Emergency Operation in the Power Supply Domain Focusing on Warm Redundancy

PHILIPP KILIAN1, PATRICK VAN BERGEN2, OLIVER KOLLER3, CARSTEN GEBAUER4, FREDERIC HEIDINGER2, AND MARTIN DAZER1

1Institute of Machine Components, University of Stuttgart, 70569 Stuttgart, Germany
2Cross-Domain Computing Solutions, Product Area Integrating Devices–Engineering Vehicle Systems (XC-AN/EPI1), Robert Bosch GmbH, 70499 Stuttgart, Germany
3Cross-Domain Computing Solutions, Product Area Integrating Devices–Senior Expert Powernet Strategy (XC-AN/PAI), Robert Bosch GmbH, 70499 Stuttgart, Germany
4Systems Engineering, Bosch Center of Competence Vehicle Safety (M/ENG-CVS), Robert Bosch GmbH, 71636 Ludwigsburg, Germany

Corresponding author: Philipp Kilian (philipp.kilian@ima.uni-stuttgart.de)

ABSTRACT To cope with the megatrends electrification, automated driving, and connectivity, new functionalities and E/E systems must be developed, which require a safe power supply. This leads to increased functional safety requirements for the power supply system, particularly regarding availability. Fault tolerance measures can be implemented to comply with an SG specifying a SaRA requirement. In this case, EO may be necessary to reach a defined safe state. However, there is some ambiguity in ISO 26262 regarding the necessary integrity with which the EO shall be implemented – this becomes in particular obvious in the case of warm redundancy. According to ISO 26262, the EO is entered once the failure of an element is controlled by an explicit fault handling, i.e., prevented from violating an SG, and the remaining ASIL capability of the item after the failure is lower than the required ASIL capability for the allowed VOS. However, in the context of warm redundancy, the EO can be automatically entered in the case of an element failure without an explicit fault handling. The objective of this paper is to transfer the concept of EO, as defined in ISO 26262, to warm-redundant power supply systems because warm-redundant power supply systems have a high level of market penetration. Besides a detailed evaluation of time dependencies, new guidelines concerning the required systematic integrity for SMs implementing EO are provided.

INDEX TERMS Automotive electronics, automotive engineering, emergency power supplies, functional safety, ISO 26262, power supplies, reliability, requirements engineering, vehicle safety.

NOMENCLATURE

| ASIL | Automotive safety integrity level |
| DPF | Dual-point fault |
| E/E | Electric and/or electronic |
| EBS | Electronic battery sensor |
| EO | Emergency operation |
| EOTI | Emergency operation time interval |
| EOTTI | Emergency operation tolerance time interval |
| EPS | Electrical power steering |
| FDTI | Fault detection time interval |
| FHTI | Fault handling time interval |
| FMC | Failure mode coverage |
| FRTI | Fault reaction time interval |
| FTTI | Fault tolerant time interval |
| HV | High-voltage |
| HW | Hardware |
| IF | Intended functionality |
| ISO | International organization for standardization |
| LFM | Latent fault metric |
| MPF | Multiple-point fault |
| MPFDTI | Multiple-point fault detection time interval |
| MPFDTI_{max} | Maximum multiple-point fault detection time interval |
| MPFHTI | Maximum multiple-point fault handling time interval |

The associate editor coordinating the review of this manuscript and approving it for publication was Dusmanta Kumar Mohanta3.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
MPFR $	ext{max}$ \text{Maximum multiple-point fault reaction time interval}
MRM \text{Minimal risk maneuver}
PMHF \text{Probabilistic metric for random hardware failures}
QM \text{Quality management}
RF \text{Residual fault}
SaRA \text{Safety-related availability}
SG \text{Safety goal}
SM \text{Safety mechanism}
SOTIF \text{Safety of the intended functionality}
SPF \text{Single-point fault}
SPFM \text{Single-point fault metric}
VOS \text{Vehicle operating state}
$T_x$ \text{Time variable of a specific time interval $x$}
$\lambda_{\text{target}}$ \text{PMHF target value}
$\lambda_{x,y}$ \text{Failure rate of element $x$ for failure mode $y$}

I. INTRODUCTION

The relevance of safety applications within the automotive industry is continuously increasing, especially driven by the megatrends electrification, automated driving, and connectivity. The ISO 26262 series of standards shall be applied in the automotive industry to ensure functional safety-compliance of safety-related E/E systems, which became mandatory for homologation driven by new legislation in China since 2022 [1], [2]. The power supply system is essential because it represents a shared resource for several safety-related E/E systems [3]. Without power, E/E systems typically cannot provide their specified function [3]. If the loss of a vehicle function can lead to a hazard, SaRA requirements are allocated to the systems necessary to implement this vehicle function, which typically includes the power supply system [3]. If this is the case, the power supply system is required to be available to ensure safe vehicle behavior; thus, state-of-the-art fail-passive approaches are not applicable [3].

Fault tolerance measures are applicable to comply with an SG specifying a SaRA requirement. In this case, EO may be necessary to reach a safe state after the loss of redundancy. According to ISO 26262, an EO is entered if a hazard is prevented from occurring but a safe state cannot be reached within the FHTI $	ext{max}$ respectively FTTI. As evaluated in [4], the guidelines and requirements in ISO 26262 implicitly focus on cold redundancy with a fault in the main system – potentially, directly violating an SG. There are ambiguities and inconsistencies when applying these to faults in backup systems. The same applies to items that implement warm redundancy. In both cases, no explicit fault handling is necessary in order to prevent the immediate occurrence of a hazardous event. Thus, the concept of EO must be adapted and extended to include warm redundancy.

A. ORGANIZATION OF THE ARTICLE

In Section I, general aspects of functional safety in the context of the power supply domain are discussed with focus on SaRA and EO. In Section II, the concept of EO as provided in ISO 26262 is extended and adapted for warm redundancy. In Section III, the newly introduced guidelines and requirements are applied to an exemplary warm-redundant power supply architecture. Finally, EO, including the newly introduced extensions, is summarized in Section IV.

In this article, faults that require an explicit and immediate fault reaction in order to prevent the violation of the SG are classified as “faults with the potential to directly violate the SG”. For this class, the fault handling shall be completed within the FHTI $	ext{max}$ respectively FTTI to prevent the hazard from occurring. Note: This terminology differs slightly from [5] and [6] where the classification considers the potential to directly violate the SG in absence of a SM, independent of the necessity of an explicit fault handling. Furthermore, the use of the term “DPF” or “MPF” is restricted to those DPFs/MPFs not requiring an explicit fault reaction to prevent the hazard from occurring. Thus, faults with the potential to directly violate an SG, which are detected and controlled by an SM, are not referred to as DPFs/MPFs within this article, contrary to ISO 26262 [5], [6], [7]. Additionally, the use of the term “warm redundancy” is restricted to warm redundancies without faults potentially directly violating the SG, i.e., no explicit fault handling is necessary to prevent any individual fault from violating the SG. This is not a limiting restriction within the context of EO since warm redundancies requiring explicit fault reactions are, as far as the EO concept is concerned, not different from cold redundancies.

B. OBJECTIVE

Warm redundancy is of particular interest for the power supply domain. Neither in ISO 26262 nor other scientific publications are guidelines and unambiguous requirements provided on how faults not directly violating the SG – as in the case if warm redundancy – are handled in the context of SaRA and EO from functional safety point of view. Even though EO is applied for an item implementing warm redundancy in [8], the basic framework to do so is not derived in a systematic manner as well as not discussed from all relevant point of views. The objective of this paper is:

1) to evaluate the concept of EO in the context of warm redundancy;
2) to adapt the currently in ISO 26262 provided definitions and properties of EO in a systematic and holistic manner;
3) to apply the introduced concept to an example of the power supply domain.

Although the concept is derived for an application in the power supply domain, it is generalized in a manner to be also applied in other domains.

C. POWER SUPPLY SYSTEM AS SHARED RESOURCE

In general, power supply systems are considered shared resources because a fault in them affects several other elements and systems [3]. Due to the growing relevance of safe power supply, the power supply system itself is increasingly...
discussed in scientific publications, see e.g. [1], [8], [9], [10], [11], [12], or [13]. Main safety requirements for the power supply system are [1], [3], [4], [8]:

1) provide safe power feed;
2) provide safe power distribution; and
3) ensure freedom from interference.

For comparability to [4] – focusing on EO in the context of cold redundancy – the same use case as provided in Table 1 in [4] is considered within this paper, too. Thus, the SG “Prevent sudden loss of steering assist” shall be fulfilled by the steering entity – rated with ASIL C [1], [3], [4]. The entity concept in general was described in [14]. If the steering assist functionality is suddenly lost, a hazardous event potentially occurs [3], [4]. Thus, a SaRA requirement is specified for the steering entity, which is applicable during VOS driving but, e.g., not in vehicle standstill [3], [4]. VOS is defined as the “operating mode in combination with the operational situation” [7]. The steering entity comprises the items “EPS” and “power supply system”; thus, the SaRA requirement of the steering entity is allocated to the EPS and the power supply system [3], [4]. Further details about this use case are provided in [3] and [4].

