Principle Guidelines for Safe Power Supply Systems Development

PHILIPP KILIAN, ARMIN KÖHLER, PATRICK VAN BERGEN, CARSTEN GEBAUER, BERND PFEUFER, OLIVER KOLLER, AND BERND BERTSCHE

1 Cross-Domain Computing Solutions, Product Area Integrating Devices–Engineering Vehicle Systems (XC-AN/EPI1), Robert Bosch GmbH, 70499 Stuttgart, Germany
2 Systems Engineering, Bosch Center of Competence Vehicle Safety (M/ENG-CVS), Robert Bosch GmbH, 71636 Ludwigsburg, Germany
3 Functional Safety, Mobility Industry/Service Line Vehicle Technology, TÜV SÜD Auto Service GmbH, 85748 Garching, Germany
4 Institute of Machine Components, University of Stuttgart, 70569 Stuttgart, Germany

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

ABSTRACT The relevance of safety applications within the automotive industry is increasing continuously, e.g. due to vehicle automation and decreasing relevance of mechanical backups. To cope with these trends, the power input of safety-related electrical and/or electronic systems needs to be ensured by the power supply system – leading to increased functional safety requirements. Compliance with ISO 26262 will be more in focus in the future. Currently, the compliance with ISO 26262 may be used to argue the state of the art focusing on product liability – however, it will become mandatory for homologation. Thereby, the power supply system is a crucial point since faults of the power supply system are currently the major contributor for vehicle breakdowns with increasing tendency. So far, there is no standard approach within the automotive industry how to ensure functional safety for power supply systems. To fill this gap, this technical elaboration evaluates functional safety with focus on power supply systems development. Hence, guidelines on how to apply the ISO 26262 are provided based on discussions within the automotive industry and research institutes. The focus is on the concept phase, i.e. item definition, hazard analysis and risk assessment, and the functional safety concept. The functional safety concept is based on a structured hierarchical breakdown to systematically derive safety requirements from the item level down to the power supply system level. The essential safety requirement – beside the safe power feed and safe power distribution – is to assure the freedom from interference between the safety and non-safety relevant components.

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

I. INTRODUCTION

The automotive industry is currently driven by the megatrends electrification and automated driving (AD) respectively advanced driver assistance systems (ADAS). To follow these trends, new functionalities and electrical and/or electronic systems (E/E systems) need to be developed. In the automotive industry, the ISO 26262 series of standards shall be applied to ensure functional safety of safety-related E/E systems. Due to the increasing number and complexity of such systems, new requirements and new failure modes arise. Thus, the safety awareness and the necessity of safe power supply domains becomes essential.

This directly affects the power supply system of the vehicles: whereas today’s development focuses mainly on voltage stability and load balance, the future activities shall also include the system’s behavior under various fault scenarios to ensure ISO 26262 compliance.

A. ORGANIZATION OF THE ARTICLE

Starting with general information and objectives, potential faults within the power supply system and their effects are introduced. Section II outlines the megatrends within the automotive industry and the resulting new and more stringent requirements on the power supply system development in more detail. In Section III, the legal situation in context of functional safety is discussed regarding technical recommendations, the consideration of the most current state of...
science and technology as well as technical regulations. The upcoming legislations in China will be of particular interest. Within the main part – Section IV – guidelines are provided how to develop a power supply system in compliance with the ISO 26262. An approach to systematically break down the requirements from vehicle level onto power supply system level is provided. Additionally, the technical realization of the requirements by lead batteries, wiring harness and melting fuses is discussed.

B. OBJECTIVE

Currently, there is no standard approach within the automotive industry how to ensure functional safety for the power supply systems. To fill this gap, this technical discussion evaluates functional safety with a focus on power supply system development. Functional safety in the context of the current and upcoming legal situation is explained. Additionally, guidelines on how to apply the ISO 26262 are provided based on discussions within the automotive industry and research institutes. The focus is on interpretations and recommendations for the practical application of the ISO 26262. Main topics are ASIL allocation and ASIL decomposition of safety requirements, budgeting and derivation of failure rates as well as the prevention of interference among different components.

C. FAULTS IN POWER SUPPLY SYSTEM

The relevance of electrical faults can be shown by recent vehicle breakdown statistics. Fig. 1 shows the massive impact of electric faults concerning vehicle breakdowns in total. In this chart, electric faults include faults from battery, alternator, starter, light, and wiring. They are not just the major contributor to vehicle breakdowns, additionally, the portion of electric faults increased about 12 percentage points within the last decade. All these electric faults may interfere with safety-relevant E/E systems, and potentially lead to a safety-critical driving situation.

Because a state-of-the-art safety-relevant load, e.g. electronic power steering (EPS), can only handle an improper power input to a certain degree by itself, additional safety measures shall be taken to control and/or prevent electrical faults. Such safety measures can be either implemented centralized in the power supply system for several safety-relevant loads combined or decentralized in each safety-relevant load itself.

In Fig. 2, a schematic power supply architecture is shown, including 48 V power supply system branch composed of an electrical generator, 48 V base loads and a 48 V/12 V DC/DC converter. The 12 V power supply system branch is composed of multiple 12 V loads – non-safety-relevant loads (e.g. seat heating and engine cooling fan) as well as safety-relevant loads (e.g. lights, braking and steering) – and a battery with an electronic battery sensor (EBS). Additionally, potential faults in the power supply system are shown.

Clustering these faults into the following categories ensure a systematic, consistent, and holistic development approach:
1) faults of power feed;
2) faults of power distribution;
3) faults of other electric components.

All these faults shall be addressed by functional safety and thus are further explained in Section IV. According to ISO 26262, faults are either caused randomly or systematically [3]. In case of a systematic fault, the cause may be traced back to the development phase and potentially forcing the original equipment manufacturers (OEM) to recall affected vehicles.

In 2018, Bosch observed overall more than 9 million vehicles worldwide affected by a recall due to faults in the power supply system, e.g. faults of battery, electrical loads or power distribution. The observation is based on published recall information, see e.g. [4]–[8]. To avoid personal injury, reduce recall costs and prevent reputation damage, these faults shall be captured by proper development process according to ISO 26262.

Faults in the power supply system are the major contributor for vehicle breakdowns. Safety measures must be applied to avoid the violation of safety goals.

II. MEGATRENDS – INFLUENCE ON THE POWER SUPPLY SYSTEM

In this chapter, the influence of
1) electrification (Section II-A);
2) AD and ADAS (Section II-B) and;
3) increasing vehicle weight (Section II-C)
on the power supply system design is evaluated.

A. ELECTRIFICATION

Due to national laws and customer demand, OEMs increasingly develop, build, and sell electrical vehicles (EVs) instead of internal combustion engine (ICE) vehicles. This is mainly driven by the purpose of reducing CO\textsubscript{2} emissions, e.g. according to the Paris climate agreement [9].

![FIGURE 1. Vehicle breakdown statistic from ADAC (Allgemeiner Deutscher Automobil-Club e. V.) identifies electric faults as major contributor with 52.4% in total. The ADAC is the biggest motoring association in Europe – representing and promoting the interests of motoring and motorsports [1].](image-url)
In Fig. 3, the expected market share of different fuel technologies is shown with focus on the increased market share of EVs. This may lead to several changes in the power supply system, e.g.:

1) introduction of new components such as electronic brake booster and electronic parking brake – however, this may also be valid for ICE vehicles;
2) less current excitation for functional battery diagnosis due to use of high-dynamic DC/DC converters instead of alternators and removal of ICE related loads;
3) missing implicit battery performance test by omission of the engine start, i.e. as long as the engine can be started by the battery, a certain performance of the battery is ensured;
4) increasing vehicle weight caused by heavy high-voltage batteries, see also Section II-C.

