Electrical Power Supply System regarding automated driving in the context of ISO 26262

VDA
450

Table of Contents

Fortsetzung Seite 2 bis 109 *Continued page 2 to page 109*

Herausgeber/*Editor*: VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA); Behrenstr. 35; 10117 Berlin; www.vda.de
Vertrieb/*Sales*: VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA); Behrenstr. 35; 10117 Berlin; www.vda.de

Table of Figures:

List of Tables:

Haftungsausschluss:	***Disclaimer:***
Die VDA-Empfehlungen sind Empfehlungen, die jedermann frei zur Anwendung stehen. Wer sie anwendet, hat für die richtige Anwendung im konkreten Fall Sorge zu tragen.	*The VDA recommendations are recommendations that are available for anyone to use. Anyone using these recommendations is responsible for ensuring that they are used correctly.*
Sie berücksichtigen den aktuellen Stand der Technik, der zum Zeitpunkt der jeweiligen Ausgabe herrscht. Durch das Anwenden der VDA-Empfehlungen entzieht sich niemand der Verantwortung für sein eigenes Handeln. Jeder handelt insoweit auf eigene Gefahr. Eine Haftung seitens des VDA und derjenigen, die an der Erstellung der VDA-Empfehlungen beteiligt sind, ist ausgeschlossen.	*The VDA recommendations give due consideration to the prevailing state-of-the-art at the time of publication. Use of the VDA recommendations does not allow a person to avoid assuming responsibility for his or her actions. In this respect, everyone acts at his or her own risk. The VDA and the parties involved in drawing up the VDA recommendations assume no liability whatsoever.*
Jeder wird gebeten, wenn er bei der Anwendung der VDA-Empfehlungen auf Unrichtigkeiten stößt oder die Möglichkeit einer unrichtigen Auslegung erkennt, dies dem VDA umgehend mitzuteilen, damit etwaige Mängel beseitigt werden können.	*We request that anyone encountering an error or the possibility of an incorrect interpretation when using the VDA recommendations contacts the VDA immediately so that any errors can be rectified.*
	The document is a translation of the German version. Therefore, the German document represents the original and should be referenced in case of discrepancies. Due to the fact that this document is a translation, it may be the case that the English text leaves room for interpretation because certain terms are often deeply rooted in the original language, and therefore it is not possible to translate them into another language without a certain degree of ambiguity arising.

1. Preface

As electrification and digitalization increase, so does the level of automation of vehicle functions. In connection with this, a safety-oriented development aimed at protecting life and limb is a prerequisite. For this reason, ISO 26262 – now available in the second edition - was launched back in 2011 as a global standard for developing pertinent vehicle functions.
As a basic function of a vehicle, the electrical power supply provides energy for all electric systems and functions in the vehicle. Without the respective function of providing energy, electric functions cannot be performed either. Traditionally, many functions currently being developed in the context of ISO 26262:2018 are implemented as Pail-Passive functions. When a fault occurs, the transition to a safe state is normally performed without the need for power supply. There are some exceptions in this case, e.g. the light function and the wiper function of a vehicle, which were designed fault-tolerant by using different power distributions for the right/left side (cross-connection).
When using semi- or fully-automated vehicle functions (level 3-5 as described in SAE J3016:2021), which allow for vehicle operation without human intervention either temporarily or completely, a Fail-Passive function is no longer sufficient as a continuation of the vehicle operation is necessary after a fault to avert current danger and furthermore to reach a safe state. In such cases, the term "Fail-Active" functions is used or, in this document, "safety-relevant vehicle functions". In this context, safety relevance refers to the availability of power.
Accordingly, the power supply for the implementation of Fail-Active vehicle functions is also subject to the same requirements for safety-oriented design and development defined in ISO 26262:2018 as the vehicle functions themselves. In the process, due consideration must be given to the fact that a vehicle shall be able to support not just one SR-Vehicle-Function but several. These may be utilized at staggered intervals or occur simultaneously.
The objective of this VDA recommendation is to define a safety standard for the electrical power supply, which is reflected in the interpretation of the relevant passages of ISO 26262:2018, the structure of the safety concept and the requirements for the Elements. Furthermore, this recommendation deals with critical issues in the application of ISO 26262:2018 and presents exemplary case studies.

2. Scope and Boundary of the Recommendation

This recommendation aims in particular at the design of electrical power supplies including their physical and functional Elements in the context of automated vehicle functions with SAE J3016:2021 level 3 to 5. It should be pointed out that a transfer of some parts to lower SAE levels is both permissible and useful. This recommendation is also relevant and applicable to safety-relevant systems such as Brake-by-Wire or Steer-by-Wire without a mechanical, hydraulic or pneumatic fallback level.

This recommendation follows a top-down approach, which derives the requirements for the electrical power supply from the SR-Vehicle Function, ISO 26262:2018 and the legal requirements for the Electrical Power Supply System and its components.

Explicitly not included in this recommendation are considerations of the communication network (all bus systems, ethernet, pulse width modulation etc.) as well as aspects regarding the intrinsic protection of the electrical power supply (wire protection, arc protection, high voltage safety etc.). It should be noted that an optional starting point for the issue of intrinsic protection of the electrical power supply and its Elements is presented in the discussion of the structure of the safety concept. (Cf. chapter 5.2.1)

3. Definition of Terms, Abbreviations and Nomenclature

3.1 Definition of Terms and Abbreviations

- **Definition/Abbreviations from ISO 26262-1:2018**
- **Cascading Failure:** Failure of an Element resulting from a root cause and then causing a failure of another Element
- **Common Cause Failure:** Failure resulting directly from a single specific event or root cause
- **Component:** "Non-system level Element that is logically or technically separable and is comprised of more than one hardware part or one or more software units.
  Example: a microcontroller
  Note 1: A component is a part of a system"
- **DC:** Diagnostic Coverage; “Percentage of the failure rate of a hardware element , or percentage of the failure rate of a failure mode of a hardware element that is detected or controlled by the implemented safety mechanism”
- **Element:** "System, components (hardware or software), hardware parts, or software units.
  Note 1: When "software Element" or "hardware Element" is used, this phrase denotes an Element of software only or an Element of hardware only, respectively.
  Note 2: An Element may also be an SEooC (Safety Element out of Context)"
- **EO:** Emergency Operation; Operating mode of an item, for providing safety after the reaction to a fault until the transition to a safe state is achieved.
- **EOTI:** Emergency Operation Time Interval – Time-span during which the Emergency Operation is maintained following a fault reaction. The Emergency Operation ends when the safe state is achieved. The time interval shall always be shorter than the EOTTI.
- **EOTTI:** Emergency Operation Tolerance Time Interval – Maximum time-span during which Emergency Operation can be maintained. The time-span is incorporated in the quantitative safety analysis and may therefore be dimensioned by a random HW failure of the system. Depending on the fault analyzed, the EOTTI may also be limited by systematic effects. During the EOTTI, exposition of the system to an unreasonable level of risk shall be ruled out.
- **FDTI:** Fault Detection Time Interval – Time-span from the occurrence of a fault to its detection.
- **FHTI:** Fault Handling Time Interval – Sum of Fault Detection Time Interval and the Fault Reaction Time Interval. The time interval reflects the duration for handling a fault with a concrete Safety Mechanism.
- **FMEA:** Failure Mode and Effects Analysis
- **FRTI:** Fault Reaction Time Interval – Time-span from the detection of a fault to reaching a safe state or to reaching Emergency Operation.
- **FTTI:** Fault Tolerant Time Interval – Time-span during which a fault in the system will not result in a Single-Point Failure of the system.
- **FSR:** Functional Safety Requirement
- **HARA:** Hazard Analysis and Risk Assessment
- **Item:** "System or combination of systems, to which ISO 26262:2018 is applied, that implements a function or part of a function at the vehicle level".
  Note: Later on, "function" is reflected by "a function that can be directly experienced by the customer".
- **LFM:** Latent Fault Metric - Quantitative metric to evaluate whether the risk posed by latent MPFs is adequately covered by the implemented safety mechanisms.
- **MPF:** Multiple-Point Fault - “individual fault that in combination with an [...] independent fault leads to a Multiple-Point Failure”
- **MPFDTI:** Multiple-Point Fault Detection Time Interval – Maximum time-span to detect a Multiple-Point Fault (individual fault of a multiple-point failure) after its occurrence.

- **PMHF:** Probabilistic Metric for Random Hardware Failures: Quantitative metric for evaluating the residual risk of a Safety Goal violation by random hardware failures.
- **RF:** Residual Fault; “Portion of a random hardware fault that by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the random hardware fault is not controlled by a safety mechanism.”
- **SEooC:** Safety Element out of Context; “safety-related element which is not developed in the context of a specific item”
- **Shared Resource:** „The same software, hardware, or system element instance is used by two elements, which are therefore affected by the failure or unavailability of that shared resource.” A system which concurrently performs a function (QM/SR functions) in the context of further functions or safety concepts. In this context, the EBN represents a Shared Resource as it is needed, for example, both for the SR function "Steering" and "Braking" as well as QM functions such as "Interior Light" at the same time.
- **SM:** Safety Mechanism; “Technical solution implemented by E/E functions or Elements, or by other technologies, to detect and mitigate or tolerate faults or control or avoid failures in order to maintain intended functionality or achieve or maintain a safe state.”
- **SPF:** Single-Point Fault - “fault in an Element, that leads directly to the violation of a Safety Goal and no fault of that Element is covered by a Safety Mechanism”
- **SPFM:** Single-Point Fault Metric - Quantitative metric to evaluate if the risk posed by SPFs/RFs is adequately covered by the implemented safety mechanisms.
- **System:** "Set of components or subsystems that relates at least a sensor, a controller and an actuator with one another.
- Note 1: The related sensor or actuator can be included in the system or can be external to the system."

- **General Definitions/Abbreviations**
- **ADS**: Automated Driving System (from UNECE FRAV-09-05). ADS is divided into the following three levels: Level 3, Level 4 and Level 5 – based on the definition in SAE J3016.
- **ADAS:** Advanced Driver Assistance System. ADAS is divided into the following two levels: Level 1, Level 2(+) – based on the definition in SAE J3016. Note: Manual driving is Level 0.
- **AQ:** Active Source (e.g. DCDC converter)
- **ATV:** Active Separating and Connecting Element (switches that separate or connect electrical systems)
- **BNL:** Bordnetzlast - Electrical Load (generic term for loads connected to the electric power supply system, which may refer to both SR-Loads and QM-Loads)
- **Conditions of Use:** Requirements agreement between different Elements of interconnected safety concepts. The requirements agreement contains, inter alia, information and requirements for connecting the Element, for independence from other Elements, for performance requirements of the Element etc. The Conditions of Use are particularly relevant for structuring the EBN safety concept as an Item. (Cf. chapter 5.2.1)
- **DFA:** Dependent Failure Analysis
- **EBN**: Energiebordnetz - Electrical Power Supply System - The Electrical Power Supply System comprises the storage, conversion and distribution of the electricity in the vehicle to the loads (e.g. ECUs, sensors, actuators) and the isolation / separation of faulty Elements from the rest of the EBN. The power interface of the consumers constitutes the limits of the EBN. The loads are therefore not part of the EBN but place certain requirements on the EBN within the scope of the Conditions of Use (e.g. energy, power).
- **EBS:** Electric Brake System
- **EM:** Energy Management
- **Entity:** Abstraction level above the item level (cf. chapter 3.4)
- **EPS:** Electric Power Steering
- **Fail-Active:** Functions / safety concepts that, after occurrence of an initial failure, require continued operation for a limited time to achieve a safe state. Fail-Active functions / safety

concepts are subdivided into Fail-Degraded and Fail-Operational functions /safety concepts.

- **Fail-Degraded:** Functions / safety concepts that, after occurrence of a failure, require continued operation for a limited time with a reduced range of functions to achieve a safe state. The reduction of functions may, for example, be reflected by reduced dynamics, maximum speeds or maximum delays.
- **Fail-Operational:** Functions / safety concepts that, after occurrence of a failure, require continued operation with full functionality to achieve a safe state.
- **Fail-Passive:** Functions / safety concepts that, after occurrence of a failure, close down safely and immediately, without requiring power, thus achieving a safe state. Another term, often used synonymously, is "fail silent".
- **FHTTI:** Fault Handling Tolerance Time Interval – The time interval specifies the maximum permissible time-span for handling a fault. FHTTI is used whenever reference is made to the requirement (as opposed to the actually realized FHTI).
- **FR**: Functional Requirement
- **FSR:** Functional Safety Requirement (corresponds with FSR in ISO 26262-1:2018)
- **LFM_bud:** The value LFM_bud describes a budgeted LFM value for the FSR according to ASIL decomposition and allocation. ISO 26262:2018 only describes the LFM definition for the SG, therefore this new term is introduced.
- **LR**: Legal Requirement, i.e. requirements that arise from laws, licensing regulations, norms or standards
- **Higher-Level Instance:** The Higher-Level Instance is a SW unit of the SR-Vehicle-Function which receives warnings and diagnoses from the different subsystems. It decides on and coordinates the release and possible fault reactions of the product when exercising the SR-Vehicle-Function. This may, for example, entail blocking the SR-Vehicle-Function, displaying a warning or initiating the Minimal Risk Maneuver.
- **MPFHTI:** Multiple-Point Fault Handling Time Interval – Sum of Multiple-Point Fault Detection Time Interval and Multiple-Point Fault Reaction Time Interval. The time interval specifies the maximum time-span of a concrete Safety Mechanism for a reaction to a Multiple-Point Fault (first fault of a multiple-point failure).
- **MPFHTTI:** Multiple-Point Fault Handling Tolerance Time Interval – The time interval specifies the maximum permissible time-span of a Safety Mechanism for a reaction to a Multiple-Point Fault (first fault of a Multiple-Point Failure). The MPFHTTI specifies the maximum time value of the MPFHTI.
- **MPFRTI:** Multiple-Point Fault Reaction Time Interval – Maximum time-span during which a Safety Mechanism shall react to a Multiple-Point Fault (first fault of a Multiple-Point Failure).
- **MRM**: The MRM (Minimal Risk Maneuver) is a procedure automatically performed by the Automated Driving System to place the vehicle in a minimal risk condition in a manner that avoids unreasonable risks in traffic. (From FRAV-09-05)
- **ODD**: Operational Design Domain (from UN ECE FRAV-09-05)
- **PAAT:** Power at All Times, analogous to VDA terminal Kl30
- **PMHF_bud:** The value PMHF_bud describes a budgeted PMHF value for the FSR in line with the ASIL decomposition and allocation. ISO 26262:2018 only describes the PMHF definition for the SG, therefore this new term is introduced.
- **PQ:** Passive Source (e.g. battery)
- **PTV:** Passive separating and connecting Elements (e.g. fuses)
- **EBN Channel:** Electrical power supply channel which feeds Loads. Therefore, none of the connected loads place safety-relevant availability requirements on the power supply of the QM-EBN Channel.
- **QM-Load:** A QM-Load is an electrical consumer that is supplied with power and energy for its functionality but does not place safety-relevant availability requirements on the power supply. An example of a QM-Load is a load that implements a Fail-Passive function or a non SR-Function.
- Note: If QM and SR functions, whose reciprocal freedom from interference is ensured, are allocated to the same load, this will be deemed an SR-Load from an EBN perspective.

- **QM-Function**: Function that places no safety requirements on the availability of the power supply
- **SG:** Safety Goal (corresponds to Safety Goal from ISO 26262:2018)
- **Short Circuit:** A faulty unintended electrical connection between two potentials that are in principle separable/disconnected from each other, which has the potential to violate a Safety Goal or requirement. It is usually accompanied by a violation of the nominal voltage range.
- **SPFM_bud:** The value SPFM_bud describes a budgeted SPFM value for the FSR in line with ASIL decomposition and allocation. ISO 26262:2018 only describes the SPFM definition for the Safety Goal (SG), therefore this new term is introduced.
- **SR-EBN Channel**: Safety-Relevant electrical power supply channel to which at least one SR-Load is allocated which places a safety-relevant availability requirement on the power supply.
- **SR-Vehicle-Function:** Function at the highest level of the safety concept (Entity or Item level, such as the SR vehicle function ADS).
- **SR-Function:** Safety-Relevant Function (subfunction of the SR-Vehicle-Function, such as braking, steering, environment perception etc.), which places a safety requirement on the availability of the power supply.
- Note: Also includes functions with a Fail-Operational requirement, which are implemented via redundancies.
- **SR-Load:** A safety-relevant load is an electrical consumer that implements a subfunction of a Fail-Active SR-Vehicle-Function, such as braking, steering or environment detection. Therefore, the SR-Load allocates a safety-relevant availability requirement to the power supply.
- **SR-Maneuver:** Safety-relevant maneuvers that must be implemented to execute an SR-Vehicle-Function (e.g. evasive maneuver, “Spielstraßenmanöver”, overtaking on rural road etc.), The MRM is also part of the SR-Maneuver which must still be executable in case of a failure.
- **V_terminal**: Supply voltage of a load at its input terminal.

3.2 Nomenclature

3.2.1 Nomenclature of Electric Power Supply Channels

DIN 72552 standardizes the designation of terminals without taking into consideration the safety aspects specified in ISO 26262:2018. To date, a differentiation of terminals 15, 30 and 31 in line with their ability to supply loads - to which SR-Functions and QM-Functions have been allocated - with the intended ASIL integrity is not envisaged. Due to this fact, vehicle-manufacturer specific terminal designations have developed.

The objective of this nomenclature is to standardize the identification of the integrity in respect of the power supply safety in order to increase awareness for the safety relevance of the terminals in the development processes and to standardize their designations.

Therefore, the following supplementary labels are introduced for the purpose of standardizing the terminal designations:

– "_s" (for safe) designates safety-relevant terminals with regard to availability of the power supply. For these terminals, the requirements described in chapter 4.2.2 apply. If several safety-relevant terminals exist, they will be numbered sequentially ("s1", "s2" …, "sN")
– "_q" (for QM) designates terminals with only QM capability to implement (safety-relevant) availability requirements. The QM capability might also be relevant in safety concepts in case of QM(x) decomposition. If several QM terminals exist, they will be numbered sequentially. ("q1", "q2" …, "qN")
– "XX" designates the terminal description according to DIN 72552.

- "Y" is an optional indication of the integrity of a safe terminal, added as a suffix to the ASIL integrity of the safety-relevant availability of the power supply. The stated integrity only refers to the avoidance and/or control of systematic faults.
- "z" designates the functional state of a terminal (e.g. "b" for living, "f" for error status). The functional status "living" refers to a switched-on terminal with a time-limited current feed.

A connection between an "_s" and a "_q" terminal shall only be made via Elements that ensure freedom from interference – cf. chapter 4.2.3.

A combination of designations results in the following generic terminal designations:

- KlXXz_sN_Y
- KlXXz_qN_Y

Alternatively, the following designation is possible for safety-relevant terminals:

- KlXXz_sN_ASIL_Y

In addition, supplementary information for the terminal designation can be added as a suffix, e.g.:

- KlXXz_sN_Y_Postcrash
- KlXXz_sN_ASIL_Y_Sensor1

In practice, the following terminal designations are of particular relevance:

- KlXX_s_Y: single safety-relevant terminal, ASIL-Y capable (e.g. ASIL B)
- KlXX_s1_Y: safety-relevant terminal to supply the first ADS cluster, e.g. ASIL-Y capable (e.g. ASIL B(D))
- KlXX_s2_Y: safety-relevant terminal to supply the second ADS cluster, e.g. ASIL-Y capable (e.g. ASIL B(D))
- KlXX_sn_Y: safety-relevant terminal to supply the n-th ADS cluster, e.g. ASIL-Y capable (e.g. ASIL B(D))
- KlXX_q: single QM terminal (if applicable QM(x))

In the ADS context, the "_s" terminal and the "_s1" terminal will in particular coincide on the same terminal if any ASIL B/C requirements for manual driving are taken into consideration for development of the 30_s1 terminal in order to allow for a scalable electrical power supply concept (cf. scenario B in Annex E). In this case, both designations (terminal Kl30_s as well as terminal Kl30_s1) are permissible and synonymous.

Table 1 contains an exemplary overview of the most important terminals based on DIN 72552 and supplementary designations in accordance with VDA 450. Alternatively, supplementary designations may also be used for safety-relevant terminals when using replacement base code systems, such as PAAT_s for a single safety-relevant terminal.

Example: Terminal Kl30b_s_B or PAATb_s_B designates a terminal fully capable of ASIL B or ASIL B(D) which is switched on upon vehicle wake-up and (as the only terminal in the vehicle) was enabled to implement safety-relevant availability requirements.

Terminal description "XX"	**Additional description**	**DIN 72552**	**Supplement according to VDA 450**
40 – power line directly from 48V battery		40	40_q 40_s 40_s1 … 40_sN

41 – ground line directly from 48V battery		41	41_q 41_s 41_s1 … 41_sN
30 – power line directly from 12 V / 24 V battery	Parking (permanently switched on) This state also includes virtual terminals that can be woken up, e.g. by exceeding a defined current threshold value.	30	30_q 30_s 30_s1 … 30_sN
30f - Terminal Kl30, deactivation in case of weak 12 V / 24 V battery	Parking, can be switched on additionally, in particular in case of a fault, to avoid deep discharge of battery	*Not yet standardized*	30f_q 30f_s 30f_s1 … 30f_sN
30b - Terminal Kl30, switchable	Living. This state also includes virtual terminals that are additionally activated upon vehicle wake-up.	*Not yet standardized*	30b_q 30b_s 30b_s1 … 30b_sN
31 – ground line directly from 12 V / 24 V		31	31_q 31_s 31_s1 … 31_sN
15 – Battery+ from ignition switch (12 V / 24 V)	Preparation for vehicle start, e.g. precharging HV Electrical Power Supply System and release of eDrive	15	15_q 15_s 15_s1 … 15_sN

Tab. 1: Overview of the most important terminals and supplementary designations according to VDA 450

3.2.2 Nomenclature of the Requirements within the Scope of the Recommendation

Within the scope of this document, requirements at different hierarchical levels and their allocation to different safety concepts or standards will be dealt with. To create a structure and provide clarity regarding the requirements, this document uses a nomenclature that entails the allocation of the requirement to its respective origin, the type of requirement and the respective goal. Initially, the allocation of the requirement to the function or an Element of the Electrical Power Supply System will be described. This is followed by the type of requirement and concluded by numbering. The numbering can include several levels. For the allocation and the type of requirement, abbreviations are used that are defined in chapter 3.1.

The allocation can have the following values:

Abbreviation/Acronym	Meaning
ADS	Automated Driving System
AQ	Active Source
ATV	Active Separating and Connecting Elements
BNL	Electrical load
EBN	Electrical Power Supply System
EBN_CU	Conditions of Use of the SR-Loads for the EBN
EBS	Electric Brake System
EM	Energy Management
EPS	Electric Power Steering
PQ	Passive Source
PTV	Passive separating and connecting Elements

The type of requirement can have the following values:

Abbreviation/Acronym	Meaning
FR	Functional Requirement
FSR	Functional Safety Requirement
LR	Regulatory requirement
SG	Safety Goal

The following nomenclature is an example of a Functional Safety Requirement for an Active Source with a second numbering level: AQ-FSR 1.2

3.2.3 Nomenclature of Associated Safety Concepts

To develop the Electrical Power Supply System compliant with ISO 26262:2018, the Electrical Power Supply System shall be classified according to the terminology of the standard (e.g. Item, System, Subsystem, Element).

According to ISO 26262-1:2018, 3.84, an item is a system that implements a vehicle function or subfunction. For the Electrical Power Supply System, there are two possible conceptional approaches:

1. Classification of the SR-Vehicle-Function ADS as an Entity, with the EBN being considered a separate Item.
2. Classification of the SR-Vehicle-Function ADS as an Item, with the EBN being considered a Subsystem.

Comment: A comparative illustration of the classification of the SR-Vehicle-Function ADS as Entity as opposed to the classification of the SR-Vehicle-Function ADS as Item is presented in chapter 5.2.

According to classification 1., the EBN is considered an Item, cf. chapter 5.2.1. The Electrical Power Supply System provides the necessary power and energy for numerous vehicle functions. Functionally, it thus becomes a part of this vehicle function. To correctly capture the interaction between the Electrical Power Supply System and the vehicle functions, the **Entity Concept** (source: Gebauer, Carsten, Safetronic 2019) is introduced. The designation "Entity" is used to represent a level of abstraction which is higher than the Item level and presents the basis for the safety concepts of the subordinate items thus derived. Within the scope of the Entity design and development, the interaction of several Items and/or Entities and their safety concepts is coordinated. An Entity can consist of one or more Items and/or one or more Entities. Figure 1 illustrates a possible breakdown of an Entity, using the example of "Automated Driving".

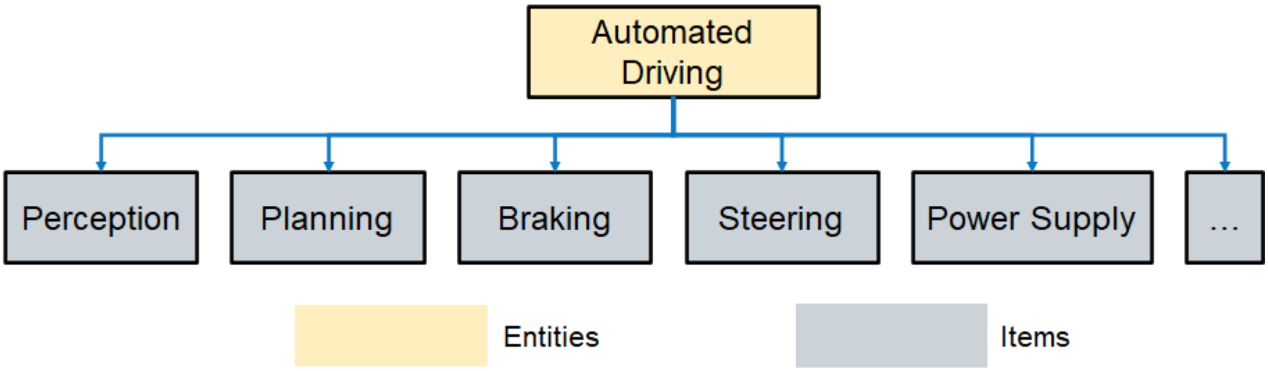


Fig. 1: Possible breakdown of an Entity using the example of the SR-Vehicle-Function ADS

In this case, the Entity "Automated Driving" represents the highest level of functional integration. In the example above, it comprises the functional components Perception, Planning, Drive, Braking, Steering and Power Supply. In turn, these functional components can then be defined as Entity or Item. A definition as Entity is useful if a subfunction can be broken down into further functional components to which the definition of Item according to ISO 26262:2018 can be applied. Figure 1 shows an exemplary application of the Entity concept where only the top level of the functional integration is defined as an Entity, without any restriction of the generality.

While use of the term Entity is not compulsory, it lends itself to structuring safety concepts, especially in relationship to the organizational structure of the respective company.

Qualitative interactions:

As a matter of principle, a safety concept shall be created at the level of the SR-Vehicle-Function (in this case Entity level) since as little as one malfunction of the SR-Vehicle-Function can result in a risk for humans and the environment. This serves to ensure the correct implementation of the required Safety-Relevant Function. For this purpose, the provisions of ISO 26262-3:2018, 7 in terms of the creation of functional safety concepts shall be complied with. As part of the functional safety concept, the chains of effects leading to the loss of the SR-Vehicle-Function shall be identified and measures defined to safeguard the chains of effects. In doing so, the chains of effects shall be considered across Items. Likewise, within the scope of the safety concept verification criteria will be defined which ensure a correct implementation and review of the underlying boundary conditions. Based on the safety concept, the requirements will then be allocated to the lower levels or – via the Conditions of Use – between the Elements of the individual levels.

Conditions of Use:

The subdivision of an Entity into functional components requires additional information called Conditions of Use. They contain information on the functional interdependencies of Entities, Items and

Systems and on the requirements they place on each other. Using the example of the electrical power supply, the dependencies of the Entities and Items in connection with the item EBN shall be specified. This includes information on the integrity level required to ensure a sufficient supply of power, including which and how many interfaces shall be supplied. To ensure a sufficient supply of power, time-dependent thresholds for undervoltage and overvoltage and the necessary power requirements shall be defined by the requesting Entities and Items. This additional information ensures, inter alia, that potential requirement decompositions of the affected Items correspond to potential requirement decompositions within the Item "Power Supply". The specified Conditions of Use shall be validated within the scope of the safety case. One example in case are the defined voltage/time limits of a safety-relevant consumer, which are allocated to the EBN via the Conditions of Use and demonstrated by means of component tests of the safety-relevant consumer.

Note: A counterexample to be avoided would be the decomposition of an ASIL D braking function regarding availability to an ASIL C(D) braking function and an ASIL A(D) braking function, while the requirement of an ASIL D power supply regarding availability on two electrical power supply channels, each one with an ASIL B(D) power supply, was decomposed to the two terminals (terminal Kl30_s1 and Kl30_s2). Consequently, the decomposed ASIL C(D) braking function on terminal Kl30_s1 (ASIL B(D)) cannot be supplied adequately.

Quantitative interactions in the Entity concept:

The basic idea behind the Entity concept is to transfer state-of-the-art systems to the context of the SR-Vehicle-Function ADS. Existing braking systems, for example, that are currently still integrated in the context of manual driving, can be used in the Entity concept as subsystems to implement the SR-Vehicle-Function ADS. Analogous to ISO 26262-5:2018, 8.2 & 9.4.2.2, the quantitative proof (PMHF, SPFM, LFM) in the Entity concept shall be performed at Item level. Quantitative proof at Entity level is not required but can be performed if proof at Item level is not expedient. For this purpose, the procedure defined in ISO 26262-5:2018, Annex F, may be consulted to identify design weaknesses and remedy them. Furthermore, this approach takes into consideration the increasing complexity of vehicle functions, such as the SR-Vehicle-Function ADS. The Entity concept and its components are not restricted to just one vehicle. As a result, the Entity concept makes it possible to develop and describe safety concepts for cross-vehicle SR functions, e.g. Platooning or Vehicle2X.

4. Regulatory Framework and Principles for the EBN

Chapter 4 explains the requirements of the SR-Vehicle-Functions arising from functional safety (ISO 26262:2018) and the different currently applicable technical rules, regulations and standards. Furthermore, basic assumptions for the interpretation of ISO 26262:2018 are introduced and their relevance for the EBN is described in more detail. This provides the basis for deriving the requirements for EBN components in chapter 5.

4.1 Requirements for the EBN in the Context of Automated Driving

The requirements for the Electrical Power Supply System are composed of requirements resulting from functional safety (cf. chapter 4.1.1), technical rules, regulations and standards (cf. chapter 4.1.2) and the performance requirements of the SR functions (chapter 4.1.3). The requirements resulting from these sources of requirements will be examined below.

4.1.1 Safety Requirements of the SR-Vehicle-Function ADS

The Safety Goals are derived from the Hazard Analysis & Risk Assessment (HARA) defined in ISO 26262:2018. To be able to recommend an interpretation of the Electrical Power Supply System within the scope of ISO 26262:2018, examples of assumed Safety Goals for the SR-Vehicle-Function ADS will be provided.

Note: This recommendation does not aim to standardize the HARA of the SR-Vehicle-Function ADS. The Safety Goals are simply intended to serve as a generic starting point to derive the EBN requirements.

Assumed Safety Goal	ASIL	FTTI	Safe State
Avoidance of excessive / unwanted lateral deviations from the desired trajectory (lateral vehicle guidance)	D	Dependent on functionality (e.g. 80 ms)	Vehicle transitioned to minimal risk status (e.g. immobilization of the vehicle at the edge of the road or handover of the vehicle to the driver completed)
Avoidance of insufficient vehicle deceleration (longitudinal deceleration)	D	Dependent on functionality (e.g. 200 ms)	Vehicle transitioned to minimal risk status (e.g. immobilization of the vehicle at the edge of the road or handover of the vehicle to the driver completed)

Based on the aforementioned Safety Goals of the SR-Vehicle-Function ADS and for the purposes of simplification, the generic Safety Goal ADS-SG1 is defined as follows for subsequent chapters:

- ADS-SG 1: "Avoid faulty ADS vehicle function" with ASIL D

Based on the Safety Goal ADS-SG 1, the EBN safety requirements are derived in chapter 5.2 and chapter 5.3.

4.1.2 Aggregated Requirements of SR-Vehicle-Functions derived from technical Rules, Regulations and Standards – Aggregation from the Annex

In addition to the requirements resulting from a safety concept of the SR-Vehicle-Functions, there are also legal and normative requirements. These requirements dimension the functional safety requirements resulting from safety concepts, e.g. in terms of redundancy (requirement of independent power supply) or performance (legal requirements for minimum deceleration, steering forces etc.). Below is an aggregated overview of the requirements contained in well-known standards and laws. In particular SR-Vehicle-Functions relevant for manual driving have a large number of EBN-relevant requirements. These are usually also relevant and applicable to the SR-Vehicle-Function ADS and take into consideration, in particular, requirements of automated vehicle functions, steering and braking systems and light functions. For the source of the respective aggregated requirement, please refer to the respective designation LR (legal requirement) in Annex A1-A4.

EBN-FR 1	The EBN shall monitor its status and communicate the latter to Higher-Level Instances/SR-Functions and/or the driver.
Aggregated from	EPS-LR 11, EPS-LR 16, EPS-LR 17, EPS-LR 18, EPS-LR 19, EPS-LR 20 EBS-LR 10, EBS-LR 11, EBS-LR 12, EBS-LR 13, EBS-LR 14 ADS-LR 1, ADS-LR 2, ADS-LR 4

EBN-FR 2	The EBN shall provide at least two completely independent energy storage devices and transmission channels to supply the SR-Function Brake. Note: This requirement applies to all forms of energy (pneumatic, electric, mechanic) due to the control unit needed in the absence of a driver as the controlling instance.
Aggregated from	EBS-LR 1

EBN-FR 3	For the interpretation/dimensioning of the EBN, specific maneuvers of the steering and braking functions shall be taken into consideration. In doing so, an overlap of different functions such as steering, braking, light, visibility and drive functions shall also be factored in.
Aggregated from	EPS-LR 2, EPS-LR 3 EBS-LR 2, EBS-LR 3, EBS-LR 5

EBN-FR 4	From a legal perspective, a prioritization of the SR-Vehicle-Functions Steering and Braking or the systems Steering and Braking in the context of the SR-Vehicle-Function ADS is only permissible if the EBN is subject to restrictions. Steering has priority over braking.
Aggregated from	EPS-LR 4, EPS-LR 9

EBN-FR 5	The drive of the Active Source for supplying the SR-Function Brake shall be designed as safely as possible. Note 1: VDA interpretation: Common development rules and regulations, e.g. ISO 26262:2018, must be applied. Note 2: The phrase "drive of the Active Source" refers to the provision of the power required for the Active Source, e.g. the combustion engine. Note 3: The VDA 450 interpretation also refers to power being supplied from higher voltage levels and energy converters.
Aggregated from	EBS-LR 15

EBN-FR 6	The design of the EBN shall ensure that faulty SR or QM-Functions do not result in a loss of the SR function Steering (also in the context of the SR-Vehicle-Function ADS).
Aggregated from	EPS-LR 1, EPS-LR 7

EBN-FR 7	When designing and developing the power supply for SR-Loads, ISO 26262:2018 shall be taken into consideration.
Aggregated from	EPS-LR 24

4.1.3 Performance Requirements of the SR Function for the EBN

The EBN is a system whose purpose in a safety concept is to provide the loads to which SR functions have been allocated with sufficient power and energy. The EBN must be implemented in a way that ensures that SR-Maneuvers can be started, executed and completed even in case of a fault. The MRM is also part of the SR-Maneuver. When carrying out SR-Maneuvers, non-SR-Maneuvers can be degraded or inhibited by the Higher-Level Instance.

Each load to which an SR-Function is allocated is essential for a safe functional operation within the safety concept of the SR-Vehicle-Function. Derived from specific maneuvers that are defined in the regulations or the safety concept, each load implies a set of generic performance requirements. These performance requirements are composed of peak power with the respective pulse duration and energy requirements during the entire maneuver. It should be noted that the performance requirements of all loads in the EBN may overlap. Accordingly, the interference described in chapters 4.2.3 and Annex B shall be taken into consideration.

The specific performance requirements of a load depend strongly on the technical design of the vehicle and can therefore not be standardized. However, the acceptance criteria whether power supplied by the EBN is sufficient to fulfill a function are already subject to technical standards and will, in this case, be standardized within the context of the safety concepts compliant with ISO 26262:2018.
The acceptance criteria for the respective performance requirements are defined by the terminal voltage at the respective SR-Load. Dependent on the power and pulse duration, a deviation from the defined voltage range may result in functional restrictions, loss of function (e.g. through a reset of control units, cf. description in Annex F) or malfunctions. The voltage classes reflect the minimum requirement from the perspective of functional safety in the SR-Vehicle-Function operation. These may be implemented on the basis of ISO 16750 or ISO 21780, cf. Annex G. Degradations of the components or interventions by the Energy Management system (cf. chapter 6) must be made within the nominal voltage range. The subsequently listed V_terminal refers to the input voltage of the SR-Load. Tolerances in the voltage measurement and voltage drops in the EBN must be taken into consideration when designing safety mechanisms.

EBN_CU-FSR 1 (12 V systems)	During automated driving, the electrical power supply shall provide the necessary power and energy to the input terminals of the loads to perform the SR-Maneuver and MRM in the voltage range 9-16 V (voltage range OEM-specific).
Time interval	**Scenario 1 "FTTI based on current EBN designs":** - Undervoltage range: • 4.5 V ≤ V_terminal < 9 V*: 100 ms • V_terminal < 4.5 V: 100 µs to 500 µs (OEM-specific) - Overvoltage range: • 16 V < V_terminal ≤ 18 V: 100 ms • 18 V < V_terminal < V_LoadDump**: 10 ms • V_LoadDump ≤ V_terminal: 0 ms Assumption: current status, for example vehicle with lead acid batteries, starter generators and fuses *: based on the design of the SR function and the technical solution the required value may differ **: Load Dump = 27 V…35 V (OEM-specific)

	Scenario 2 "FTTI based on future EBN designs": - Undervoltage range: • 6.5 V ≤ V_terminal < 9 V*: 100 ms • V_terminal < 6.5 V: 100 µs to 500 µs (OEM-specific) Assumption: future use of new passive or Active Sources (e.g. Lithium-Ion batteries), ATVs instead of fuses or EBN channels without a storage device - Overvoltage range: • 16 V < V_terminal ≤ 18 V: 100ms • 18 V < V_terminal < 24 V**: 10 ms • 24 V ≤ V_terminal: 0 ms Assumption: future use of new energy sources (passive or active) and absence of starter generators. Safety mechanisms to adhere to the upper voltage limit must be provided for, e.g. provision for energy absorption by Passive Sources for regenerative power supply of the consumer and/or shut-off mechanisms for Active Sources in case of faults. *: based on the design of the SR function and the technical solution the required value may differ **: Max. voltage in the EBN limited by Active Source, energy storages in Passive Sources or protective mechanisms in the components.
Safe state of the Element	Dependent on the higher-level Safety Goal / level of automation: transfer of the driving function to the driver / return to safe state (cf. chapter 4.2.3.1)
Integrity	ASIL C-D (dependent on the SR-Vehicle-Function, the associated HARA and the associated safety concept) In case of ASIL decomposition: e.g. ASIL B(D)+ASIL B(D)
Mode	Automated driving
Applicability to variants	All EBN variants
Derived from	ADS_SG 1 in due consideration of the Conditions of Use for the SR-Loads
Comment	When deviating from the voltage/time intervals at the input terminal of an SR-Load, the function of the SR-Load can no longer be implemented (due to insufficient power). Consequently, an adequate fulfillment of the associated Safety Goal is no longer possible.

EBN_CU-FSR 1 (24 V systems)	The electrical power supply shall provide the necessary energy and power to the input terminals of the loads to carry out the SR-Maneuver and MRM in the voltage range 18.5-32 V (if applicable OEM specific) during automated driving.
Time interval	**Scenario 1 "FTTI based on current EBN designs":** – Undervoltage range: • 9 V ≤ V_terminal < 18.5 V*: 100 ms • 6 V ≤ V_terminal < 9 V: 50 ms

	• V_terminal < 6 V: 100 µs to 500 µs (OEM-specific) – Overvoltage range: • 32 V < V_terminal ≤ 36 V: 380 ms • 36 V < V_terminal < V_LoadDump**: 100 ms • V_LoadDump ≤ V_terminal: 0 ms Assumption: current status, e.g. vehicles with lead acid batteries, starter generators and fuses *: based on the design of the SR function and the technical solution the required value may differ **: Load Dump = 55 V…60 V (OEM-specific) **Scenario 2 "Based on future EBN designs":** – Undervoltage range: • 12 V ≤ V_terminal < 18.5 V*: 100 ms • V_terminal < 12 V: 100 µs to 500 µs (OEM-specific) Assumption: future use of new passive or Active Sources (e.g. Lithium-Ion batteries), ATVs instead of fuses or EBN channels without storage device – Overvoltage range: • 32 V < V_terminal ≤ 36 V: 100 ms • 36 V < V_terminal < 48 V**: 10 ms • 48 V ≤ V_terminal: 0 ms Assumption: future use of new energy sources (passive or active) and absence of starter generators. Safety mechanisms to adhere to the upper voltage limit must be provided for, e.g. provision for energy absorption by Passive Sources for regenerative power supply of the consumer and/or shut-off mechanisms for Active Sources in case of faults. *: based on the design of the SR function and the technical solution the required value may differ **: Max. voltage in the EBN limited by Active Source, energy reserve in Passive Sources or protective mechanisms in the components.
Safe state of the Element	Dependent on the higher-level Safety Goal / level of automation: transfer of the driving function to the driver / return to the safe state (cf. chapter 4.2.3.1)
Integrity	ASIL C-D (dependent on the SR-Vehicle-Function, the associated HARA and the associated (EBN) safety concept) In case of ASIL decomposition: e.g. ASIL B(D)+ASIL B(D)
Mode	Automated driving
Applicability to variants	All EBN variants
Derived from	ADS-SG1 in due consideration of the Conditions of Use for the SR-Loads
Comment	When deviating from the voltage/time intervals at the input terminal of an SR-Load, the function of the SR-Load can no longer be implemented

	(due to insufficient power). Consequently, an adequate fulfillment of the associated Safety Goal is no longer possible.

EBN_CU-FSR 1 (48 V systems)	The electrical power supply shall provide the necessary energy and power to the input terminals of the loads to carry out the SR-Maneuver and MRM in the voltage range 36-52 V (if applicable OEM specific) during automated driving.
Time interval	As 48 V systems are not yet common for SR-Loads, this is only a representation of a scenario for FTTI of future EBN designs in line with ISO 21780:2020. – Undervoltage range: • 31 V ≤ V_terminal < 36 V: 2 s • V_terminal < 31 V: 100 µs – Overvoltage range: • 52 V < V_terminal ≤ 54 V: 120 s • 54 V < V_terminal ≤ 58 V*: 640 ms • 58 V < V_terminal < 70 V*: 40 ms • 70 V ≤ V_terminal: 0 ms *: Max. voltage in the EBN limited by Active Source, energy reserve in Passive Sources or protective mechanisms in the components.
Safe state of the Element	Dependent on the higher-level Safety Goal / level of automation: transfer of the driving function to the driver / return to the safe state (cf. chapter (cf. chapter 4.2.3.1)
Integrity	ASIL C-D (dependent on the SR-Vehicle-Function, the associated HARA and the associated (EBN) safety concept) In case of ASIL decomposition: e.g. ASIL B(D)+ASIL B(D)
Mode	Automated driving
Applicability to variants	All EBN variants
Derived from	ADS-SG1 in due consideration of the Conditions of Use of the SR-Loads.
Comment	When deviating from the voltage/time intervals at the input terminal of an SR-Load, the function of the SR-Load can no longer be implemented (due to insufficient power). Consequently, an adequate fulfillment of the associated Safety Goal is no longer possible.

4.2 Specifics of the Application of ISO 26262:2018

When applying ISO 26262:2018 to the EBN as opposed to the SR-Vehicle-Functions, several specifics need to be considered. These specifics will be explained in more detail in this chapter. The specifics result from the fact that the EBN can present a Shared Resource for several SR-Functions and must be designed as a Fail-Active safety concept, which in itself must also ensure a certain level of intrinsic protection. To prevent a different interpretation of ISO 26262:2018 in the course of its concrete application, the following specific issues in the application of ISO 26262:2018 within the context of EBN will be described in more detail:

- Timing requirements (chapter 4.2.1)
- Independence during application of the ASIL decomposition (chapter 4.2.2)
- Freedom from interference (chapter 4.2.3)
- Emergency Operation (chapter 4.2.4)

Using the example of the SR-Vehicle-Function ADS, the requirement for the EBN to provide power to the safety-relevant loads with ASIL D integrity ensues from chapter 4.1.1. Chapter 4.1.2. reveals the need for redundant EBN channels due to technical rules, regulations and standards (cf. inter alia to EBN-FR2).

4.2.1 Timing Requirements

The terms Fault Tolerant Time Interval (FTTI), Fault Handling Time Interval (FHTI) and Multiple-Point Fault Detection Time Interval (MPFDTI) are clearly defined in ISO 26262:2018. However, these terms might be confused if the power supply for an SR-Vehicle-Function is implemented by at least two independent power supply channels. In terms of time, different time intervals are relevant depending on the fault.

For the reaction to a SPF, the fault diagnosis and the fault reaction must be completed within the Fault Handling Tolerance Time Intervals (FHTTI). This comprises the Fault Detection Time Interval (FDTI) and the Fault Reaction Time Interval (FRTI).

In case of Multiple-Point Faults, the Multiple-Point Fault Detection Time Interval (MPFDTI) is crucial. In the process, the MPFDTI may exceed the FTTI in terms of time. A fault reaction time for MPF is not explicitly defined in ISO 26262:2018. However, in general the handling of faults (fault detection and fault reaction) must be completed within the Emergency Operation Tolerance Time Intervals (EOTTI) (cf. chapter 4.2.4) to keep the risk of a subsequent Dual-Point Failure at an acceptable level.

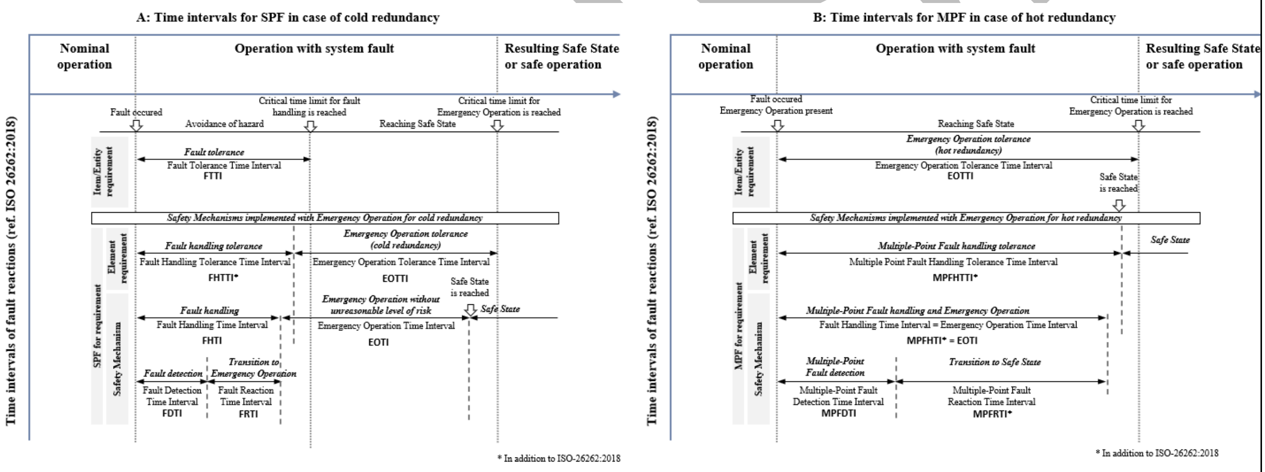

A: Time intervals for SPF in case of cold redundancy
Nominal operation
Operation with system fault
Resulting Safe State or safe operation
Time intervals of fault reactions (ref. ISO 26262:2018)
Fault occured
Critical time limit for fault handling is reached
Critical time limit for Emergency Operation is reached
Avoidance of hazard
Reaching Safe State
Item/Entity requirement
Fault tolerance
Fault Tolerance Time Interval
FTTI
Safety Mechanisms implemented with Emergency Operation for cold redundancy
SPF for requirement
Element requirement
Fault handling tolerance
Fault Handling Tolerance Time Interval
FHTTI*
Emergency Operation tolerance (cold redundancy)
Emergency Operation Tolerance Time Interval
EOTTI
Safe State is reached
Safe State
Safety Mechanism
Fault handling
Fault Handling Time Interval
FHTI
Emergency Operation without unreasonable level of risk
Emergency Operation Time Interval
EOTI
Fault detection
Transition to Emergency Operation
Fault Detection Time Interval
FDTI
Fault Reaction Time Interval
FRTI
* In addition to ISO-26262:2018
B: Time intervals for MPF in case of hot redundancy
Nominal operation
Operation with system fault
Resulting Safe State or safe operation
Time intervals of fault reactions (ref. ISO 26262:2018)
Fault occured Emergency Operation present
Critical time limit for Emergency Operation is reached
Reaching Safe State
Item/Entity requirement
Emergency Operation tolerance (hot redundancy)
Emergency Operation Tolerance Time Interval
EOTTI
Safe State is reached
Safety Mechanisms implemented with Emergency Operation for hot redundancy
MPF for requirement
Element requirement
Multiple-Point Fault handling tolerance
Multiple Point Fault Handling Tolerance Time Interval
MPFHTTI*
Safe State
Safety Mechanism
Multiple-Point Fault handling and Emergency Operation
Fault Handling Time Interval = Emergency Operation Time Interval
MPFHTI* = EOTI
Multiple-Point Fault detection
Transition to Safe State
Multiple-Point Fault Detection Time Interval
MPFDTI
Multiple-Point Fault Reaction Time Interval
MPFRTI*
* In addition to ISO-26262:2018

Fig. 2: Temporal correlations for fault reactions

4.2.1.1 Timing Requirements (FTTI, FHTI and FHTTI)

The FTTI is the time-span during which a fault may occur without a resulting failure of an SR-Vehicle-Function. It is defined at Item or Entity level, thus providing the temporal framework for the safety mechanisms to avoid Single-Point Failures. Exceeding this Fault Tolerant Time Interval may therefore result in a violation of the Safety Goal of the SR-Vehicle-Function.

Thus, the FTTI constitutes the highest temporal requirement and is always linked to the voltage/time intervals of the control units realizing the SR-Vehicle-Function. In case of an undervoltage or overvoltage that leads to non-availability of the SR-Vehicle-Function for a time-span that is longer than the accepted range, this constitutes a violation of the Safety Goal of the SR-Vehicle-Function. In addition to the voltage/time intervals, the respective HARA is relevant, which analyses how long non-availability of the affected control unit remains uncritical.

If the EBN is applied as an Item in the context of an Entity as described in chapter 3.4, there will be a Safety Goal both at Entity level and at Item level. To achieve the FTTI of the higher-level SG, it may be necessary to allocate to the subordinate SG an FTTI that deviates from that of the higher-level SG. ISO 26262:2018 contains no such distinction. In the context of the publication, a distinction is therefore made between the FTTI at Item level and the FTTI at Entity level.

The FTTI at Item level must always be derived within the respective context, based on chains of effects that result in the violation of the FTTI at Entity level. This analysis must, inter alia, give due consideration to the "Conditions of Use" described in chapter 3.4. If applicable, it may be necessary to also implement the procedure described here at deeper abstraction levels of the requirements derivation.

The FHTTI is a generic timeframe for safety mechanisms and is less than or equal to the FTTI. The following exceptions may occur in the specific application for the purpose of a derivation within a safety concept:

- Within a safety concept, several FHTTI can be defined. The crucial issue is the specific fault pattern and the technical implementation of the safety mechanisms.
- The FHTTI can be a timeframe for just one Safety Mechanism and thus be equal to the FHTI.
- Exceptions for avoidance strategies of SPF: Using preventive safety mechanisms (fault predictions such as diagnoses of the battery performance or diagnosis of early fault indicators, e.g. by means of the voltage level), an SPF can be prevented. The prevention of faults, just like a fault reaction, is subject to a timing requirement which is dependent on the time horizon of the early detection or prediction. To avoid introducing further time intervals, it is advisable to continue using the FHTTI as a timing requirement. In these cases, the FHTTI is expanded, for specific Safety Mechanisms, by the time horizon of early detection or prediction and may thus become greater than the FTTI. An increase of the FHTTI will only ever be effective before the hypothetical occurrence of a fault.

In contrast to the FHTTI, the FHTI is always allocated to a concrete Safety Mechanism and must always be less than or equal to the generic FHTTI.

The FHTI is the sum of the Fault Detection Time Interval (FDTI) and the Fault Reaction Time Interval (FRTI).

When deriving requirements for the level below, the FTTI of the SG at Item level is converted to the FHTTI of the sub-requirement of the level below, based on ISO 26262-1:2018, 3.61 Note 6. The FHTTI covers the maximum Fault Handling Tolerance Time Interval in the left part of the V-model – with a focus on the requirements specification -, while the FHTI describes the actual Fault Handling Time Interval of an implemented Safety Mechanism in the right part of the V-model.

In accordance with the case study in Annex D and the requirements described in chapter 4.1.2., arising from technical rules, regulations and standards, it is advisable to implement the EBN for the SR-Vehicle-Function ADS by means of independent EBN channels. The implementation of at least two sufficiently independent terminals for the electrical power supply (terminal Kl30_s1 and Kl30_s2) and the consistent avoidance of dependent failures reduces single-point faults and residual faults to a minimum. As mentioned in chapter 4.2.3.1, due consideration must be given to the fact that in case of a conversion of single-point faults to multiple-point faults by means of decomposition, the term FHTTI will still be referred to in each decomposed EBN channel due to the requirements regarding decomposition according to ISO 26262:2018:

If the safety requirements are derived via decomposition, all safety-relevant sub-requirements inherit the FHTTI in a manner that ensures that the higher-level requirement is met independently by all decomposed sub-requirements, cf. ISO 26262-9:2018, 5.4.4. This means that all safety mechanisms required to implement the decomposed ASIL integrity must be developed in line with the FHTTI of the higher-level requirement. To ensure the adherence to the FHTTI, a proof is required that the FHTI of the implemented Safety Mechanism is not greater than the specified time budget (FHTI <= FHTTI).

Note: Depending on the requirement level, the FHTTI and the FHTI may be budgeted from time intervals of the higher-level requirement level.

In summary, all faults with the potential to violate a defined safety requirement must be avoided by means of an appropriate ASIL within the FHTTI and/or controlled by means of a suitable Safety Mechanism.

4.2.1.2 Timing Requirements (MPFDTI, MPFHTTI)

As many of the EBN's safety mechanisms detect the first fault of a multiple-point failure and react to it, it is advisable to define the Multiple-Point Fault Handling Tolerance Time Interval (MPFHTTI) as a supplement to ISO 26262:2018.
The MPFHTTI constitutes a generic timeframe for safety mechanisms to handle the MPF and must always be less than or equal to the sum of FTTI and EOTTI.
In contrast to the MPFHTTI, the MPFHTI is always allocated to a concrete Safety Mechanism and must always be less than or equal to the generic MPFHTTI.
The MPFHTI is composed of the Multiple-Point Fault Detection Time Interval (MPFDTI) and the Multiple-Point Fault Reaction Time Interval (MPFRTI), cf. Figure 2.
The advantage of this MPFHTTI is that the time label and the corresponding time-related classification make it possible to directly identify whether the failure of a respective Safety Mechanism will result directly in a violation of a top-level safety requirement or a decomposed TOP level safety requirement or whether further faults must occur first.
The MPFHTTI - instead of the FHTTI - must be stated in the respective technical safety requirements for the specific allocated safety mechanisms in the respective Elements and be identified as such.

A common procedure for the design of EBN safety concepts is the use of ISO 26262-4:2018, 6.4.2.5 according to which the SM for the detection of latent MPFs can be implemented with a reduced ASIL. These SM are not tied to the timeframes of the FTTI or the FHTTI. The described latent fault diagnosis is used to detect the MPF which requires adherence to the MPFHTTI during fault handling. However, the implementation of these diagnoses with reduced ASIL integrity within the MPFHTTI is only valid if faults with the potential to directly violate the SG or the derived safety requirement (e.g. of the EBN channel) are already avoided by means of a corresponding ASIL within the FTTI or the FHTTI and/or controlled by means of a suitable Safety Mechanism.

Note: If a potential single-point failure was converted into a multiple-point failure due to a decomposition, each decomposed subfunction must inherit the original timing requirement of the FTTI. Accordingly, every decomposed channel (terminals Kl30_s1 and Kl30_s2) is subject to the timing requirements of the overall system EBN. The FHTTI of the EBN is allocated to the individual EBN channels without any changes. In these cases, the term FHTTI is still used even if, strictly speaking, a corresponding Safety Mechanism addresses an MPF. This serves to emphasize that exceeding the time limit of a requirement has massive effects on the system integrity and thus indicates a serious system failure.

When defining the MPFHTTI top-down for specific functions at the level of technical safety concepts, the following aspects must therefore be taken into consideration:

- EOTTI in case of a fault
- composed of failure rates of the fault-specific defective system and a faultless system and the planned operating time
- FTTI predetermined by the SR-Vehicle-Function
- the order (number of errors in the error chain until the SG is violated) of the MPF.
- expected frequency of individual faults.

4.2.2 Independence in Case of Applying an ASIL Decomposition

Redundancy in the EBN is used to meet the requirements of the technical rules and regulations (e.g. EBN-FA2), while at the same time reducing the requirements for the systematic design and development process by means of decomposition in the individual EBN channels (terminal Kl30_s1 and Kl30_s2). Concomitantly with the decomposition, requirements arise in terms of sufficient independence between the decomposed Elements. For an ISO 26262:2018 compliant decomposition between the electrical power supply channels (e.g. terminal Kl30_s1 and terminal Kl30_s2) or within an electrical power supply channel (e.g. terminal Kl30_s), the following conditions must be met:

- The higher-level Safety Requirement is decomposed into redundant safety requirements (ISO 26262-9:2018, 5.1)
- The decomposed safety requirements are implemented by means of sufficiently independent design Elements (ISO 26262-9:2018, 5.1)
- Dependent failures must be avoided in accordance with the initial ASIL (ISO 26262-9:2018, 5.4.3)
- The decomposition is performed in accordance with a valid decomposition scheme (ISO 26262-9:2018, 5.1)
- Each decomposed requirement must implement the initial requirement completely and independently. This includes, in particular, also the allocation of the Fault Tolerance Time Intervals (FTTI) and the Fault Handling Tolerance Time Intervals (FHTTI) (cf. chapter 4.2.1; ISO 26262-9:2018, 5.4.4)

To avoid dependent failures (ISO 26262-1:2018, 3.29), freedom from interference for coexisting Elements must be ensured to avoid cascading failures (ISO 26262-1:2018, 3.17) as well as Common Cause Failures (ISO 26262-1:2018, 3.18). That means that the implementation of sufficient independence requires the avoidance and/or control of both cascading failures as well as Common Cause Failures with the initial ASIL.

To achieve sufficient independence between systems and/or Elements that implement a higher-level requirement within the scope of an ASIL decomposition independently and autonomously, the following faults must be avoided:

- Cascading Failure: failure of both subsystems or subelements due to a fault that propagates from one subsystem and/or subelement to another subsystem and/or subelement (e.g. discharge of both Passive Sources in terminals Kl30_s1 and Kl30_s2 due to an excessive power consumption of a consumer)
- Common Cause failure: failure of both subsystems and/or subElements due to a common cause (due to common cause initiators such as humidity or EMC)

The proof of sufficient independence required for decomposition will be provided by means of a Dependent Failure Analysis (DFA).

The relevance of ensuring sufficient independence within the EBN arises from the decomposition, as described in ISO 26262-9:2018, 5.1. Safety concepts of the EBN often have two use cases that will be described in more detail here:

- Proof of independence between decomposed EBN channels
- Proof of independence between decomposed sources within an EBN channel

In this case, the independence requirement relates to technical independence (arising from the technical concept), not organizational independence, cf. ISO 26262-9:2018, 5.1 Note. To ensure technical independence either the absence of dependent failures or the implementation of suitable measures for handling dependent failures are proven by a DFA. If measures are required for handling the dependent failures, they must be implemented with a sufficient ASIL. Measures for remedying faults may be of a technical or process nature. Depending on the measures taken, an indirect independence requirement for the measures regarding organizational structures may result.

Note 1: The ASIL decomposition is used to reduce the procedural requirements for the systematic design and development process of the decomposed Elements, if requirements are implemented by several, independent Elements.
Note 2: In case of a derivation of requirements for the EBN, due consideration must be given to the fact that some individual faults may result in the direct loss of an SR function. A decomposition into two EBN channels does not change the integrity requirement for controlling these dependent failures (e.g. common cause or cascading). One example in case is an overvoltage at the steering component of an EBN channel, which causes the steering to lock. The following specifications serve as remedial action:

- Systematically avoid fault(s) with the initial ASIL D
- Adhere to the specifications regarding random hardware failure as described in ISO 26262-5:2018, 9.4.1.2 and 9.4.1.3:
    - SPF/RF of a HW Element < 0.01 FIT or
    - SPF/RF of the HW Element is handled by the SM with a DC of at least 90% (the overall PMHF must still be met) or
    - The avoidance of faults is argued via dedicated measures

4.2.2.1 Independence between EBN Channels

The independent EBN channels (e.g. terminal Kl30_s1 and terminal Kl30_s2) are used to decompose the ASIL D requirement for the power supply and to achieve the hardware metrics demanded by ISO 26262:2018. The ISO 26262:2018 metric targets relevant to the electrical power supply must be derived in accordance with the procedure as described in Annex E. In doing so, a distinction must be made as to whether the Electrical EBN is treated as an Item or a Subsystem, cf. chapter 5.1. To avoid dependent failures, both the freedom from interference for coexisting Elements and the avoidance of Common Cause Failure must be ensured. One example of a dependent failure is the failure of the HV system or the 12 V generator, which leads to a discharge of both 12 V batteries; cf. case study in Annex D.

Example: When using at least two independent, redundant EBN channels, the redundancy can be used for decomposition to avoid systematic failures. This results in the following reduced requirements:

- Due to the redundancy, each of the two independent EBN channels must now avoid systematic failures only with ASIL B(D).

Note: The requirements of the exemplary decomposition can be extended by other requirements, for example from other SR-Vehicle-Functions, and, if applicable, substituted or supplemented by stricter requirements.

4.2.2.2 Independence of decomposed Sources within an EBN Channel

Typically, the requirement in respect of the provision of sufficient power and energy for the EBN channel is decomposed to the available passive and Active Sources, cf. EBN-FSR 1.1.1 in chapter 5.3. The reason for this is that the ASIL requirement for the sources can be reduced by decomposition, which in turn may allow for the use of existing industrial modular products. Generators or DC/DC converters, for example, can be used as energy sources that, due to their dependence on the availability of the drivetrain or their history, only implement the provision of power and energy in QM. If the electrical source power is dependent on the mechanical input power of the drivetrain, the availability of the power output can usually only be implemented in QM.

The decomposition then results in the requirements for sufficient independence of the decomposed sources. Sufficient independence means that both sources can, independently as well as jointly, ensure safe supply for the SR-Loads. When providing proof of the independent supply from one decomposed source, the power and energy of the other decomposed source must not be accounted.

Example: If the decomposition aims at the sole provision of the SR-Maneuver (incl. MRM) by the Active Source, the buffer capability of the Passive Source must not be taken into consideration for the proof. If such proof cannot be provided, there is insufficient independence according to ISO 26262-9:2018, 7. The implementation of the independent supply by the Active Source is particularly challenging if sources with restricted dynamics are to be incorporated in the safety concept (e.g. conventional generators).

4.2.2.3 Use of Homogenous Redundancy within the EBN Safety Concept

As a matter of principle, the use of homogenous redundancy is inconsistent with the use of an ASIL decomposition, as the use of the same Elements in redundant paths generally makes it impossible to fully support the argument of sufficient independence. Therefore, the redundant paths in case of homogenous redundancy usually inherit the initial ASIL D. Consequently, diverse redundancy is the approach for using decomposition. However, if the use of diverse Elements for a decomposition is not possible or useful for each Element of the decomposed systems, one of the following options must be implemented:

A.1 Proof by means of a Dependent Failure Analysis (DFA, cf. ISO 26262-9:2018, 7.4.4) that the use of the homogenous Elements cannot result in a violation of Safety Goals caused by dependent failures;

A.2 Design and development of the homogenous Elements according to the initial ASIL.

Example: The safety-relevant ASIL D availability requirement for supplying the SR-Vehicle-Function ADS of the EBN is decomposed to the EBN channels terminal Kl30_s1_B(D) and terminal Kl30_s2_B(D). For economic reasons, the same component for power distribution (cf. chapter 5.2. EBN-FSR 1.1.2 / 1.2.2) and assurance of freedom from interference (cf. chapter 5.2. EBN-FSR 1.1.3/ 1.2.3) is to be used in both EBN channels. By using the same component, systematic design faults may, for example, result in the simultaneous loss of the redundantly designed SR-Vehicle-Function ADS and thus in a direct violation of the ADS-SG1. Consequently, those functions of the component used, which – being dependent failures – may lead to a violation of the Safety Goal, must be avoided by means of the initial ASIL D.

4.2.3 Freedom from Interference in the Electrical Power Supply System

Irrespective of a potential decomposition, freedom from interference within a system and/or a component must always be ensured. According to ISO 26262-9:2018, 6, the focus is on interactions between subsystems and subElements, which implement the requirements with a different ASIL (e.g. QM software Element affects the ASIL D software Element detrimentally). This is applied, for example, to avoid interferences from a vehicle component to safety-relevant functions within an electrical power supply channel (e.g. within terminal Kl30_s).

In summary, there are two sources that require freedom from interference:

- As part of the independence requirement (cf. chapter 4.2.2) when decomposition is used to reduce ASIL requirements.
- Arising from ISO 26262-9:2018, 6, when Elements with a different ASIL coexist in a system (coexistence of Elements).

The need to ensure freedom from interference generally arises when Elements with different ASIL classifications coexist in a system and have the potential to affect each other in terms of the safety requirements.

In practice, the requirement to ensure freedom from interference in the EBN context essentially affects the following three use cases:

- Proof of freedom from interference between two EBN channels (e.g. terminal Kl30_s1 and Kl30_s2) as part of the independence requirement when using an ASIL decomposition.
- Proof of freedom from interference within one EBN channel (e.g. terminal Kl30_s) as part of an independence requirement in case of a decomposition of the supply of energy and power for sufficiently independent active and Passive Sources.
- Proof of freedom from interference within one EBN channel (e.g. terminal Kl30_s) due to co-existing vehicle components with different safety integrities in terms of their safety-relevant availability requirements for the EBN. In particular vehicle components with no availability requirement placed on the EBN or a lower availability (than the integrity of the EBN channel) must be taken into consideration.

The freedom from interference between the EBN channels is explained in more detail in 4.2.3.1. Chapter 4.2.3.2 elaborates on the characteristics to be observed for a decomposition of the supply of energy and power to active and Passive Sources. The freedom from interference for vehicle components within an EBN channel is described in 4.2.3.3.

4.2.3.1 Freedom from Interference between two EBN Channels

As described above, the requirement of freedom from interference between different EBN channels presents an important part of the independence requirement. To ensure independence of the EBN channels, freedom from interference must be ensured for each Element of the EBN in different channels. This is particularly relevant for:

- Loads (e.g. independent activation, independence in case of supply from several decomposed EBN channels)
- Active and passive separating and connecting Elements (e.g. independent grounding studs, wiring)
- Active and Passive Sources (e.g. independent activation/deactivation)
- Energy Management (e.g. independence of commanded degrading).

If dependent failures are identified within the scope of a DFA, they must be avoided and/or controlled by means of the initial ASIL (ISO 26262-9:2018, 5.4.3).

4.2.3.2 Freedom from Interference for Sufficiently Independent Sources

The requirement regarding freedom from interference arises in case of a decomposition of the requirement for the provision of power and energy within an EBN channel. As described in chapter 4.2.2.2, a decomposition within an already decomposed EBN channel is usually performed if several active and Passive Sources exist. The objective is to specify requirements with a lower ASIL for the supply of energy and power by redundant active and/or Passive Sources, cf. chapter 6.1 and 6.2. Consequently, freedom from interference for the vehicle Elements must be proven separately for each decomposed supply path. According to ISO 26262-9:2018, 5.4.4, the decomposed supply paths must be able to fulfill the initial requirement both independently and jointly.

Example: In an already decomposed ASIL B(D) EBN channel, the supply of energy and power is implemented redundantly by one active and one Passive Source each, thus allowing for the provision of higher PMHF budgets for both sources. