabilistic Saf. Assessment Manage. Conf. (ESREL-PSAM), Venice, Italy, Nov. 2020, pp. 60-67, DOI 10.3850/978-981-14-8593-0.

Philipp Kilian was born in Göggingen, Germany in 1995. He studied mechanical engineering at the University of Stuttgart and earned his Master of Science degree in 2020.
He is working as a doctoral student in the field of functional safety in the area of automotive electronics – power supply system.
He is pursuing his PhD studies with focus on modular and scalable safety concepts in cooperation with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart.

Oliver Koller was born in Stuttgart, Germany in 1985. He studied electrical engineering and information technology at the University of Stuttgart and earned his diploma degree in 2011. From 2011 he started his PhD studies in the field of Reliability Engineering of 48V Mild Hybrid systems at Robert Bosch GmbH in cooperation with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart which he finished in 2016.
Since 2018 he is leading the systems engineering and application development for power supply components and since 2019 he is part of the VDA450 group “power supply systems for automated driving”.

Patrick van Bergen was born in Waiblingen, Germany in 1989. He studied mechanical engineering at the Reutlingen University and University of Stuttgart and earned his Master of Science degree in 2015.
He was working as a doctoral student in the field of functional safety for automotive electronics – power supply system with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart. He began his professional career at Robert Bosch GmbH 2018 and is now coordinating the functional safety topics in the power supply system area.

Carsten Gebauer began his professional career at the Robert Bosch GmbH in 2000. He has been working in the field of safety since 2004. In 2009 he became a member of the ISO/TC 22/SC 32/WG 8, the working group tasked with the compilation of ISO 26262 next to other automotive safety standards.

Frederic Heidinger was born in Freiburg, Germany in 1986. He studied mechanical engineering at the University of Stuttgart and earned his diploma degree in 2014. Between 2014 and 2017, he worked at the Institute of Thermal Turbomachinery of the University of Stuttgart as a research engineer. From 2017 he worked as doctoral student in the field of reliability of automotive electronics – power supply systems at the Robert Bosch GmbH. As of 2019 he was leading the systems engineering development team for power supply components. Since 2021 he is section manager for the systems engineering of power supply components.

Martin Dazer received the B.Sc. degree in mechanical engineering from Baden-Württemberg Cooperative State University (DHBW) in 2011, the M.Sc. degree in mechanical engineering from University of Stuttgart in 2015 and the Dr.-Ing. degree in reliability engineering from University of Stuttgart in 2019.
From 2015 to 2018 he was a research assistant at the Institute of Machine Components. He is currently head of the reliability and drive technology department at the Institute of Machine Components. His research covers a multitude of aspects of reliability engineering with its main focus on life testing.
He is founder and consultant of RefTest-Solutions at the TTI GmbH Stuttgart, Germany. He is member of the technical committee of reliability management of the VDI (Verein Deutscher Ingenieure), and member of the advisory board of safety and reliability of the VDI, Germany."