B. AUTOMATED DRIVING AND ADAS

ADAS is considered as pre-stage of AD, whereby the driver is still responsible to supervise the ADAS features to avoid accidents in case of malfunctions. In Fig. 4, the global market trend for development of ADAS is shown. From 2015 to 2019, the market size worldwide doubled up to 15.63 billion U.S. dollar. A further doubling from 2019 – up to 31.95 billion U.S. dollar – is projected for 2023.

In SAE J 3016, there are six levels defined regarding the capability of ADAS respectively AD. Each step accompanying specific standards for the behavior of the vehicle. Whereas Level 0 is not considering any driving automation, Level 5 represents full driving automation [11].

With increasing level of automation, the responsibility of the driver concerning vehicle guidance is decreasing. From Level 0 up to Level 2, the driver is fully responsible for the vehicle behavior. As of Level 3, the system takes over responsibility as long as the feature is engaged [11]. Because the driver is not available anymore, the backup is realized by redundancy on the electronic level to ensure performance of a minimal risk maneuver [11], [12].
If AD is realized with a X-by-wire system, additional legal requirements need to be considered for power supply systems, e.g., energy reserve for ensuring defined emergency braking maneuvers in case of electrical faults [12]. X-by-wire systems may also be applied in manual driving use cases.

C. VEHICLE WEIGHT

In Fig. 5, the increasing average curb weight of newly registered vehicles in Germany between 2007 and 2019 is shown [14]. This trend is mainly driven by SUVs and battery electric vehicles (BEVs). Increasing vehicle weight might affect the results of the hazard analysis and risk assessment (HARA).

The controllability by the driver in case of a sudden loss of steering assist is getting worse for heavier vehicles due to increasing rack forces to steer the vehicle. Additionally, heavier vehicles may lead to a higher severity classification due to higher impact forces in case of an accident. Less controllability and higher severity lead to higher automotive safety integrity level (ASIL) ratings in the HARA evaluation. Therefore, the safety requirements for the power supply system to prevent and/or mitigate faults—like the sudden loss of steering assist—increase accordingly. Further details will be explained in Section IV.

A further increase of safety requirements for future power supply systems is expected based on current market forecasts.

III. LEGAL SITUATION

The necessity to consider functional safety within the power supply system development is driven by legislation and standards. In Fig. 6, a summary of the contributors is shown which are affecting the future power supply system development process. It shall be distinguished between the common power supply system design process, technical recommendations (Section III-A), the most current state of science and technology (Section III-B) and technical regulations (Section III-C).

A. STANDARD – TECHNICAL RECOMMENDATION

The ISO 26262 is the adapted version of the IEC 61508 “to address the sector specific needs of electrical and/or electronic (E/E) systems within road vehicles” [3]. It is developed by a technical committee of the International Organization for Standardization (ISO). Generally, the compliance with the requirements of ISO 26262 is voluntary [16], i.e., not mandatory for vehicle homologation.

The use of standards is highly recommended. In product liability cases, the compliance with the state of the art must be proven as minimum requirement to exclude from the duty of damage compensation [17] and personal liability [18]. Technical recommendations, e.g., ISO standards, are considered to be representative for the state of the art. They are developed once based on a certain knowledge and are not continuously updated.

B. STATE OF SCIENCE AND TECHNOLOGY

In addition to technical recommendations, each OEM and supplier has the responsibility to consider also the most current state of science and technology to argue in product liability cases. The most current state of science and technology can be obtained by participating in expert-committees and on conferences to keep up with the progressing state. Several publications are dealing with different aspects of the power supply system development from functional safety perspective, see e.g., [2], [19]–[22].

The VDA (Verband der Automobilindustrie), a technical society of several German OEMs and suppliers, is capturing—among other things—the most current state of science and technology and adapting it to best practices for industrial application. For example, the VDA group 450 is currently defining the minimum requirements and possible topology implementations for power supply systems in an AD context. The requirements for the power supply system design are derived according to the ISO 26262 [23]. A white paper will be published by the VDA by the end of 2021, which will then become state of the art for power supply systems development.

Compliance with technical recommendations and the most current state of science and technology are strongly recommended to argue in case of a product liability trial.

C. LEGISLATION – TECHNICAL REGULATION

Besides the technical recommendations and publications regarding the most current state of science and technology, there are also legal requirements. Legal requirements are defined by technical regulations, which are mandatory for homologation and legally enforced [12].

Within Europe, the United Nations Economic Commission for Europe (UNECE or ECE) is responsible for such
regulations. The objective for the ECE is to promote pan-
Europe economic cooperation and integration and to unify
their technical regulations [24]. Relevant inputs for the power
supply systems can be derived from ECE regulations like
“Uniform provisions concerning the approval of vehicles
with regard to:
1) braking” – ECE R 13 H [12];
2) steering equipment” – ECE R 79 [25];
3) the protection of the occupants in the event of a frontal
collision” – ECE R 94 [26].

These regulations – directly or indirectly – introduce several
requirements for the power supply system development. According to ECE R 94, e.g., “at least one door […] per row
of seats” shall be able to be opened. In other words, the power
supply system may need to ensure power supply for at least
one door-ECU per row even in a post-crash scenario.

Additionally, the ECE announced in June 2020 a regulation
regarding automated lane keeping systems (ALKS) for
Level 3 automation vehicles [27]. This regulation – ECE
R 157 – explicitly states, that “functional and operational
safety for the automated system [shall be] performed by the
manufacturer during the design and development processes”
[28]. The derived documentation shall provide an argument
to ensure that the system “is free of unreasonable safety risks
to the driver, passengers, and other road users” [28].

In China, technical recommendations and regulations are
included within the national Chinese standards, also called
Guobiao Standards:
1) GB/T 34590 – “Road vehicles – Functional safety” [29]
is the Chinese complement of the ISO 26262.
2) GB 17675 – “Steering system of motor vehicles. Basic
requirements” is the Chinese complement of the ECE R 79 and
mandatory for homologation [30].

An update of the GB 17675 of the former version from
1999 was released beginning of 2021. The new version – GB
17675-2021 [31] – is valid for new type approvals starting
from the beginning of 2022. The updated version includes a
normative reference to GB/T 34590 which makes functional

Compliance with GB/T 34590 respectively ISO 26262 will
become mandatory for steering electronic control systems
including the power supply system for homologation in
China starting from 2022.

IV. SAFE POWER SUPPLY SYSTEM DEVELOPMENT
ACCORDING TO ISO 26262 – CONCEPT PHASE

The objective of the ISO 26262 is to provide guidance to
prevent and/or mitigate risk caused by systematic failures
and random hardware failures due to increasing technological
complexity, software and mechatronic implementation [3].
The standard is divided into 12 parts. Each part is either
focusing on different phases and/or activities during the
safety lifecycle of safety-related E/E systems or provides
valuable application guidelines and explanations.

This paper presents an approach how to systematically
develop a safe power supply system according to ISO 26262,
focusing on Part 3: Concept phase, specifying requirements
for:
1) item definition (Section IV-A);
2) hazard analysis and risk assessment (Section IV-B);
3) functional safety concept (Section IV-C).

Additionally, a detailed view on components of the power
supply system in context of functional safety (Section IV-D)
is provided.

A. ITEM DEFINITION

The first step in the ISO 26262 development process is called
item definition. The objective is “to define and describe the
item, its functionality, dependencies on, and interaction with
the driver, the environment and other items at the vehicle
level” [3]. This is a crucial point for all subsequent phases:
it needs to be ensured that the item under development shall be defined unambiguously to avoid any misunderstandings, including [3]:

1) legal requirements, national and international standards;
2) functional behavior and operating modes;
3) boundaries, interfaces and functional dependencies;
4) environmental conditions;
5) known failure modes and hazards.

The item itself is defined as “system or combination of systems, to which ISO 26262 is applied that implements a function or part of a function at the vehicle level” [32]. This step is usually in responsibility of the OEM, because only the OEM knows the whole vehicle and its boundary conditions. It is advised to include all involved stakeholders, e.g. product management, sales, potential suppliers or certification authorities in order to define the functionalities and boundary conditions as precisely as possible.

**FIGURE 7. Item and systems definition.**

For example, a vehicle function – i.e. “behaviour of the vehicle, […] that is observable by the customer” [32] – like steering functionality, may be implemented by the item “steering”. The item can be allocated to the systems electric power steering (EPS) and the power supply system, see Fig. 7. This definition is valid as long as each of the systems “relates at least a sensor, a controller and an actuator with one another […] The related sensor or actuator can be included in the system, or can be external to the system” [32]. In this case, the power supply system may be developed as a safety element out of context (SEooC) according to ISO 26262-10:2018, 9, i.e. as a platform solution independent of a specific vehicle context. However, during the integration of the power supply system as a SEooC into a vehicle-specific item, all the assumptions made during the tailored SEooC development process need to be validated. Alternatively, the power supply system can be defined as item itself. In this case, the HARA must be performed on power supply system level according to ISO 26262-3:2018, 6.4.2.6, considering the impact on multiple systems, which can lead to higher ASIL ratings.

In the following, we chose the first option and consider exemplarily the power supply system as a system below the item steering.

### B. HAZARD ANALYSIS AND RISK ASSESSMENT

After the item is sufficiently defined, “the hazardous events caused by malfunctioning behavior of the item” [3] shall be identified and classified. This is usually done by a situation analysis. Afterwards, the hazardous events are classified and the corresponding ASIL rating shall be derived. Additionally, all the safety goals to prevent and/or mitigate the hazardous events shall be formulated.

To systematically identify the complete set of potential hazardous events, it may be useful to utilize guideword analysis and driving situation catalogues. Such a guideword analysis can be the hazard and operability analysis (HAZOP). The HAZOP supports to identify hazardous events. In [33], it is defined as “an explorative type of analysis where applicable guidewords are applied to each of the functions of an item [and it] may be used to identify and evaluate malfunctioning behaviors of an item” – see also [34].

By use of these guidewords, the identification of hazardous events can be executed in a more structured and systematic way. Additionally, driving situation catalogues capture systematically different combinations of influencing factors by including without limitation:

1) locations: e.g. freeway or urban traffic;
2) road conditions: e.g. paved or asphalt;
3) traffic situations/maneuvers: e.g. overtaking, parking or turning;
4) vehicle states: e.g. coasting or accelerating;
5) different vehicle speeds.

For example, one of such catalogues was published by the VDA in 2015 [35]. In this catalogue, each situation owns an exposure rating. Additionally, SAE J 2980 includes several potential vehicle operational situations [33]. Besides the exposure (E) rating based on a certain situation, the controllability (C) and severity (S) of a hazardous event shall be classified according to ISO 26262.

**Table 1 describes the evaluation of E, C and S in more detail** [3]. It is explicitly stated that not just the driver is considered as a person potentially at risk, additionally, also cyclists, pedestrians or occupants of other vehicles shall be considered [3]. Furthermore, if the classification regarding exposure, controllability or severity is ambiguous, it shall be classified conservatively, “i.e. whenever there is a reasonable doubt, a higher S, E or C classification is chosen” [3].

More specific examples about the classification of hazards are given in Annex B of Part 3 of ISO 26262. Based on the exposure, controllability and severity, the ASIL rating can be derived.

**Table 2 presents the determination of the ASIL rating [3]:**

1) QM: Quality Management processes are considered as sufficient to manage the identified risk. This does not
TABLE 1. Evaluation of exposure, controllability and severity [3].

| Description          | Example                                                                 |
|----------------------|-------------------------------------------------------------------------|
| **Exposure**         |                                                                         |
| E1 Very low probability | less often than once a year for the great majority of drivers            |
| E2 Low probability    | Occurs a few times a year for the great majority of drivers             |
| E3 Medium probability | Occurs once a month or more often for an average driver                 |
| E4 High probability   | Occurs during almost every drive on average                              |
| **Controllability**  |                                                                         |
| C1 Simply controllable | > 99 % of the average drivers are able to avoid harm                   |
| C2 Normally controllable | Between 90 % and 99 % of the average drivers are able to avoid harm   |
| C3 Difficult to control or uncontrollable | < 90 % of the average drivers are able to avoid harm                   |
| **Severity**         |                                                                         |
| S1 Light and moderate injuries | Front collision with another passenger car with very low speed          |
| S2 Serve and life-threatening injuries | Bicycle accident with low speed                                        |
| S3 life-threatening and fatal injuries | Front collision with another vehicle with medium speed                  |

TABLE 2. Determination of ASIL rating [3].

|   | C1 | C2 | C3 |
|---|----|----|----|
| S1 | QM | QM | QM |
| E1 | QM | QM | QM |
| E2 | QM | A  | B  |
| E3 | QM | A  | B  |
| E4 | QM | A  | B  |
| S2 | QM | QM | QM |
| E1 | QM | QM | QM |
| E2 | QM | A  | B  |
| E3 | QM | A  | B  |
| E4 | QM | A  | B  |
| S3 | A  | B  | C  |
| E1 | A  | B  | C  |
| E2 | A  | B  | C  |
| E3 | A  | B  | C  |
| E4 | A  | B  | C  |

automatically mean an identified risk is not safety-related, but there is no requirement to comply with ISO 26262.

2) ASIL: ASIL A is considered as lowest safety integrity, whereas ASIL D implies the highest safety integrity.

The last step in the HARA is to specify the safety goals together with their ASIL ratings. Generally, a “safety goal shall be determined for each hazardous event with an ASIL evaluated in the hazard analysis and risk assessment” [3]. The safety goals are also called top-level safety requirements [3]. Additionally, similar safety goals can be combined. In this case, the highest ASIL rating shall be assigned to the combined safety goal [3]. Typically for deriving the safety goal, the hazard is combined with guidewords like prevent or mitigate.

Table 3 shows exemplarily an evaluation for the hazard “Sudden loss of steering assist” including the corresponding derivation of the safety goal “Prevent sudden loss of steering assist”. The fault tolerant time interval (FTTI) is defined as “minimum time span from the occurrence of a fault in an item to a possible occurrence of a hazardous event” and a “relevant attribute for safety goals” [32], and thus, defined on item level. It is derived from the HARA according to the specific hazardous events. In our case, we assume that 150 ms without steering assist may lead to a hazardous event, i.e., the FTTI is set to 150 ms.

Because a loss of the steering functionality directly leads to a hazardous situation while driving, a safety related availability (SaRA) requirement for the steering item is specified. For this safety goal, the following safe state definitions are possible:

1) Steering assistance needs to ensure that the driver is able to perform the minimal risk maneuver until the vehicle is transitioned to standstill based on the OEM specific warning and degradation strategy.

2) Pre-warning of the driver about the upcoming unavailability of the steering function and slowly fading out the steering system within a reasonable time span.

Safe state definition 2 might conflict with other safety goals. For example, steering heavy may have to be avoided with ASIL A after a loss of assistance according to vehicle hazard No. 3 in [31].

SaRA requirements request the availability of a function with the corresponding ASIL rating of the safety goal or requirement. If SaRA requirements with different ASIL ratings occur, several safety measures may be required. They are addressed by safety measures, including [36]:

1) fault prevention;
2) fault tolerance;
3) fault forecasting and fault detection.

Fault prevention shall be considered as strong foundation respectively minimum requirement for quality and functional safety. This is – at least to some degree – already achieved by following a guided development processes, e.g. according to the ISO 26262, or by solely using components which are rated with a certain quality grade. Regarding the power supply system development, there are currently two main strategies observable in the market to ensure safe power supply of braking and steering systems:
FIGURE 8. Exemplarily hierarchical requirements derivation for the safety goal “Prevent sudden loss of steering assist.”

1) Fault tolerance strategies focusing on additional backup supply with redundant power supply system branches, e.g. implemented by redundant DC/DC converters. In case fault tolerance is implemented by separable power supply system branches, a detection mechanism to trigger the separation is required.

2) Fault forecasting and fault detection strategies focusing on advanced diagnostics as well as fast and fine-grained switching characteristics based on electronic fuses. Effect mitigation due to e.g. reduced maximum vehicle speed – “limp home mode” – is not considered as separate strategy. Instead, effect mitigation may be addressed within a safety concept focusing on fault tolerance or fault forecasting and fault detection to reduce the risk of a certain hazard in the presence of one or more faults. Hence, an emergency operation can be ensured.

Within the next years, we expect a continuously increasing number of electric power steering systems rated with ASIL C to “Prevent sudden loss of steering assist”. Reasons are increasing vehicle weights, see Section II-C, and driver’s lack of experience with heavy steering situations – shifting acceptable steering forces in mechanical back-up situations to a lower limit.

C. FUNCTIONAL SAFETY CONCEPT

To prevent and/or mitigate the earlier derived hazardous events, i.e. to comply with the safety goals, the functional safety concept introduces safety measures and specifies functional safety requirements. Among other, the objectives of the functional safety concept are [3]:

1) “to specify the functional or degraded functional behavior of the item”;
2) “to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals”.

As a final step, the functional safety requirements are allocated to the system architectural design. In early development phases, this is supported by preliminary architectural assumptions [3].

Usually, the refinement of the safety goal is done in a hierarchical manner. In Fig. 8, such a hierarchical breakdown is shown for the safety goal “Prevent sudden loss of steering assist” – rated with ASIL C.

In the shown case, especially driven by the SaRA requirement, the following shall be specified [36]:

1) the functionality needed to prevent the hazardous event;
2) the failure reaction (emergency operation);
3) the safe state.

The safe state, i.e. “operating mode, in case of a failure, of an item without an unreasonable level of risk” [32] as defined on
item level is exemplarily broken down on system level to the
EPS itself and the power supply system:

1) SR1: The EPS itself shall be available. Non-availability
is allowed if its duration is below 150 ms – according
to FTTI – or its loss of function is timely
warned.
2) SR2: The input-voltage at the EPS shall not be < 8 V
for longer than 150 ms – premise: the minimal risk
maneuver is fully supported as long as the EPS voltage
is ≥ 8 V. Additionally, the hardware (HW) reset of the
steering system (e.g. U < 6 V for t > 100 µs) shall be
avoided because the time to restart and ramp in the EPS
after a HW reset is far longer than the FTTI.

By implementation of decentral measures, e.g., separation
of the logic supply from the load and implementing a
decentral storage element for the logic supply, the robust-
ness against HW reset (SR2) in a single component
can be increased. As this measure would have to be
applied for several safety-relevant loads while still not
solving SR1, holistic power supply system measures on
infrastructure level dealing with SR1 and SR2 at the
same time are strongly recommended. Regarding the HW
reset threshold, the fault handling time interval (FHTI_{max})
is set to 100 µs. Additionally, software (SW) switch-
off thresholds shall be considered. In Fig. 8, only the
shortest FHTI_{max} is shown. However, no generally valid
voltage-time-limits can be stated due to the dependency
on the implemented component and defined minimal risk
maneuvers.

Regarding the power supply system level (sub-system
level), there are three major topics to address:

1) SR2.1 – Power feed: An energy source and/or storage
must feed the electrical power for the electrical loads.
2) SR2.2 – Power distribution: The wiring, fusing and
switches of the power supply system must distribute the
electrical power from the energy source/storage to the
electrical loads.
3) SR2.3 – Freedom from interference: Electrical loads, the
physical power supply system components and the
power supply management must not interfere with
the power supply by violation of SR2. The freedom
from interference between sub-elements implementing
functions with different ASIL ratings is a basic principle
of ISO 26262 [37].

In the following, several recommendations, and hints
according to power supply system development with focus
on the ISO 26262 are highlighted.

### High-level safety requirements for safe power supply
systems development:

1) power feed;
2) power distribution;
3) freedom from interference.

In case of an ASIL decomposition into two redundant
functions, each single function shall be able to perform the
initial function on its own and in combination with the
redundant function together – under consideration of the
initial FHTI.

Sufficient independence between battery and DC/DC con-
verter shall be ensured, e.g. by a dependent failure analysis
(DFA). If a dependent failure is identified, e.g. discharge
of the battery in case of a failure of the DC/DC, a safety
mechanism to handle this dependency shall be applied with
the initial ASIL C and the increased requirements according to Section IV-C.3 need to be considered. To avoid these increased requirements, a preferred measure is to additionally detect continuous battery discharge within an electronic power distributor as a further ASIL decomposition.

### TABLE 4. HW metric targets dependent on ASIL rating [38].

| Metric | ASIL A | ASIL B | ASIL C | ASIL D |
|--------|--------|--------|--------|--------|
| General handling | avoid potential failures by robust and tested design | control potential failures |
| PMHF | No | No | < 100 FIT | < 100 FIT | < 10 FIT |
| SPF | No | No | > 90 % | > 97 % | > 99 % |
| LFM | No | No | > 60 % | > 80 % | > 90 % |

#### 2) HARDWARE METRICS INCLUDING BUDGETING

Besides the ensurance of systematic development, ISO 26262 requires the quantitative safety evaluation of random HW faults by so called HW metrics. Table 4 summarizes the targets of the HW metrics with respect to the different ASIL ratings [38]:

1) Probabilistic metric for random hardware failures (PMHF): “represents a quantitative analysis which evaluates the violation of the considered safety goal by random failures of the hardware elements”.

2) Single-point fault metric (SPFM) “reveal whether or not the coverage by the safety mechanisms, to prevent risk from single-point or residual faults in the hardware architecture, is sufficient”.

3) Latent-fault metric (LFM) is similar to SPFM, but with focus on the sufficiency of “the safety mechanisms, to prevent risk from latent faults in the hardware architecture”.

The result of the PMHF calculation is considered as “average probability per hour over the operational lifetime of the item” [38]. The unit is failure in time (FIT). 1 FIT is defined as one failure per $10^{9}$ operational hours. The PMHF target value as well as the target of the HW architectural metrics, i.e. SPFM and LFM, shall be reached at item level [38].

The ISO 26262 is not considering explicit target values for allocated and decomposed safety requirements. However, the OEM can allocate a certain PMHF budget to specific failure modes of the technical components. The budgeting must be performed in a way that the PMHF on item level will not be increased. Regarding the HW architectural metrics, the following recommendations can be applied as a first assumption:

1) ASIL allocation: It is sufficient to take over the target values for SPFM and LFM from higher-level requirement.

2) ASIL decomposition: The SPFM is taken over from the LFM of the higher-level requirement. No direct requirements for the LFM are considered on lower level. Alternatively, SPFM budgeting between the decomposed requirements can be performed, as long as the initial LFM target is fulfilled.

An exemplary budgeting is shown in Fig. 8. For explanation: single point faults (SPF) on lower-level requirements do not directly violate the higher-level safety requirement in case of redundancy and absence of a dependency. Instead, the single point fault on lower level can be considered as a latent fault for the higher-level requirement.

According to Table 4, the derived PMHF target value on item level is 100 FIT for a safety goal rated with ASIL C. Regarding the PMHF-budget assignment this target value on item level “may be directly allocated to each system composing the item” [38]. Hence, the EPS itself (SR1) and the power supply of the EPS (SR2) need to achieve the PMHF target value of 100 FIT on system level independently from each other. Currently, there is no established common understanding about the applicability of ISO 26262-5:2018, 9.4.2.3. According to this clause, following conditions need to be fulfilled [38]:

1) “each of these systems has the potential to violate the same safety goal and;
2) the corresponding item target value is not increased by more than one order of magnitude.”

Note: this procedure is only valid in case of a requirements derivation onto systems, as explained in Section IV-A respectively Fig.8, i.e. system definition of ISO 26262 needs to be considered [32]. However, in case the power supply system is considered as item – i.e. according to the alternative option in Section IV-A – the PMHF target value is less ambiguous but dependencies on/to other items must be analyzed carefully.

Currently, there is no established common understanding about the applicability of ISO 26262-5:2018, 9.4.2.3. Further clarification would be appreciated in the third version of the ISO 26262.

#### 3) DERIVATION OF FAILURE RATES WITH FOCUS ON SINGLE POINT FAULTS AND RESIDUAL FAULTS

In case of an ASIL C or ASIL D safety goal, additional ISO 26262 requirements for SPF and residual faults (RF) must be considered [3], [38]. Quantitative or qualitative measures shall be taken to argue “sufficiently low probability of occurrence” [38] of SPF and of RF, see Table 5:

### TABLE 5. FIT rate targets of SPF and RF [38].

|       | SPF   | RF (DC* < 90 %) |
|-------|-------|-----------------|
| ASIL C | < 0.1 FIT | RF < 0.1 FIT |
| ASIL D | < 0.01 FIT | RF < 0.01 FIT |

*Diagnostic Coverage

In the example given in Fig. 8, the probability of a SPF of a hardware part to violate the safety goal, e.g. an open
circuit of a wire to the EPS, shall be < 0.1 FIT. For a quantitative analysis, a failure modes, effects and diagnostic analysis (FMEDA) may be used as inductive analysis instead or additional to the deductive FTA [39]. For detailed analysis of the power supply system, different time bases can be considered, e.g. for diagnostics, see [40].

The failure rates of the base events in FMEDA respectively FTA are typically derived from failure rate catalogues in combination with failure distributions. The SN 29500 [41] is a prevalent failure rate catalogue within the automotive industry – typically combined with the failure distribution according to Birolini [42]. However, there are more failure rate catalogues, e.g.:

1) IEC 62380 [43];
2) MIL HDBK 217 F [44];
3) IEC 61709 [45];
4) FIDES 2009 EdA [46];
5) GJB/Z 299C [47].

To use failure rates of these catalogues within a specific use case, i.e. certain temperature profile or voltage range, they may need to be adapted by a certain mission profile, e.g. provided by the IEC 62389 or based on internal investigations. Instead of using a failure rate catalogue – in the ISO 26262 described as “recognised industry source” [38] – failure rates may be estimated based on statistics of field returns or expert judgements [38]. A sufficient evidence shall be provided to argue the method used to derive the failure rates [38].

4) FREEDOM FROM INTERFERENCE
“Freedom from interference is used to justify the coexistence of elements with different, or no, assigned ASIL” [37]. The power supply system includes safety-relevant loads, rated with a certain ASIL, and QM components without any ASIL rating. A potential fault is a short circuit of a QM component, e.g. engine cooling fan or seat heating, which leads to a voltage drop in the power supply system. As a result, an undervoltage scenario occurs affecting the functionality of safety relevant loads. This interference of the QM component on the safety-relevant functions shall be avoided. To do so, potential measures may be:

1) Proof that even under worst-case conditions faults of the QM components do not impact the safety-relevant functions, also considering dependent failures.
2) Qualification of QM components according to the highest ASIL rating to avoid interference with safety-relevant functions. Due to several reasons, this approach leads to major draw backs, e.g.: a. high costs due to qualification of a high number of components; b. reduced scalability in case of differing power supply system requirements within different vehicle segments; c. high development complexity due to required ISO 26262 compliant development process, rolled out over the whole vehicle and supply chain.

3) Definition of dedicated safety mechanisms to handle the QM component faults within the defined FHTI. For this reason, additional components like electronic switches, distributors and/or backup power storages are installed in the safety-relevant power supply systems.

In case of using backup power storages, a mechanism to separate the backup supply from the main power supply during under- and overvoltage scenarios is mandatory. Backup storage can be used either for the power supply of one single component or a cluster of components. Another solution would be a complete redundant power supply or a redundant functional system.

To avoid fully redundant and independent power supply systems – e.g. like used in the avionics – additional components like electronic switching devices or backup storage are required to ensure freedom from interference in safety-relevant power supply systems.

D. CRUX: ALLOCATION OF FUNCTIONAL SAFETY REQUIREMENTS TO TECHNICAL SOLUTIONS
In the following, each safety requirement SR2.1, SR2.2 and SR2.3 is discussed in more detail with focus on the different technical solutions. These components are evaluated for their suitability in a safety-relevant application.

1) SR2.1 – POWER FEED
As discussed in Section IV-C, we decompose the power feed into “power feed by a power storage”, e.g. lead battery or lithium-ion battery, and “power feed by a power source”.

a: USE OF LEAD BATTERIES FOR SAFE POWER FEED
This chapter is focusing on power feed by a 12 V lead battery. In case the power feed is considered as a safety-relevant function in the safety concept, the power feed by the battery needs to be considered in the development process according to [3] due to its electrical interfaces – even though it is an electro-chemical element.

According to ISO 26262, systematic faults and random HW faults must be differentiated. Typically, systematic faults, i.e. if a root cause can be explained, are not considered within the quantitative analysis since safety measures are defined in the development process to avoid a critical failure effect. However, in case a systematic root cause leads to a random HW fault due to, e.g., insufficient safety measure or systematic measurement deviation in control function at production, these causes must be considered in the quantitative evaluation according to ISO 26262. Therefore, Bosch is considering major systematic battery issues, e.g. corrosion or sulphation, in the quantitative analyses.

From diagnostic perspective, faults of the battery shall be divided into:

1) Gradual faults: which can be pre-detected, i.e. detection before SR2.1.1 is violated;
2) Sudden faults: which can only be post-detected, i.e. after SR2.1.1 is violated – post-detection mechanisms are only applicable in case of redundant power supply systems to improve ISO 26262 metrics. Gradual faults of the battery are triggered by systematic effects, e.g. age, low state-of-charge (SoC) or low temperature of the battery, which cannot be avoided completely by design. Therefore, measures need to be implemented to pre-detect non-performant batteries, i.e. before violation of SR2.1.1 due to gradual faults. To ensure ISO 26262 compliance for the power feed by the battery, each failure mode of the battery needs to be handled by a dedicated safety mechanism. Additionally, without dedicated safety mechanisms, ISO 26262 target metrics typically cannot be met due to dominance of battery failures within the power supply system. Since the battery lifetime highly depends on its usage, simple measures like time-based battery exchange and advanced load management are not capable to sufficiently handle gradual faults. Depending on the stress of the battery over lifetime, the time-based battery exchange might either occur too early – leading to unnecessary maintenance cost for the end user – or might even occur too late – resulting in a possible hazard. Due to the weak correlation of the calendric battery age and its health status, a time-based battery exchange is by default imprecise. To ensure a safe power feed by the battery, dedicated safety mechanisms by an enhanced battery monitoring are required. Such a monitoring shall be able to detect battery faults before they lead to a safety critical condition in the power supply system. This includes battery faults leading to reduced power and/or energy capability, e.g. corrosion, sulphation, loss of active mass, cell short circuit and water loss. In addition, battery conditions like low SoC and low temperature shall be avoided by design, e.g. with an intelligent energy management. Nevertheless, these faults shall also be detected by the battery monitoring and communicated to a higher-level ECU. Because the typical lead battery lifetime is shorter than the vehicle lifetime due to cycling by normal battery usage and calendric ageing, the lead battery systematically fails within the vehicle lifetime. Therefore, the reduction of the ASIL rating according to [48] cannot be applied for the battery monitoring.

Sudden faults cannot be detected before their occurrence. They are caused by systematic or random HW faults, e.g. the rupture of terminal shaft. Sudden faults directly lead to the loss of the power feed by the battery and to a violation of SR2.1.1. Thus, sudden faults shall be avoided with the initial ASIL derived for the power feed by the battery according to SR2.1.1 in Fig. 8. Because sudden battery faults can only be avoided by design, these faults are considered by allocation to other technology [3] and shall be handled in the development and manufacturing process by the battery manufacturer.

As described earlier, safety mechanisms for the sudden battery faults can only be applied in case of redundancy in the power feed of the power supply system. Otherwise, the safety mechanisms are not effective because they cannot be achieved within the FTTI. For example, during use of a redundancy concept, these sudden faults are treated as latent faults. Thereby, the redundancy is required with the initial ASIL. And for each redundant sub-system, if applicable, an additional safety mechanism is to be implemented to prevent fault from being latent. These additional safety mechanisms can be implemented with reduced ASIL according to ISO 26262-4:2018, 6.4.2.5 [48].

Intelligent and ASIL compliant battery monitoring with high diagnostic coverages enables safe power supply systems based on 12 V lead batteries despite high failure rates. Sudden faults must be considered in the development and manufacturing process by the battery manufacturer.

b: USE OF POWER SOURCES FOR SAFE POWER FEED
In case of a conventional ICE vehicle with an alternator, the requirement to ensure the power feed independent of the battery cannot be achieved by default. Therefore, additional measures may have to be implemented to take reduced dynamic performance of the alternator into account, e.g. reduce dynamics of loads after detection of battery off or double-layer capacitors to buffer high transients. Since the alternator is relying on mechanical energy from the powertrain, only a QM-rated power feed by the alternator can be ensured. Otherwise, several mechanical components involved in the propulsion of the vehicle would inherit an ASIL-rating. In DC/DC converter vehicles, there is no safety relevance on the mechanical parts anymore due to second full electro-chemical system. As a result, the constraints of keeping the QM rating is not mandatory any longer. Anyway, the QM-rating on the power source enables scalable solutions between ICE and non-ICE vehicles. Additionally, no safety requirements need to be allocated to the high voltage power supply system branch in case of a non-ICE vehicle. A further advantage of a QM-rated power feed is that QM components can stay within this QM power supply system branch without additional measures or qualification because no freedom from interference requirements arise. In this case, a centralized safety measure may be used to argue the freedom from interference between safety-relevant and non-safety-relevant power supply system branches.

2) SR2.2 – POWER DISTRIBUTION
According to ISO 26262, failure rates of wiring harness components shall be considered in quantitative analyses [38]. One crucial point for the quantitative evaluation may be the FIT rate determination of the physical components of the power supply system. Not all physical components, e.g. wires, fuses, cable lugs, connectors, splices and screw connections are listed in the SN 29500 [41]. The SN 29500 was originally not focusing on the automotive industry.
Currently, there is no state-of-the-art source available including failure rates for all relevant parts of a power supply system. Hence, it is necessary to combine different failure rate sources to evaluate a power supply system with regards to random HW faults. Beside failure rates from failure rate catalogues, results from statistics based on field returns or expert judgements can be used.

The ISO 26262 explicitly allows such a combination of failure rates of different sources, if failure rates are missing in the preferred data source – in our case the SN 29500. A scaling factor shall be derived to adapt “the quality of prediction of the different failure rates” [38]. To do so, the scaling factor is determined as the ratio of two similar elements which are listed in both sources – in consideration of the confidence levels of the data bases [38]. However, there are still evidences required for both sources to argue their sufficiency, e.g. regarding comparability or the generally applicable foundations of statistics. The ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie) is currently working on a technical guideline – called “Ausfallraten für Bordnetz-Komponenten im Automobil - Erwartungswerte und Bedingungen“ – focusing on FIT rates of the physical power supply system. We expect that this document will become state of the art and applicable according to ISO 26262.

Upcoming technical guideline by ZVEI will provide standardized failure rates for ISO 26262-compliant metric calculation of the wiring harness.

### Table 6. ISO 8820-3: Operating times of melting fuses [49].

| Operating time (s) | Type C* P* | Type E* |
|-------------------|------------|---------|
| 2 \cdot I_{th}   | 0.15       | 5       |
| 3.5 \cdot I_{th} | 0.04       | 0.5     |
| 6 \cdot I_{th}   | 0.02       | 0.1     |

*medium; P*miniature; I*current

An example for interference effects between a QM component and the EPS is shown in Fig. 9. In this case, a Type E 80 A fuse is applied in the supply path of the engine cooling fan to protect the wiring harness of the engine cooling fan. After a short circuit to ground in the connector of the engine cooling fan occurs, a significant voltage drop at the EPS follows. In this example, the duration of the melting fuse to blow is so long that the power supply by the DC/DC converter is interrupted, and the voltage falls below the EPS HW reset threshold. As already described in Section IV-C, the time to restart and ramp in the EPS after a HW reset is far longer than the FTTI for the steering function. Therefore, a sudden loss of steering assist, as described in Fig. 8, cannot be prevented by a melting fuse.

**3) SR2.3 – FREEDOM FROM INTERFERENCE**

Melting fuses seem to be a proper safety measure to ensure freedom from interference of a QM component. However, the basic idea of melting fuses is to separate the wiring harness before a thermal incident occurs, i.e. to ensure wiring protection while being robust against typical load profiles. Because of the thermal capacity of the wiring, there is no need for fast separation within µs. As a result, a certain tolerance in the melting behavior can be accepted.

Table 6 shows an extract of the ISO 8820-3 focusing on the operating times of melting fuses to blow. As shown below, the specified time to blow a melting fuse differs widely. Typical melting fuses within the automotive industry are Type C and E fuses. Whereas Type C fuses are in the range between 1 A and 40 A, Type E fuses covering the range from 20 A to 100 A [49].

Using melting fuses in a safety application, the following disadvantages must be considered:

1) Due to slow separation (typically several ms) and high tolerance range, functional protection of safety relevant ECUs cannot be achieved. Therefore, freedom from interference may not be ensured.

2) No diagnostics possible to determine the current state of health of the melting fuse. For example, latent faults due to thermal stress leading to shifted fuse characteristics cannot be forecasted.

3) Melting fuses are typically accessible by the end user. Thus, it needs to be ensured that the respective vehicle is always equipped with the correct fuse. Particularly the replacement with aftermarket fuses needs to be considered if the safety concept relies on the use of melting fuses which are qualified by certain manufacturers to exceed market standards.

An example for interference effects between a QM component and the EPS is shown in Fig. 9. In this case, a Type E 80 A fuse is applied in the supply path of the engine cooling fan to protect the wiring harness of the engine cooling fan. After a short circuit to ground in the connector of the engine cooling fan occurs, a significant voltage drop at the EPS follows. In this example, the duration of the melting fuse to blow is so long that the power supply by the DC/DC converter is interrupted, and the voltage falls below the EPS HW reset threshold. As already described in Section IV-C, the time to restart and ramp in the EPS after a HW reset is far longer than the FTTI for the steering function. Therefore, a sudden loss of steering assist, as described in Fig. 8, cannot be prevented by a melting fuse.

The HW reset threshold is not the only threshold which needs to be considered. Before the HW reset threshold is reached, the voltage drops to a level, where the steering ECU deactivates the support due to insufficient power input. If the
duration of the deactivation is longer than the FTTI, the safety goal is also violated. Even if the short circuit is separated and the voltage rises above a certain value within the FTTI, a sudden loss of steering assist may not be avoided due to a slow ramp in of the steering assistance.

After the steering assistance was lost for a longer time span – this time span is application-specific – the steering assistance is ramped-in slowly within a range of several hundred milliseconds to avoid oversteering of the vehicle by the driver.

To use melting fuses as a safety mechanism to ensure freedom from interference, a sufficient argument needs to be provided to proof fast separation within a specific use case. The argumentation shall include following aspects:

1) Consideration of every single fuse-protected QM load;
2) Consideration of worst-case boundary conditions:
   a) Slowest fuse blow characteristics according to ISO 8820 [49] or statistically proven faster fuse blow characteristics including measures to avoid use of unauthorized fuses;
   b) High load conditions, e.g. winter scenario;
   c) Activation of high transient loads, e.g. steering and braking;
   d) Low ambient temperatures, e.g. -25 °C;
   e) Aged components within specification, e.g. wiring connectors and battery;
   f) Discharged battery within specification – typically around the warning threshold;
   g) Variation of short circuit resistance;
3) In case of an ASIL decomposition to realize the power feed requirement SR2.1 in Fig. 8, consideration of every power feed path and the combination of both power feed paths is necessary:
   a) Power feed from battery (SR2.1.1) and a short circuit at the same time;
   b) Power feed from source, e.g. alternator or DC/DC converter (SR2.1.2) and a short circuit at the same time;
   c) Combined power feed of battery and power source and a short circuit at the same time;

To explain the last requirement in more detail, the following example is used: The power feed is decomposed into power feed by battery and DC/DC converter, comparable to Fig. 8. Therefore, both power feed paths must supply the safety relevant loads independently. If a short circuit of a fuse-protected QM load can disturb the power feed of the battery path – which is rated with ASIL A or higher – a measure to ensure freedom from interference is required with the same ASIL rating as the power feed by the battery. A standard melting fuse cannot ensure such a separation and thus, is not a valid safety mechanism in this case.

To properly ensure freedom from interference, we recommend to use electronic switches due to very fast and fine-grained switching characteristics within the range of microseconds, see e.g. [50]–[52], and advanced diagnostics.

| Melting fuses focus on thermal wiring protection – they are not effective safety measures to ensure functional protection of safety relevant ECUs due to undefined and slow separation as well as missing diagnostics. |

V. CONCLUSION

Especially driven by the megatrends electrification and automation, functional safety requirements for the power supply system are increasing continuously. However, faults in the power supply system are the major contributor for vehicle breakdowns and thus, potentially violating safety goals. Whereas nowadays functional safety is strongly recommended to argue in case of a product liability trial, the fulfillment of functional safety requirements will become mandatory for vehicle homologation in the future. As of 2022, steering electronic control systems, including its power supply, must be developed and assessed according to functional safety standards to achieve homologation in China.

Before creating a functional safety concept, the scope, i.e. the item, needs to be defined and hazards need to be identified. These first two steps are typically in responsibility of the OEM.

To ensure safe power supply, a consistent and holistic functional safety concept based on three high-level safety requirements must be considered:

1) Power feed by the power sources and storages;
2) Power distribution via the wiring harness;
3) Freedom from interference between safety-relevant and non-safety-relevant loads respectively safety-relevant loads with different ASIL ratings.

In case of an ASIL decomposition for the power feed into two redundant paths, each single power source or storage shall be able to perform the initial function on its own. Regarding the power feed by the battery, a detection of gradual faults by an intelligent battery diagnostic is mandatory. At least enough power and energy to perform a minimal risk maneuver must be ensured. Such an advanced and intelligent battery diagnostic can be implemented, e.g., on an ASIL-qualified electronic battery sensor. Therefore, safe power supply systems based on 12 V lead batteries can be enabled.

The wiring harness is in scope of the ISO 26262 for systematic development as well as for the quantitative evaluation of the HW metrics. However, there are no standardized failure rates for all components of the wiring harness available to enable an ISO 26262-compliant metric calculation. An upcoming technical guideline by ZVEI will close this gap.

To ensure freedom from interference in safety-relevant power supply systems without fully redundant and independent power supply systems – e.g. like used in the avionics – additional components are required. Melting fuses
focus on thermal wiring protection and are not effective safety measures to ensure functional protection of safety relevant ECUs. To properly ensure freedom from interference, we recommend using electronic switches due to very fast and fine-grained switching characteristics and extended diagnostics, e.g. implemented in a centralized smart safety switch or decentral electronic fuses.

Power supply systems are in a phase of change and standardization is needed to avoid insufficient dimensioning, especially with focus on functional safety. This paper contributes to a further standardization of the power supply system development process from a functional safety perspective.

ACKNOWLEDGMENT

The authors would like to thank Boerge Carstens, Michael Dehnert, David Linden, Frederic Heidinger, Jiang Shangxing, and Markus Wörz for many inspiring discussions and particularly their contributions regarding the GB 17675-2021 as well as the input for the functional safety concept.

REFERENCES

[1] ADAC. Pannenstatistik 2020: Die Zuverlässigkeit-Hitliste. Accessed: Apr. 4, 2021. [Online]. Available: https://www.adac.de/rund-ums-fahrzeug/uns-fahren-scheiden/panne/adac-pannenstatistik/

[2] A. Koehler and B. Bertsche, “An approach of fail operational power supply for next generation vehicle powernet architectures,” in Proc. 50th Eur. Saf. Rel. Conf. 15th Probabilistic Saf. Assessment Manage. Conf. (ESREL-PSAM), Venice, Italy, Nov. 2020, pp. 60–67. [Online]. Available: https://www.rpsonline.com.sg/proceedings/esrel2020/pdf/5731.pdf; doi: 10.3850/978-981-14-8593-0.

[3] Road Vehicles–Functional Safety—Part 3: Concept Phase, Standard ISO 26262-3:2018(E), 2018.

[4] Recall. Citroën C3 Aircross (2016–2019). Accessed: Apr. 5, 2021. [Online]. Available: https://car-recalls.eu/recall/citroen-c3-aircross-2016-2019/

[5] Harris Lowry Manton LLP. BMW Recalls More Than One Million Cars Because of Electrical Fire Danger. Accessed: Apr. 5, 2021. [Online]. Available: https://www.hmlawfirm.com/blog/bmw-recalls-more-than-one-million-cars-electrical-fire-danger/

[6] USA Today. Audi Recalls 1.2 Million Vehicles; Coolant Pumps Can Overheat. Accessed: Apr. 5, 2021. [Online]. Available: https://eu.usatoday.com/story/money/cars/2018/04/24/audi-recall-coolant-pumps-overheat/545548002/

[7] K. Holt. Toyota Recalls Over a Million Hybrid Vehicles Due to Fire Risk. Accessed: Apr. 5, 2021. [Online]. Available: https://www.engadget.com/2018-09-05-toyota-recalls-over-a-million-hybrid-vehicles-due-to-fire-risk.html

[8] NBC New. GM is Recalling 1M Pickup and SUVs because the Power Steering Can Suddenly Fail. Accessed: Apr. 5, 2021. [Online]. Available: https://www.nbcnews.com/business/consumer/gm-recalling-1m-pickup-suv-because-power-steering-can-suddenly-fail-no90196

[9] Paris Agreement, United Nations. Accessed: Apr. 5, 2021. [Online]. Available: https://unfccc.int/sites/default/files/english_paris_agreement.pdf

[10] STATISTA GmbH. Breakdown of Global Car Sales in 2019 and 2020, by Fuel Technology. Accessed: Oct. 16, 2020. [Online]. Available: https://www.statista.com/statistics/827460/global-car-sales-by-fuel-type/

[11] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, document SAE J 3016, 2018.

[12] ECE R 13-H, Regulation No 13-H of the Economic Commission for Europe of the United Nations (UN/ECE)—Uniform Provisions Concerning the Approval of Passenger Cars With Regard to Braking, 2015.

[13] STATISTA GmbH. Projected Global ADAS Market Size Between 2015 and 2023. Accessed: Jan. 22, 2021. [Online]. Available: https://www.statista.com/statistics/591579/adas-and-ad-systems-in-light-vehicles-global-market-size/
A. Köhler and B. Bertsche, “Evidence of the effectiveness of cyclic technical safety mechanisms,” *IEEE Access*, vol. 9, pp. 82188–82198, 2021, doi: 10.1109/ACCESS.2021.3085662.

Siemens AG, *Failure Rates of Components—Expected Values, General*, document SN29500, 2004.

A. Birolini, *Reliability Engineering: Theory and Practice*, 2nd ed. New York, NY, USA: Springer, 2017, doi: 10.1007/978-3-662-54209-5.

*MIL HDBK 217 F Notice 2, Military Handbook: Reliability Prediction of Electronic Equipment, U.S. Dept. Defense, Washington, DC, USA, 1995.*

*Electric Components–Reliability–Reference Conditions for Failure Rates and Stress Models for Conversion; Corrigendum 1*, document IEC 61709 CORRIGENDUM, 2019.

*FIDES guide, Reliability Methodology for Electronic Systems, Edition A, Paris, France, 2010.*

*Handbook of Reliability Prediction of Electronic Equipment, Beijing: The General Reserve Department of PLA, [48] document ISO 26262:4-2018(E), 2006.*

*Road Vehicles–Functional Safety—Part 4: Product Development at the System Level, document ISO 8820-3:2015(E), 2018.*

*Road Vehicles–Fuse-Links—Part 3: Fuse-Links With Tabs (Blade Type) Type C (Medium), Type E (High Current) and Type F (Miniature), document ISO 8820-3:2015(E), 2015.*

*STMicroelectronics. (Sep. 2011). STB155N3LH6. [Online]. Available: https://www.st.com/resource/en/datasheet/stb155n3lh6.pdf*

*Vishay Siliconix. IRF510, SIHF510. Accessed: Nov. 16, 2015. [Online]. Available: https://www.vishay.com/docs/91015/sihf510.pdf*

*Infineon. OptiMOS-T2 Power-Transistor. Accessed: Nov. 30, 2011. [Online]. Available: https://www.infineon.com/dgdl/Infineon-IPD60N10S4L_12-DS-v01_00-en.pdf?fileId=d8b3a3043372dc801374f5d1cd0505*

*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 in modular and scalable safety concepts with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart-in cooperation with Robert Bosch GmbH. He is also working as a Doctoral Student in the field of functional safety in the area of automotive power supply systems.*

*ARMIN KÖHLER was born in Berlin, Germany, in 1993. He received the Master of Science degree in electrical engineering from the Karlsruhe University of Applied Sciences, in 2018. He is currently pursuing the Ph.D. degree in technical safety mechanisms with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart-in cooperation with Robert Bosch GmbH. He is also working as a Doctoral Student in the field of functional safety in the area of automotive power supply systems.*

*PATRICK VAN BERGEN was born in Waiblingen, Germany, in 1989. He received the Master of Science degree in mechanical engineering from Reutlingen University and the University of Stuttgart, in 2015. He was working as a Doctoral Student in the field of functional safety for automotive electronics–power supply systems with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart. In 2018, he began his professional career at Robert Bosch GmbH, where he is currently coordinating the functional safety topics in the power supply system area.*

*CARSTEN GEBAUER began his professional career at Robert Bosch GmbH, in 2000, where 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.*

*BERND PFEUFER began his professional career at CONTEXT AG, Munich, from 2010 to 2019. He has been working as a functional safety engineer and a consultant for several OEMs and 1st Tier. Since 2015, he has been involved into the development of the power supply domains for several OEMs and manufacturers. In 2016, he joined the ZVEI WG ASIL Metric at Bayern Innovativ for gaining information about failure rates of power net components. Since 2019, he has been working for TÜV SÜD Auto Service GmbH, where he became the Head of the Inspection Body for Automotive Functional Safety.*

*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. Since 2018, he has been leading the systems engineering and application development for power supply components and the part of the VDA450 Group “Power supply systems for automated driving,” since 2019.*

*BERND BERTSCHE began his professional career at Daimler AG, Stuttgart, from 1989 to 1992. He has been a Professor of mechanical engineering with the Institute of Machine Components, University of Stuttgart, and the Head of the Reliability Engineering Department, since 1996. In 2001, he became the head of the institute and the Head of the VDI Advisory Board “Reliability Management.” He has been a member of the DIN/DKE Standardization Committee K132 Reliability, since 2003, and the National Academy of Science and Engineering, since 2015. He was elected to be a member of the Review Board of the German Research Foundation, in 2012. In 2013, he was elected to be the Managing Director of the WiGeP e.V.*