D. SAFETY-RELATED AVAILABILITY IN THE POWER SUPPLY DOMAIN

According to [1], “SaRA requirements request the availability of a function with the corresponding ASIL rating of the SG or requirement”. They can be addressed by safety measures focusing on 1) fault avoidance; 2) fault forecasting; and/or fault tolerance [3], [5], [9], [10]. A detailed evaluation of SaRA in general and its application in the power supply domain was presented in [3].

Fault tolerance measures are implemented by redundancy. Generic redundancy concepts are provided, e.g., in [15] and [16]. Within this paper, a redundant power supply system is considered a basic premise – even though redundancy in general is typically accompanied by a negative impact on system costs, packaging, and weight [3]. The decision between measures focusing on fault avoidance, fault forecasting and/or fault tolerance – to comply with a SaRA-requirement – is not part of this paper. Redundancy in the context of power supply systems may also be mandatory for homologation due to technical regulations [17]. Thereby, the performance of the backup system during nominal operation can be refined, e.g. according to Biroolini as follows [18]:

1) Cold redundancy – also referred to as standby redundancy: “Redundant elements are subjected to no load until they become operating”; “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”; the failure rate during nominal operation “is somewhere between active and standby” – thereby, “until they become operating” is not defined unambiguously; however, in a previous version of [18] it is defined more precisely as “until one of the operating elements fails” [19];
3) Hot redundancy – also referred to as active redundancy: “Redundant elements are also referred to from the beginning to the same load as operating elements”.

Therefore, an action such as activating or switching to the backup system is required in the case of cold redundancy. However, no action to activate the backup is necessarily required in the case of warm/hot redundancy – according to the premises stated in Section I-B – because the backup system is already active during nominal operation [4].

E. EMERGENCY OPERATION IN THE CONTEXT OF ISO 26262 FOCUSING ON COLD REDUNDANCY

In [7], 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”. As such, the focus is on cold redundancy because with warm or hot redundancy no explicit fault handling – comprising fault detection and reaction – is necessarily required in order to prevent the occurrence of a hazard [4]. The guidelines in [5] also focus on cold redundancy. During EO, the item respectively entity only relies on its backup, whereby its ASIL capability is lower than the ASIL rating of possible hazards [4] – the “functionality is kept operating” [5]. To achieve the absence of unreasonable risk, EO is restricted in time, i.e., by the EOTI [5]. EOTI is defined as “specified time-span during which [EO] can be maintained without an unreasonable level of risk” [7]. The actual time during which EO is maintained is defined as the EOTI [7]. To prevent an SG violation, a safe state shall be reached within EOTI, i.e., $\text{EOTI} \leq \text{EOTTI}$ [5]. A detailed evaluation of EO with a focus on cold redundancy in general and its application in the power supply domain was presented in [4].

According to [4], the two separately described safe states in ISO 26262-10:2018, 12.2.4.2 are equal in their generic form. Thus, the guidelines and requirements specified in ISO 26262 are applicable to both safe states equivalently. Among others, SMs to maintain the safe state, i.e., to prevent entering possible VOSs in which the ASIL rating of possible hazards exceeds the remaining ASIL capability, inherit the initial ASIL according to ISO 26262-10:2018, 12.2.4.2 Note 6 [5].

II. EMERGENCY OPERATION FOCUSING ON WARM REDUNDANCY

The focus of this section is on EO in the context of warm redundancy. Second-order redundancy is assumed; thus, DPFs are of particular relevance. However, the following framework is also transferable to hot redundancy and MPFs in general. Additionally, “item” is considered the highest abstraction layer even though the framework is also applicable to an “entity” as highest abstraction layer.

Regarding random HW faults not directly violating the SG – as typically in the case of warm redundancy – guidelines and requirements are provided driven by the HW-metrics, e.g., in the PMHF calculation according to ISO
In contrast to Birolini, the failure rate of a system in the reserve state is not considered zero in this paper [4]. However, no guidelines and only ambiguous requirements are provided regarding the necessary systematic integrity of SMs which handle faults not directly violating the SG specifying a SaRA requirement. As indicated in [4], two high level interpretations may be argued in the case of a SaRA requirement and warm redundancy:

1) Interpretation 1: The item does not enter an EO after a fault in the backup system since no explicit fault reaction is necessary to avoid an SG violation. Instead, SMs only to prevent faults from being latent may be applied. These SMs can be implemented with reduced ASIL capability according to ISO 26262-4:2018, 6.4.2.5 [20].

2) Interpretation 2: EO is entered after a 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] due to the lost redundancy. Thus, SMs may need to be implemented with the initial specified ASIL of the SG to ensure a transition to a safe state within EOTTI and to restrict possible VOS after EOTTI as stated in ISO 26262-10:2018, 12.2.4.2 Note 6 [5].

According to our interpretation, the most dominant property of the EO as defined in ISO 26262 in combination with an SG specifying a SaRA requirement is that the “ASIL capability of the item is lower than the ASIL rating of the possible hazard” [5] during EO. Although this implies compliance with Interpretation 2, the following framework is based on a combination of Interpretation 1 and 2. This framework provides a consistent and holistic approach how the loss of redundancy is handled in the case of an SG specifying a SaRA requirement considering cold and warm redundancies. Basic premise: An EO can be entered in both redundancy concepts if none of the redundant systems implement the ASIL capability of the initial possible hazard:

1) Cold redundancy:
   a. If the main system fails while the backup system is working, a hazardous event is prevented by an explicit fault handling, i.e., switching to the backup within the FHTI ≤ FHTI max ≤ FTTI, and thus, entering an EO.
   b. If the backup system fails while the main system is working, no explicit fault handling is required to prevent a hazardous event. Nevertheless, an EO is entered because the ASIL capability of the item is lower than the ASIL rating of the possible hazard.

2) Warm redundancy: No formal differentiation is necessary which redundant system fails first. Similar to the scenario in which the backup system fails first in the case of a cold-redundant item, an EO is entered even without an explicit fault handling to prevent a hazardous event.

A. CONCEPT DEFINITION OF EMERGENCY OPERATION INCLUDING WARM REDUNDANCY

Considering EO in the context of warm redundancy does not fully comply with some definitions in ISO 26262. The major difference is the absence of an explicit fault reaction for warm-redundant items, see also Section II-C. As introduced, from our point of view, the decisive property of EO is not the fault reaction aspect; instead, it is the operation after the occurrence of a fault with an ASIL capability lower than the ASIL rating of possible hazards – a characteristic described in [5]. In other words: The ASIL capability of the specified vehicle function concerning its availability is only provided with a too low integrity during EO. Not providing any availability of the specified function is not considered an EO. Therefore, it is reasonable to apply the EO-concept also for warm redundancies where no explicit fault reaction is required to prevent a hazard from occurring after a fault.

The ASIL capability after the loss of either redundant system is typically lower than the ASIL rating of the possible hazard because [4]:

1) Systematic faults: If ASIL decomposition is applied, at least one of the redundant systems only prevents and/or controls systematic faults with a lower ASIL than the hazard’s ASIL rating.

2) Random HW faults: Redundancy enables lower requirements concerning random HW faults for each redundant system. After the loss of redundancy, the remaining system stand-alone typically does not comply with the initial target values for random HW faults. If the safety capability of both redundant systems by themselves – without consideration of the redundant system – would comply with the initial ASIL rating of the hazards, no further action may be required at all after a fault has occurred in one of the systems. However, this approach seems to be an overdesign and thus, is not considered in the following.

In this most dominant property of the EO stated above, only “ASIL capability” is mentioned. However, “QM capability” is also considered to be sufficient even though “QM is not an ASIL” according to ISO 26262-1:2018, 3.117 [7]. This is particularly relevant for the power supply domain, where QM(X) elements are commonly considered a part of an ASIL decomposition. Therefore, QM(X) capability of the backup system is applicable to ensure a safe transition to a safe state within an EO, i.e., it is explicitly considered a valid option – as long as a valid decomposition scheme is used. To prevent misinterpretations, the term “ASIL capability” is replaced by “safety capability” in the following. “Safety capability” comprises “ASIL capability” and “QM capability”.

The relevant properties of EO as currently defined in ISO 26262 are summarized in Table 1 – according to [4]. Additionally, the necessary adaptations and modification to consider EO for an item implementing warm redundancy are highlighted in blue. This framework can be considered a possible extension to ISO 26262. In the following sections, each property is evaluated in detail.
**TABLE 1.** Properties of EO according to ISO 26262 – including additions and adaptions to include warm redundancy.

| Property | Focusing on cold redundancy | Focusing on warm redundancy |
|----------|-----------------------------|-----------------------------|
| EO1      | EO shall be restricted in time by the EOTTI in order to achieve the absence of unreasonable risk, i.e. it is only a temporary operating mode until a safe state is reached within EOTTI – EO is not a safe state itself. | EO is entered as soon as the safety capability is lower than the ASIL rating of the possible hazards due to the occurrence of a fault – no explicit fault handling within FTTI required. |
| EO2      | EO is entered if the occurrence of a hazardous event is prevented within FTTI due to an explicit fault handling but a safe state cannot be reached within FTTI. | EO immediately starts with the occurrence of a corresponding MPF – there is no need for an explicit fault handling to prevent the occurrence of a hazardous event. |
| EO3      | EO shall be triggered within FTTI. | EO is entered automatically by design. |
| EO4      | EO starts after the completion of the explicit fault handling, which is required to prevent the occurrence of the hazardous event, i.e. as soon as switching to the backup is completed. | By design, the specified functionality is available without interruption after the occurrence of a first fault – no unavailability has to be considered. |
| EO5      | EO starts as soon as the specified functionality is available again after the occurrence of a first fault. However, from occurrence of a fault until start of EO, i.e., during FIHTI, the specified functionality may not be available. |  |
| EO6      | EO is maintained during EOTI, whereby the safety capability of the item is lower than the ASIL rating of the possible hazards. | EO is solely relying on one part of the redundant system and thus – during EOTI – a fault in the redundant part of the system potentially leads to a violation of an SG. |
| EO7      | EO is solely relying on the backup system and thus – during EOTI – a fault in the backup potentially leads to a violation of an SG. | |

**B. RELEVANT TIME INTERVALS IN THE CONTEXT OF EMERGENCY OPERATION AND WARM REDUNDANCY**

The focus of this section is on EO1, EO2, EO3 and EO7 as defined in Table 1. In general, EO is entered if – among others – a “safe state […] cannot be timely reached” [7] according to ISO 26262-1:2018, 3.43. Thereby, “timely” is defined more precisely in ISO 26262-4:2018, 6.4.2.2 and ISO 26262-10:2018, 4.4.2.2 as within the FTTI [5], [20].

For warm redundancies, the loss of either redundant system is considered a DPF not yet causing a dual-point failure – if the redundant system does not fail at the same time. Therefore, no hazardous event must be prevented within FIHTI respectively FTTI. Instead, a MPFDTI can be specified to prevent a first DPF from being latent. MPFDTI is defined as “time-span to detect a [MPF] before it can contribute to a multiple-point failure” [7] and is typically longer than FTTI. In Table 2, several definitions, and explanations in the context of MPFDTI from ISO 26262 are summarized.

**TABLE 2. Definitions and explanations in context of MPFDTI in ISO 26262.**

| ISO 26262 Reference | Definition and explanation |
|---------------------|----------------------------|
| 1:2018, 3.98 [7]    | “time-span to detect a [MPF] before it can contribute to a multiple-point failure” |
| 4:2018, 6.4.2.4 [20]| “A second-order multiple-point failure comprises two faults, separated by the [MPFDTI]” |
| 5:2018, 6.4.8 Note 1 [6] | “If the corresponding safety concept does not prescribe specific values, the [MPFDTI] can be specified to be equal to or lower than the item’s “power-up to power-down” cycle” |
| 5:2018, 7.4.3.4 [6] | “to prevent a fault from being latent […] evidence of the ability of the [SM] to detect faults and to achieve or maintain a safe state or to notify them to the driver, within the acceptable [MPFDTI] for latent faults”, i.e., it cannot be [MPFDTI] is longer than the relevant [MPFDTI] for latent faults” |

1) **INTRODUCTION OF MAXIMUM MULTIPLE-POINT FAULT DETECTION TIME INTERVAL**

To prevent misinterpretations, we suggest renaming MPFDTI as the MPFDTI\(_{\text{max}}\) – analogous to FHTI\(_{\text{max}}\) [1], [3]. MPFDTI\(_{\text{max}}\) represents the maximum available time budget in the requirements specification to detect a first DPF. The corresponding implemented SM detects the first DPF within the FDTI. Note: The FDTI itself is a general property of an SM that describes the time the SM needs to detect the fault under consideration. If the fault under consideration needs to be detected within the FIHTI\(_{\text{max}}\) or within the MPFDTI\(_{\text{max}}\) determines the maximum value to which FDTI is compared to but has no impact on the name of the term itself. Based on ISO 26262-5:2018, 6.4.8 Note 1, MPFDTI\(_{\text{max}}\) = 1 driving cycle = 1 h is considered in the following [6]. This is a valid definition if the safety concept does not prescribe any specific values [6].

2) **INTRODUCTION OF MAXIMUM MULTIPLE-POINT FAULT HANDLING TIME INTERVAL**

The definitions in ISO 26262-1:2018, 3.98 and ISO 26262-5:2018, 7.4.3.4 concerning MPFDTI are not fully consistent with each other:

1) ISO 26262-1:2018, 3.98: The focus is only on the fault detection [7];
2) ISO 26262-5:2018, 7.4.3.4: The focus is on the fault detection and fault reaction because to “achieve or maintain a safe state” [6] also a fault reaction is generally required.

From a practical application point of view, this wording inconsistency may not impact the functional safety concept if FRTI \(\ll\) FDTI. In this case, the probability of a second DPF leading to a dual-point failure during FRTI has only a minor impact on the safety evaluation, e.g., the PMHF calculation, compared to FDTI. FRTI \(\ll\) FDTI is typically the case for fail-passive items. Thereby, FDTI may be in the range of one hour. The time to react on a fault (FRTI),
e.g., switching off the functionality is typically completed within the range of several microseconds or milliseconds. In the case of an SG specifying a SaRA requirement and especially for higher automation degrees, the fault reaction may be in the range of seconds up to hours. Therefore, the duration of the fault reaction cannot be neglected any longer and the definitions in ISO 26262 should be revised. To adapt and/or extend the definitions provided in ISO 26262, the more general MPFHTI\(_{\text{max}}\) is introduced according to [8].

MPFHTI\(_{\text{max}}\) is more universal than MPFDTI\(_{\text{max}}\) by composing fault detection and fault reaction. Instead of only replacing MPFDTI\(_{\text{max}}\) with MPFHTI\(_{\text{max}}\), the introduction of MPFHTI\(_{\text{max}}\) as an extension ensures consistency with current safety concepts as explained previously. The MPFHTI\(_{\text{max}}\) shall be used for time budgeting as part of the requirements specification in a hierarchical breakdown according to [1] or [6] in the left part of the V-model. A DPF shall be handled within MPFHTI\(_{\text{max}}\) before it can contribute to a dual-/multiple-point failure – if applicable. In the right part of the V-model, evidence shall be provided that the FHTI – as an actual characteristic of an implemented SM – for handling the DPF is not greater than the specified MPFHTI\(_{\text{max}}\).

In the case of a dual-point failure, MPFHTI\(_{\text{max}}\) represents the time interval between two corresponding DPFs. If a first DPF causes a reduced safety capability of the item, it is considered equal to EOTTI. Therefore, it is ensured that SMs implemented to transition to a safe state are sufficiently fast and no contradictions between MPFHTI\(_{\text{max}}\) and EOTTI occur:

\[
T_{\text{MPFHTI,max}} = T_{\text{EOTTI}}. \tag{1}
\]

MPFHTI\(_{\text{max}}\) is derived analogously to EOTTI. Thus, as a mandatory requirement, MPFHTI\(_{\text{max}}\) is derived based on the PMHF calculation – e.g., according to ISO 26262-10:2018, 12.3.1.2. Vice versa, the time-span during which a first fault is present in the item can be considered in the PMHF calculation, e.g. according to ISO 26262-10:2018, 8.3.2.4 by \(T_{\text{service}} = T_{\text{EOTI}}\). Additionally, MPFHTI\(_{\text{max}}\) may be further limited by solely considering the operation after a first fault according to ISO 26262-10:2018, 12.3.1.1. As introduced in [4], the quantitatively derived MPFHTI\(_{\text{max}}\) based on random HW faults may need to be shortened due to systematic effects because the conditional probability of a second fault being of systematic nature is typically far higher than being a random HW fault [4]. For more details on the derivation of EOTTI, please refer to [4] and [5]. In general, the specification of MPFHTI\(_{\text{max}}\) may be interpreted as a tradeoff between functional safety, SOTIF and customer satisfaction:

1) From functional safety point of view: The fault shall be detected, and the item shall complete its transition to a safe state as soon as possible in order to keep the time in which a second fault can occur as short as possible – leading to short MPFHTI\(_{\text{max}}\).

2) From SOTIF point of view: Different maneuvers are associated with different levels of risk, e.g., an emergency full stop within the lane on a busy highway will result in a higher level of risk of causing an accident with other traffic participants than a lane change to the emergency lane and stopping there.

3) From customer satisfaction point of view: False-positive fault detections shall be avoided by de-bouncing of errors, e.g., implementing error counters requiring fault detection more than once before triggering an error reaction, and the driver shall have sufficient time to reach a safe state – leading to long MPFHTI\(_{\text{max}}\).

Additionally, further technical recommendations and/or regulations may affect the definition of MPFHTI\(_{\text{max}}\). For example, in [21] it is required “to carry out at least 24 ‘figure of eight’ maneuvers [in] the event of a failure of the energy source of the control transmission” [21]. Thus, MPFHTI\(_{\text{max}}\) may need to be long enough to be able to execute this maneuver. If the resulting MPFHTI\(_{\text{max}}\) is shorter, the design of the item shall be adapted. Because an EO is entered if the safety capability of the item is reduced after a first DPF, the safe states as defined in the context of EO are applicable at the end of MPFHTI\(_{\text{max}}\), see e.g., ISO 26262-10:2018, 12.2.4.2.

By considering MPFHTI\(_{\text{max}}\) as extension to MPFDTI\(_{\text{max}}\), additionally, the commonly used assumption MPFDTI\(_{\text{max}} = 1\) h can be considered a plausibility check. If the derived MPFHTI\(_{\text{max}}\) is (much) greater than 1 h, MPFDTI\(_{\text{max}} = 1\) h can be considered the starting point for designing the detection mechanism. However, this is only a guideline – the relevant requirement is FHTI \(\leq\) MPFHTI\(_{\text{max}}\). If the resulting MPFHTI\(_{\text{max}}\) is shorter than 1 h, it is obvious that the assumption MPFDTI\(_{\text{max}} = 1\) h according to ISO 26262-5:2018, 6.4.8 Note 1 must be revised.

3) INTRODUCTION OF MAXIMUM MULTIPLE-POINT FAULT REACTION TIME INTERVAL

For the sake of completeness, additionally, the maximum MPFRTI\(_{\text{max}}\) is introduced for time budgeting as part of the requirements specification. However, a clear distinction between MPFDTI\(_{\text{max}}\) and MPFRTI\(_{\text{max}}\) is not necessarily required, as long as the actual time to handle the MPF by a specific SM, i.e., FHTI, is not greater than the specified MPFHTI\(_{\text{max}}\). Note: Regarding a RF, the equivalent FHTI \(\leq\) MPFHTI\(_{\text{max}}\) is not refined in a maximum fault detection time interval and a maximum fault reaction time interval – even if this might make sense for certain scenarios.

MPFRTI\(_{\text{max}}\) is part of the requirements specification, whereby the sum of MPFDTI\(_{\text{max}}\) and MPFRTI\(_{\text{max}}\) shall be not greater than MPFHTI\(_{\text{max}}\), i.e., MPFDTI\(_{\text{max}}\) + MPFRTI\(_{\text{max}}\) \(\leq\) MPFHTI\(_{\text{max}}\). Thereby, MPFRTI\(_{\text{max}}\) represents the time budget for the driver and/or the item to transition to a safe state while a first fault is present. This includes, e.g., the time for a MRM or the time for the driver to bring the vehicle to a workshop.

4) SUMMARY OF PROPOSED ADAPTATIONS AND EXTENSION TO ISO 26262 TIME INTERVALS

The proposed extensions to the current definitions in ISO 26262 concerning the timing requirements are summarized...
in Table 3. Changes compared with Table 2 are highlighted in blue. Whereas the focus of ISO 26262-5:2018, 7.4.3.4 is only on “prevent a fault from being latent” [6], the focus shall be on handling a DPF before it can contribute to a dual-point failure, i.e., comprising fault detection and fault reaction.

By these adaptions, fail-passive items can still be addressed without changes by considering MPFDTI\(_{\text{max}}\) = MPFHTI\(_{\text{max}}\). However, more use cases can be addressed; especially use cases with SMs including a timely significant fault reaction after a first fault not directly violating the SG – as in the case of warm redundancy and an SG specifying a SaRA requirement.

| Table 3. Proposal to adapt definitions in ISO 26262 in context of MPFDTI. |
|---------------------------------------------|
| (ISO 26262) Reference | Description + definition |
| Newly introduced | MPFHTI\(_{\text{max}}\) (according to ISO 26262-1:2018, 3.98): “maximum time-span to handle a [MPF] before it can contribute to a multiple-point failure” |
| 2018, 3.98 adapted | MPFDTI\(_{\text{max}}\): “maximum time-span to detect a [MPF] before it can contribute to a multiple-point failure” |
| 2018, 4.4.2.4 adapted | MPFHTI\(_{\text{max}}\): “A second-order multiple-point failure comprises two faults, separated by the [MPFHTI\(_{\text{max}}\)]” |
| 2018, 4.4.8 Note 1 adapted | MPFDTI\(_{\text{max}}\): “if the corresponding safety concept does not prescribe specific values, the [MPFDTI\(_{\text{max}}\)] can be specified to be equal to or lower than the item’s "power-up to power-down cycle"” |
| 2018, 7.4.3.4 adapted | MPFHTI\(_{\text{max}}\): “evidence of the ability of the [SM] to detect failures and to achieve or maintain a safe state or to notify them to the driver, within the acceptable [MPFHTI\(_{\text{max}}\)] for latent faults”, i.e., a latent MPF “cannot be considered covered if the [FHTI] of the associated [SM] is longer than the relevant [MPFHTI\(_{\text{max}}\)] for latent faults” |
| Newly introduced | MPFHTI\(_{\text{max}}\): maximum time-span from the detection of a MPF until a safe state is reached |

In summary, if the remaining safety capability of the item after a first fault is lower than the ASIL rating of the possible hazard, an EO is entered in the following cases:

1) The first fault has the potential to directly violate the SG; an SM is implemented to activate the backup functionality within the FHTI\(_{\text{max}}\) respectively FTTI to prevent the occurrence of a hazardous event; and a safe state cannot be reached within FHTI\(_{\text{max}}\) respectively FTTI. In this case, the maximum time-span relying solely on the backup functionality is defined as EOTTI.

2) The first fault does not have the potential to directly violate the SG. In this case, the time-span relying solely on the redundant functionality is defined as EOTTI, which is equivalent to MPFHTI\(_{\text{max}}\).

C. TRANSITION TO EMERGENCY OPERATION IN THE CONTEXT OF WARM REDUNDANCY

As introduced, an EO may be entered after the occurrence of a fault which is not directly violating the SG, see EO4 in Table 2. Thereby, no explicit fault handling is necessarily required to prevent the occurrence of a hazardous event, i.e., to activate the redundant system. This is not fully compliant with the definitions and examples provided in ISO 26262 – implicitly focusing on cold redundancy – whereby an explicit fault reaction is required for two reasons:

1) To prevent the occurrence of a hazardous event and thus, prevent the direct SG violation, by activating a backup functionality within the FHTI\(_{\text{max}}\) respectively FTTI;

2) To enter an EO after the activation of the backup until a safe state is reached.

For example, EO is defined in ISO 26262-1:2018, 3.43 as “operating mode […] after the reaction to a fault” [1]. In the case of warm redundancy, no fault reaction is required to enter the EO; thus, a fault may not be immediately detected. In other words: The item may enter an EO – in the sense of operating with a remaining safety capability lower than the ASIL ratings of possible hazards – without being noticed for a significant time. The EO remains undetected for the duration of FDTI, which may be in the range of one hour. However, in the case of cold redundancy, entering the EO is typically recognized instantly because of the active switching to the backup.

Because a fault reaction is not necessary for all items to reach an EO, the statement provided in ISO 26262-10:2018, 4.4.1 – EO “is initiated prior to the end of the FTTI” [5] – should be revised. According to the introduced concept, EO must not be “initiated” [5] in general. Nevertheless, at a certain point in time, a fault detection and fault reaction are necessary to ensure a transition to a safe state within EOTTI. Without any fault detection and fault reaction, neither the driver nor any other system would ever be informed about the present EO and a transition to a safe state would not be triggered. However, the necessary fault handling in the case of warm redundancy only needs to be performed within MPFHTI\(_{\text{max}}\) – instead of the typically much shorter FHTI\(_{\text{max}}\).

If the probability of two independent random HW faults causing a dual-point failure – each causing the loss of either redundant system – is sufficiently low, the subsequent EO may last for the rest of the vehicle lifetime from random HW faults point of view. In this case, no fault detection may be required at all. However, the residual risk of the specific fault scenario shall be sufficiently unlikely. To prove this – among others – the actual PMHF of the item shall be less than the PMHF-target according to ISO 26262-5:2018, Table 6. However, if the resulting risk from the operation solely relying on one of the redundant systems after losing the redundancy is considered to be unreasonable due to systematic effects, still a transition to safe state and thus, a fault detection, is required. This may be the case even if systematic faults are avoided and/or controlled with the initial ASIL.

D. AVAILABILITY OF THE SPECIFIED VEHICLE FUNCTION IN THE CONTEXT OF WARM REDUNDANCY

According to EO5 of Table 1, in the case of cold redundancy, the specified functionality is unavailable from the occurrence of a fault in the main system until the transition to the backup is completed, i.e., during FHTI. However, in the case of warm redundancy, the specified functionality is continuously
available because the redundant system must not be activated – it is already active when the first fault occurs. In other words: The specified functionality is not necessarily unavailable for a FHTI due to elimination of the switching mechanism. Thus, the availability of this functionality is increased. However, the safety capability of the item is in both cases lower than the ASIL rating of possible hazards during EO, see EO6.

Warm-redundant systems are typically more stressed during nominal operation than passive backup systems in the case of cold redundancy. This may lead to higher failure rates due to higher stress factors. The specified functionality is only unavailable in the case of a dual-point failure, i.e., if a first DPF remains latent or if it is not yet repaired and a second fault occurs. After the occurrence of the second fault, no safe transition to safe state is typically possible any longer.

**E. TRANSIENT FAULTS CAUSING EMERGENCY OPERATION IN THE CONTEXT OF WARM REDUNDANCY**

Transient faults in the context of warm redundancy require further considerations in addition to Section II-E in [4]. In the case of transient faults causing temporary unavailability of a redundant system, i.e., a temporary EO, the overall risk cumulates that a second fault occurs when the redundant system is unavailable [4]. If such a temporary EO is present multiple times, all temporary EOs, i.e., EOTI, shall be combined respectively accumulated and compared to EOTTI to ensure a transition to a safe state within EOTTI [4]:

$$\sum_i \text{EOTI}_i \leq \text{EOTTI}.$$  \hspace{1cm} (2)

However, if a transient fault, which causes a loss of either redundant system, disappears within FDTI, an EO is temporarily entered without being detected because the presence of this transient fault is too short to even be detected. Therefore, the duration of such an undetected EO cannot be considered in the EO recording, e.g. according to (2). In this case, it cannot be ensured that the derived EOTTI is met.

For example, assuming a power supply system comprising redundant power feeds by a DC/DC converter and battery according to [1]. A fault detection once at the beginning of a drive cycle, i.e., FDTI = 1 h, to detect a non-performant battery as effect of cold environmental conditions, may not be sufficient. The following scenarios are possible:

1) If such a fault is detected once at the beginning of a drive cycle, the entire drive cycle must be considered a temporary EO that contributes to the accumulated EOTI.

2) If the detection mechanism is executed at the beginning of the drive cycle, but the transient non-performant battery fault occurs during the drive cycle – for whatever reason – the temporary EO is not detected at all.

If the second scenario occurs multiple times due to a random combination of worst-case boundary conditions, the temporary EOs cannot be monitored; thus, the EOTTI can be exceeded. To prevent this, the non-performant battery – respectively the loss of either redundant system in general – must be recognized instantly, leading to an MPFDTI \( \rightarrow 0 \) for such transient faults. Only in this case is a transition to a final safe state within EOTTI ensured and the transient faults can be considered acceptable. An MPFDTI \( > 0 \), e.g. in the range of the FTTI or larger to not detect very short EOs, may be granted in the case of a technical argumentation. To enlarge the permissible MPFDTI, the design and corresponding thresholds to indicate an imminent fault respectively the EO can be adapted. Note: EO is only applicable in the case of random HW faults or a random combination of worst-case boundary conditions; however, it is not applicable in the case of a systematically insufficient design of the item.

**F. DEPENDENCY OF EMERGENCY OPERATION TOLERANCE TIME INTERVAL**

In general, the operating mode after the occurrence of a first fault is defined in the OEM specific warning and degradation strategy according to ISO 26262-10:2018, 4.4.1 [5]. It shall be specified “how to alert the driver of potentially reduced functionality and of how to provide this reduced functionality to reach a safe state” [7]. However, the focus of the example in ISO 26262-10:2018, 12.2.5 is only on a fault in the main system in a cold-redundant item. In this example, the backup system is activated and the driver is informed about the loss, see also EO7 in Table 1. Therefore, only the EO relying on the backup system is evaluated. However, driven by the newly introduced additions and adaptions in Table 1, an EO may also be present in the case of a fault in the backup systems while the main system is working. The same applies to items based on warm redundancy. In the case of warm redundancy, both fault sequences need to be considered. In other words: An EO may need to be designed for both fault sequences and a corresponding concept for the warning and degradation strategy shall be developed. Among others, the permissible EOTTI depends on the remaining system respectively the first fault causing the EO. Different EOs and warning and degradation strategies can be designed – depending on the architecture, the remaining system, and targets to be achieved with this system.

**G. SYSTEMATIC SAFETY INTEGRITY TO ENSURE SAFE EMERGENCY OPERATION AND TO MAINTAIN A SAFE STATE**

As introduced, regarding the systematic safety integrity of SMs which handle faults that are not directly violating a SaRA requirement, no guidelines and only ambiguous requirements are provided in ISO 26262. In this section, various interpretations and their drawbacks are evaluated.

As a first reference, the requirements and guidelines for handling faults potentially directly violating an SG are introduced. In other words: The necessary systematic integrity of SMs to handle faults directly violating the SG specifying a SaRA requirement are evaluated in the context of EO, e.g., a fault in the main system in a cold-redundant item.
Following phases are differentiated to evaluate the systematic integrity:

1) **Phase 1 – Explicit fault handling:**
   a. Functionality is unavailable after a fault in the main system, whereby a hazardous event is prevented by an explicit fault handling, i.e., by activating the backup within $FHTI_{\text{max}}$, i.e., $FHTI \leq FHTI_{\text{max}}$.
   b. The explicit fault handling is implemented with the initial ASIL of the SG to prevent the occurrence of the hazardous event. Note: In the case of redundant and sufficiently independent functions to prevent the hazardous event from occurring, the ASIL of each function can be reduced by an ASIL decomposition.

2) **Phase 2 – Transition to safe state:**
   a. During EO, the specified functionality is provided with reduced safety capability for the duration of $EOTI \leq EOTTI$ since it solely relies on the backup.
   b. The transition to safe state shall either be triggered by the function that was already used for the explicit fault handling of Phase 1 or by an additional SM. The transition to a safe state can be performed, e.g., by a driver warning or a warning to a different ECU. It shall be ensured with the initial ASIL of the SG.

3) **Phase 3 – Maintain safe state:**
   a. After reaching a safe state, it shall be maintained.
   b. The safe state is maintained with the initial ASIL according to ISO 26262-10:2018, 12.2.4.2 Note 6.

As a result, the explicit fault handling (Phase 1), the subsequent transition to a safe state, i.e., the EO, (Phase 2) and the maintenance of the safe state (Phase 3) are ensured with the initial ASIL of the SG.

In contrast, a fault in the backup system of a cold-redundant item or in either redundant system of a warm-redundant item does not have the potential to directly violate the SG. Therefore, there is no need for an explicit fault handling at all (Phase 1) to prevent the occurrence of a hazardous event with the initial ASIL of the SG. No requirements concerning these faults in the context of EO are stated in ISO 26262. However, ISO 26262-4:2018, 6.4.2.5 can be applied to faults not directly violating the SG. According to this, SMs can be implemented with reduced systematic safety integrity to prevent MPFs from being latent. Thereby, the term “reduced systematic safety integrity” depends on the safety integrity concerning the availability of each redundant element respectively the backup. In the case of ASIL decomposition, the reduced safety integrity depends on the decomposed safety requirement according to ISO 26262-4:2018, 6.4.2.5 Note. Because an SM generally comprises a fault detection and fault reaction, the reduced systematic safety integrity is applicable to the fault detection and reaction. Accordingly, the EO shall be ensured with reduced systematic safety integrity.

The application of ISO 26262-4:2018, 6.4.2.5 results in an asymmetry in the systematic integrity how faults are handled in the case of EO:

1) **SMs to handle faults potentially directly violating the SG and to ensure the subsequent transition to a safe state are implemented with the initial ASIL.**

2) **SMs to handle faults not directly violating the SG, i.e., first DPFs, and to ensure the subsequent transition to a safe state are implemented with reduced safety integrity.**

Because a safe state is achieved with reduced systematic safety integrity, the maintenance of the safe state can also only be triggered with reduced safety integrity. Thus, maintaining the safe state can at a maximum achieve the integrity of the reduced safety level – due to its triggering input. However, maintaining a safe state with reduced safety integrity contradicts to ISO 26262-10:2018, 12.2.4.2 Note 6. This contradiction cannot be resolved in a fully ISO 26262-compliant manner. The following options are possible – depending on the weighting of guidelines and requirements:

1) **ISO 26262-10:2018, 12.2.4.2 Note 6 is only applicable after faults with the potential to directly violate the SG. However, after faults without the potential to directly violate the SG, the safe state is maintained with reduced systematic safety integrity.** Following this, potential hazards – rated with the initial ASIL – are only prevented by limiting the relevant VOS with reduced systematic safety integrity.

2) **ISO 26262-10:2018, 12.2.4.2 Note 6 is applicable independent of the initiating fault since the hazards – rated with the initial ASIL – shall be prevented with the initial ASIL by limiting the relevant VOS. However, this leads to either one of the following:**
   a. The SM to maintain the safe state is implemented with the initial ASIL but is only triggered by the SM that detects the fault and triggers the transition to a safe state with reduced systematic safety integrity.
   b. To ensure ASIL-consistency among the fault detection, the transition to safe state and its maintenance, no reduced systematic safety integrity is applicable at all.

Regarding option 1), the risk during the safe state seems to be unreasonable because the risk mitigation has a lower safety integrity than the hazard. However, this fits to the current argumentations and requirements concerning DPFs and MPFs in ISO 26262. Option 2b) can be considered the safest but this seems to accompany with an overdesign. Additionally, this questions ISO 26262-4:2018, 6.4.2.5 at all, i.e., the possibility to consider reduced systematic safety integrity concerning latent faults. From our point of view, option 2a) seems to be the most appropriate compromise – although there is an inconsistency in the ASIL-chain.

Considering this, the systematic integrity for SMs to ensure EO for cold- and warm-redundant items can be summarized as shown in Table 4. Thereby, “initial ASIL” refers to the
ASIL of the SG – “reduced safety integrity” depends on the (decomposed) safety integrity concerning the availability of each redundant element. In general, the safety capability concerning availability of the specified functionality during EO can be lower than the initially specified ASIL for the hazard. However, the transition to EO shall be ensured with the systematic safety integrity as listed in Table 4.

TABLE 4. Systematic safety integrity for SMs to ensure EO.

| Cold redundancy | Warm redundancy |
|-----------------|-----------------|
| Faulty main system | Faulty backup system | Fault in either redundant system |
| Fault detection | Initial ASIL\(^a\), Reduced safety integrity | Reduced safety integrity |
| Explicit fault reaction\(^b\) | n/a | n/a |
| Transition to safe state | Initial ASIL | Reduced safety integrity | Reduced safety integrity |
| Maintain safe state | Initial ASIL | Initial ASIL |

\(^a\)explicit fault reaction to prevent hazardous event from occurring,\(^b\)part of the explicit fault handling

Therefore, all functions required to be available to ensure the transition to a safe state must ensure their availability during EO with the corresponding systematic safety integrity. Otherwise, the transition to safe state cannot be ensured safely. For example, assuming the vehicle standstill as safe state, the transition to it can be ensured by reducing the vehicle speed via the engine control unit – with systematic safety integrity according to Table 4. If this function is implemented as fail-passive, no additional requirements are allocated to the power supply system. However, if this function must be available to ensure the transition to the safe state, the power supply shall be ensured with the corresponding systematic safety integrity even during EO. Note: The systematic safety integrity focuses on the systematic integrity of the SM – random HW faults in the SM are typically considered a DPF in the quantitative safety evaluation. The following applies for the power supply domain: If the SM to ensure a transition to a safe state – such as the vehicle speed reduction –...

1) …requires safe power supply for its execution, the power supply must be ensured with the corresponding systematic safety integrity even during EO.
2) …does not require safe power supply for its execution respectively is implemented as fail-passive, no further requirements must be considered for the power supply system during EO.

III. EMERGENCY OPERATION IN THE CONTEXT OF WARM-REDUNDANT POWER SUPPLY SYSTEMS

In this section, the previously discussed properties of EO are explained for an exemplary warm-redundant power supply system. As introduced in Section I-C, the power supply system is considered an item below the steering entity. A SaRA requirement is allocated from the superior entity to the item power supply system, whereby the availability is only safety-relevant during the VOS driving. Thus, it is assumed that the safety integrity depends exemplarily only on the vehicle speed.

A. FUNCTIONAL SAFETY CONCEPT AND PRELIMINARY ARCHITECTURAL ASSUMPTIONS

For this example, the architecture proposed in [3] is considered to comply with the SG introduced in Section I-C, see Fig. 1. It comprises two terminals: T.30\(_q\) and T.30\(_s\) [3]. Basic premise: Each terminal is able to provide sufficient power for the EPS by itself. An EBS is implemented to monitor the battery. Among others, the smart safety switch is implemented as a centralized safety measure to ensure sufficient independence between the redundant power feeds, e.g. by handling dependent failure initiators and. The functional safety concept is based on the generic safety requirements according to Section I-C, see also [1], [3], [4], and [8]. To lower the initial ASIL C for each power feed, an ASIL decomposition is applied. The power feed by the DC/DC converter shall be implemented with QM(C) integrity; the power feed by the T.30\(_s\) battery with ASIL C(C) [1], [3].

This is considered a warm redundancy [3]. The loss of both redundant power feeds represents a dual-point failure.

In general, different faults can cause an EO in the exemplarily architecture, e.g.:
1) Faults in the power feed like a non-performant battery;
2) Faults in the power distribution such as an open circuit in the wiring from either energy source/storage to the smart safety switch;
3) Faults in the smart safety switch leading to the incapability of ensuring freedom from interference between QM-loads and safety-relevant loads;
4) Faults in QM-loads leading to fault isolation by the smart safety switch, i.e., disconnecting T.30\(_q\) and T.30\(_s\) which leads to a lower safety integrity regarding power feed and power distribution, too.

In this paper, the focus is on the redundant power feed by the DC/DC converter and the battery. After the loss of either redundant power feed, the power feed is provided with a lower safety capability than the ASIL of the possible hazard:
1) The following applies for the DC/DC converter:
   a. Systematic faults are prevented and/or controlled with QM(C) integrity due to ASIL decomposition, which is lower than the hazard’s ASIL C rating.
   b. ASIL C target values for random HW faults are not met by the power feed solely relying on the DC/DC converter.

2) The following applies for the battery:
   a. Systematic faults are prevented and/or controlled with ASIL C(C) due to ASIL decomposition, which meets the hazard’s ASIL C rating.
   b. ASIL C target values for random HW faults are not met by the power feed solely relying on the battery.

Thus, an EO is entered if a fault in either power feed occurs. If fail-degraded behavior is acceptable on item respectively entity level, i.e. not providing full performance of the specified functionality after a fault, the performance requirements for the power feed may be reduced, e.g., leading to a smaller battery. An additional measure to lower the performance requirements is the separation of QM-loads by the smart safety switch during the EO [3]. In this case, the timing requirement to disconnect the QM-loads mainly depends on the battery design and the power consumption of the QM-loads. Rule of thumb: The bigger the battery, the longer the permissible time to disconnect QM-loads due to energetic reasons.

### B. EXEMPLARY FAULT SCENARIO

In general, the operation solely relying on the T.30_s battery is limited in time because the battery cannot be recharged if the power feed by the DC/DC converter is unavailable [3]. Therefore, the safe state in case of a loss of either power feed is defined as vehicle standstill, similar to safe state 1 in [3] and [5]. During vehicle standstill, no SaRA requirements are allocated to the power supply system by the steering entity.

The time intervals discussed in Section II are summarized in Fig. 2; the relevant time steps are described in Table 5. In the following, the operating phases highlighted in Fig. 2, i.e., nominal operation, EO and operation with disabled functionality, are discussed in detail.

#### 1) NOMINAL OPERATION

Analogous to [4], the starting point of the investigation is the nominal operation, which is the fault free operation. At a random point in time, a first fault occurs, e.g., an insufficient power feed from the DC/DC converter due to a short circuit to ground caused by a HV base load. In this case, the EO is to be designed based on the power feed by T.30_s battery, which is evaluated in the following. Nevertheless, the EO is also to be designed vice versa, i.e., a fault causing the loss of the T.30_s battery leading to an EO relying on the power feed by the DC/DC converter.

#### 2) EMERGENCY OPERATION

The EO and thus, EOTI and EOTTI, start after the occurrence of the fault in the power feed by the DC/DC converter – without any explicit fault handling within FHTI max or FTTI. Therefore, the EO is present immediately after the fault occurrence. Premise: The power feed by the battery is fault-free at this time. In contrast to cold redundancy, the power supply to the EPS is not interrupted. The steering functionality is not even for a short period of time unavailable. As of the fault occurrence, the required power feed is only provided by the battery. A further fault in the battery may cause a hazard because no power would be provided anymore. The availability of the power supply for the EPS is ensured by the battery with ASIL C(C). However, the hazard is still rated with ASIL C because the VOSs are not limited. Therefore, as stated in Section III-A, the remaining safety capability of the item power supply system – and thus also of the entity steering – does not comply with the ASIL of the initial hazard. An unreasonable risk is prevented by transition to a safe state within EOTI ≤ EOTTI = MPFHTI max. During EO, a VOS without a SaRA requirement may be entered and left again; however, the safe state is entered once and maintained in the following. Thus, it is possible to temporarily park the vehicle and restart it again knowing that the power feed by the DC/DC converter is insufficient.

To ensure an EO without an unreasonable level of risk, an SM is implemented to detect the fault in the power feed by the DC/DC converter and transition to a safe state in time:

1) Fault detection during FDTI: During this time span, the fault is not detected and there is no information available about the loss of the redundant power feed, i.e., the EO is present – but not noticed. The detection of a non-performant power feed by the DC/DC converter can be implemented, e.g. in the smart safety switch, a different ECU or the DC/DC converter itself.
2) Transition to a safe state as fault reaction during FRTI:
After detection of the fault, the loss of the redundant power feed is notified to the driver and/or any other ECU to trigger and ensure a transition to safe state, e.g., by reducing the vehicle speed via the engine control unit.

The sum of FDTI and FRTI, i.e., FHTI, is equal to EOTI.

According to Table 4, the SM to detect the fault and to ensure the transition to a safe state is to be implemented with reduced safety integrity. However, there is no established common understanding regarding the applicability of the Note in ISO 26262-4:2018, 6.4.2.5, whether the reduced safety integrity depends on the decomposed safety requirement – in our example QM(C) integrity of the power feed by the DC/DC converter – or the initial ASIL of the SG itself – in our example ASIL C. Further clarification would be appreciated in the third version of the ISO 26262. To be conservative, the ASIL of the initial SG is considered. Thus, ASIL A is sufficient according to ISO 26262-4:2018, 6.4.2.5 for the SM which detects the fault in the power feed by the DC/DC converter and ensures the transition to safe state within EOTI. In this case, the power supply is still provided with ASIL C as far as systematic safety integrity is concerned. Thus, the SM to ensure the transition to safe state can rely on a safe power supply.

However, if the battery fails first causing an EO, ASIL A is still sufficient to detect the fault and ensures the transition to a safe state within EOTI. However, in this fault sequence, the power feed is only provided with QM(C) integrity. Thus, the SM to detect the fault and ensure the transition to safe state within EOTI cannot rely on a safe power supply with ASIL A. In other words: The SM to detect the fault and limit the time during EO must be implemented as fail-passive.

Note: Among others, the execution of the MRM is based on steering and braking function. Thereby, the actual availability of these functions during EO respectively for the execution of the MRM need to be considered due to EO as long as the SM to ensure the transition to a safe state, i.e., to bring the vehicle to standstill within EOTI, is implemented as fail-passive. Rule of thumb: The lower the systematic integrity concerning availability of the specified vehicle function during EO – in our example the steering function – the shorter the EOTI should be.

3) FUNCTIONALITY DISABLED
As introduced, the vehicle standstill shall be reached as a safe state because no SaRA requirement is allocated from the steering entity to the power supply system at vehicle standstill. Thus, the vehicle shall either reach a workshop or park in a minimal risk condition within EOTI to enable towing to the next workshop [4]. The vehicle standstill shall not only be reached within EOTI, additionally, this safe state shall be maintained after EOTI as long as the vehicle is not repaired. According to Section II-G, the SM to maintain the safe state is implemented with the initial ASIL of the SG. In general, other safe states are also possible, see [4] for more details.

C. EXEMPLARY DERIVATION OF EMERGENCY OPERATION TOLERANCE TIME INTERVAL BASED ON RANDOM HARDWARE FAULTS
In this section, an exemplary MPFHTI_max respectively EOTI is derived for the introduced use case. The PMHF calculation is based on ISO 26262-10:2018, 8.3.2.4, whereby no SPFs or RFs are assumed for the redundant power feed – according to the premises stated in Section I-B:

\[
PMHF = \lambda_{SPF} + R_{RF} + \sum_{i} \lambda_{SM1,DPF,latent} \cdot \lambda_{IF,DPF,T_{life}} + \lambda_{SM1,DPF,detected} \cdot \lambda_{IF,DPF,T_{service}}
\]

Following assumptions and mappings are made:
1) IF: is represented by the power feed from T.30_q;
2) SM1: is represented by the power feed from T.30_s;
3) SM2 & SM3: are considered to prevent faults from being latent in either IF or SM1 and to ensure the transition to a safe state, i.e., to timely limit EO; 4) Target safe state: vehicle standstill; 5) $T_{\text{life}} = 8000h$.

The focus is on the PMHF budget for the power feed – it shall be $\leq 60$ FIT [1]. The patterns are considered as follows:

1) Pattern 1: Applied, because “fault in SM1 is mitigated by [IF] but not notified” due to imperfect FMC of SM2. In other words: The loss of power feed by the battery is tolerated due to power feed by the DC/DC converter. The fault detection and the transition to a safe state within EOTTI is ensured by SM2 – implemented with reduced safety integrity. Thus, $\lambda_{\text{SM1,DFP,latent}} = (1 - \text{FMC}_{\text{SM2}}) \cdot \lambda_{\text{SM1}}$ and $\lambda_{\text{SM1,DFP,detected}} = \text{FMC}_{\text{SM2}} \cdot \lambda_{\text{SM1}}$.

2) Pattern 2: Applied, because “fault in SM1 is mitigated by [IF] and notified by SM2” – see 1).

3) Pattern 3: Applied, because “fault in IF is mitigated by SM1 but not notified” due to imperfect FMC of SM3. In contrast to Pattern 1, the loss of power feed by the DC/DC converter is tolerated by the power feed by the battery; the safe state is achieved by SM3.

4) Pattern 4: Applied, because “fault in IF is mitigated by [SM1] and notified by [SM3]” – see 3).

In Table 6, exemplary failure rates for these components are shown. For sake of simplicity, SMs implemented to prevent the violation of each decomposed safety requirement are not considered in this exemplary calculation.

Considering the mandatory formula to calculate the EOTTI according to [4] – respectively MPFHTI$\text{max}$ as introduced in this paper – based on the formula to calculate the PMHF, this leads to (4) according to ISO 26262-10:2018, 12.3.1.2. Thereby, it is assumed that the EO after a fault in the power feed by the DC/DC converter is equal regarding EOTTI respectively MPFHTI$\text{max}$ as the EO after a fault in the power feed by the battery. In general, different EOTTIs respectively MPFHTI$\text{max}$ can be derived for the different scenarios. $\lambda_{\text{target}}$ represents the PMHF target value, which is assumed to be 60 FIT for the power feed as previously introduced.

$$T_{\text{EOTTI}} = T_{\text{MPFHTI, max}}$$

$$\leq \left( \frac{\lambda_{\text{target}} - 0.5 \cdot \lambda_{\text{SM1,DFP,latent}} \cdot \lambda_{\text{IF,DFP}} \cdot T_{\text{life}} - 0.5 \cdot \lambda_{\text{IF,DFP,detected}} \cdot \lambda_{\text{SM1,DFP}} \cdot T_{\text{life}}}{\lambda_{\text{SM1,DFP,detected}} \cdot \lambda_{\text{IF,DFP}} + \lambda_{\text{IF,DFP,detected}} \cdot \lambda_{\text{SM1,DFP}}} \right) \approx 747h.$$  

(4)

To prevent too optimistic results, a second formula is considered to derive EOTTI respectively MPFHTI$\text{max}$, additionally, by focusing only on the operation during EO – according to ISO 26262-10:2018, 12.3.1.1 [2], [5]. Thereby, it is differentiated between which fault triggers the EO. Note: The applicability of SMs after the loss of redundancy shall be revised. For example, a short circuit to ground in a QM-load can still be isolated by the smart safety switch if the entity solely relies on the power feed by the battery. However, it cannot be isolated by the smart safety switch in the proposed architecture if the entity solely relies on the power feed by DC/DC converter since this would also disconnect the power feed. If the power feed by the battery fails first, i.e., IF is the remaining system; EOTTI is calculated according to (5):

$$T_{\text{EOTTI,IF}} = T_{\text{MPFHTI, max,IF}}$$

$$\leq T_{\text{life}} \cdot \frac{\lambda_{\text{target}}}{\lambda_{\text{IF,DFP}}} \approx 53 \text{ h}.$$  

However, if the power feed by the DC/DC converter fails first, i.e., SM1 is the remaining system, it results in (6):

$$T_{\text{EOTTI,SM1}} = T_{\text{MPFHTI, max, SM1}}$$

$$\leq T_{\text{life}} \cdot \frac{\lambda_{\text{target}}}{\lambda_{\text{SM1,DFP}}} \approx 178 \text{ h}.$$  

(6)

Thereby, it is not differentiated between the failure rate for the power feed by T.30_s during nominal operation – not fully stressed – and after a fault in T.30_q – fully stressed. The failure rate considering full stress is assumed as worst-case condition. In the following, the shortest EOTTI of (4), (5) and (6) is considered, i.e., $T_{\text{EOTTI}} = 53 \text{ h}$. Considering this and the aforementioned assumptions, the PMHPF$\text{PF}$ for the power feed results in (7) according to (3), where $T_{\text{service}}$ is replaced by $T_{\text{EOTTI}}$. In the worst-case scenario, the full budget of $T_{\text{EOTTI}}$ is required to achieve a safe state, i.e., $T_{\text{EOTTI}} = T_{\text{EOTTI}} = 53 \text{ h}$.

$$\text{PMHPF}_{\text{PF}} \approx 32 \text{ FIT}.$$  

(7)

For sake of completeness, the SPF and LFM is also evaluated. Because no SPFs/RFs are assumed, $\text{SPFM}_{\text{PF}} = 100 \%$. $\text{LFM}_{\text{PF}}$ is determined by (8) – according to ISO 26262-5:2018, Annex C, whereby $\sum_{\text{SR,HW}} \lambda_{X}$ represents the “sum of $\lambda_{X}$ of the safety-related HW elements of the item to be considered” [6]:

$$\text{LFM}_{\text{PF}} = 1 - \frac{\sum_{\text{SR,HW}} \lambda_{\text{MPF,latent}}}{\sum_{\text{SR,HW}} \lambda_{\text{SR}}} \approx 84, 1\%.$$  

(8)

Because of $\text{PMHPF}_{\text{PF}} \leq 60 \text{ FIT}$, $\text{SPFM}_{\text{PF}} \geq 97 \%$ and $\text{LFM}_{\text{PF}} \geq 80 \%$, the power feed can be considered ASIL.
C-compliant as far as random HW faults are concerned – assuming the other systems achieve their budget as well. Note: Whereas the power feed by the DC/DC converter is not timely limited in general, the power feed by battery is systematically limited in time due to electrical discharging without recharging. Thus, the EO solely relying on the power feed by the battery is typically far shorter than the calculated 53 h; among others, it depends on battery dimensioning, load management and vehicle-specific power demand.

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 EO – in the context of functional safety – for warm-redundant items. The guidelines and requirements concerning EO in ISO 26262 focus on cold redundancy. Warm redundancy is of particular interest for the power supply domain due to its high level of market penetration; however, no guidelines and only ambiguous requirements are provided in ISO 26262 for it. In contrast to ISO 26262, an EO can also be entered without an explicit fault reaction to prevent a hazardous event by switching to a backup system. In general, an EO is entered if the safety capability of a fault tolerant item respectively entity after a fault first is lower than the ASIL rating of the initially possibly hazard – independent of cold or warm redundancy. In this paper, a consistent and holistic approach is presented how the loss of redundancy is dealt with in the case of an SG specifying a SaRA requirement and EO.

The focus of this paper is on guidelines and requirements concerning the relevant time intervals and the required systematic integrity of SMs to implement an EO. Among others, this includes the introduction of the MPFHTI\textsubscript{max}, which can be equal to EOTTI in the case of warm redundancy. The systematic safety integrities of SMs to timely limit an EO are based on an asymmetric approach:

1) SMs to handle faults potentially directly violating the SG and to ensure the subsequent transition to safe state, i.e., the EO, are implemented with the initial ASIL.

2) SMs to handle faults not directly violating the SG, i.e., DPFs, and to ensure the subsequent transition to safe state, i.e., the EO, are implemented with reduced systematic safety integrity.

In both cases, the safe state after EO is maintained by SMs implemented with the initial ASIL of the SG.

This paper contributes to a further standardization of functional safety in the power supply domain by suggesting several possible adoptions and extensions to the current version of ISO 26262. Newly introduced acronyms and definitions comply with the current version of ISO 26262.

REFERENCES

[1] P. Kilian, A. Köhler, P. Van Bergen, C. Gebauer, B. Pfeuffer, O. Koller, and B. Bertsche, “Principle guidelines for safe power supply systems development,” IEEE Access, vol. 9, pp. 107751–107766, 2021, doi: 10.1109/ACCESS.2021.3100711.

[2] Steering System of Motor Vehicles. Basic Requirements, Standard GB 17675-2021, 2021.

[3] P. Kilian, O. Koller, P. Van Bergen, C. Gebauer, and M. Dazer, “Safety-related availability in the power supply domain,” IEEE Access, vol. 10, pp. 47869–47880, 2022, doi: 10.1109/ACCESS.2022.3171261.

[4] P. Kilian, O. Koller, P. Van Bergen, C. Gebauer, F. Heidinger, and M. Dazer, “Emergency operation in the power supply domain according to ISO 26262,” IEEE Access, vol. 10, pp. 47557–47569, 2022, doi: 10.1109/ACCESS.2022.3170903.

[5] Road Vehicles—Functional Safety—Part 10: Guidelines on ISO 26262, document ISO 26262-10:2018(E), 2018.

[6] Road Vehicles—Functional Safety—Part 5: Product Development at the Hardware Level, document ISO 26262-5:2018(E), 2018.

[7] Road Vehicles—Functional Safety—Part 1: Vocabulary, document ISO 26262-1:2018(E), 2018.

[8] VDA Empfehlung für Einen Mindestsicherheitsstandard der Energieversorgung und Deren Elemente im Rahmen der ISO 26262, Standard VDA 450, 2021.

[9] C. Gebauer, “Fail operational and ISO 26262 2nd edition,” presented at the Safetronic, Stuttgart, Germany, Nov. 2018.

[10] A. Köhler and B. Bertsche, “An approach of fail operational power supply for next generation vehicle powertrain architectures,” in Proc. 30th Eur. Syst. Rel. Conf. 15th Probabilistic Saf. Assessment Manage. Conf., Venice, Italy, 2020, pp. 60–67.

[11] L. Braun, “Global powernet diagnostics: Miniaturization of the powernet by using a diagnostic function,” presented at the Int. Conf. Automot. Wire Harness, Oct. 2018.

[12] F. Bierwirth, “Predictive diagnosis of E-fuse-protected supply paths in vehicle low-voltage energy systems,” presented at the Electr. Electron. Hybrid Electr. Vehicles Elect. Energy Manag. (EEHE), Essen, Germany, Nov. 2021.

[13] S. Schumi, “Energy and supply concepts for automated driving,” in Proc. IEEE Int. Conf. Electr. Syst. Aircr., Railway, Ship Propuls. Road Vehicles Int. Transp. Electrific. Conf. (ESARS-ITEC), Nov. 2018, pp. 1–5.

[14] C. Gebauer, “Item definition & PMHF budgeting for automated driving functions,” presented at the safetronic, Stuttgart, Germany, Nov. 2019.

[15] A. Schnellbach, “Fail-operational automotive systems,” Ph.D. dissertation, Inst. Automot. Eng., TU Graz, Graz, Austria, 2016.

[16] B. Sari, “Fail-operational safety architecture for ADAS/AD systems and a model-driven approach for dependent failure analysis,” Ph.D. dissertation, Inst. Automot. Eng., Univ. Stuttgart, Wiesbaden, Germany, 2020, doi: 10.1109/ACCESS.2021.3100711.

[17] 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, document ECE R 13-H, 2015.

[18] A. Birolini, Reliability Engineering: Theory and Practice, 8th ed., New York, NY, USA: Springer, 2017, doi: 10.1007/978-3-662-54209-5.

[19] A. Birolini, Reliability Engineering: Theory and Practice, 7th ed., New York, NY, USA: Springer, 2014, doi: 10.1007/978-3-642-39535-2.

[20] Road Vehicles—Functional Safety—Part 4: Product Development at the System Level, document ISO 26262-4:2018(E), 2018.

[21] Regulation No 79 of the Economic Commission for Europe of the United Nations (UNECE)—Uniform Provisions Concerning the Approval of Vehicles With Regard to Steering Equipment, document ECE R 79, 2018.

PHILIPP KILIAN was born in Göppingen, Germany, in 1995. He received the Master of Science degree in mechanical engineering from the University of Stuttgart, in 2020, where he is currently pursuing the Ph.D. degree with a focus on modular and scalable safety concepts in cooperation with the Reliability Engineering Department, Institute of Machine Components.

He is also working as a Ph.D. Student in the field of functional safety in the area of power supply system.
PATRICK VAN BERGEN was born in Waiblingen, Germany, in 1989. He received the Master of Science degree in mechanical engineering from the Reutlingen University and University of Stuttgart, in 2015. He is currently pursuing the Ph.D. degree in 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, in 2018, and is also coordinating the functional safety topics in the power supply system area.

OLIVER KOLLER was born in Stuttgart, Germany, in 1985. He received the Diploma degree in electrical engineering and information technology from the University of Stuttgart, in 2011, and the Ph.D. degree in reliability engineering of 48V mild hybrid systems from Robert Bosch GmbH in cooperation with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart, in 2016. Between 2018 and 2021, he was leading the systems engineering and application development for power supply components. Since 2019, he has been part of the VDA 450 Group, Power Supply Systems for automated driving. Since 2021, he has been the representative for E/E architectures and responsible for the powernet strategy at Robert Bosch GmbH—Cross-Domain Computing Solutions.

CARSTEN GEBAUER began his professional career at Robert Bosch GmbH, in 2000. He is currently working at the Center of Competence Vehicle Safety, Bosch. Before that, he worked in different positions at Bosch dealing with safety topics. 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 received the Diploma degree in mechanical engineering from the University of Stuttgart, in 2014. He is currently pursuing the Ph.D. degree in reliability of automotive electronics–power supply systems with Robert Bosch GmbH. From 2014 to 2017, he worked as a Research Engineer at the Institute of Thermal Turbomachinery, University of Stuttgart. As of 2019, he was leading the Systems Engineering Development Team for power supply components. Since 2021, he has been a 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, and the M.Sc. degree in mechanical engineering and the Dr.-Ing. degree in reliability engineering from the University of Stuttgart, in 2015 and 2019, respectively.

From 2015 to 2018, he was a Research Assistant at the Institute of Machine Components. He is currently the Head of the Reliability and Drive Technology Department, Institute of Machine Components. He is also a Founder and a Consultant of RelTest-Solutions, TTI GmbH, Stuttgart, Germany. His research interest includes multitude of aspects of reliability engineering with its main focus on life testing.

Dr. Dazer is a member of the Technical Committee of Reliability Management of the Verein Deutscher Ingenieure (VDI), Germany, and a member of the Advisory Board of safety and reliability of the VDI.

***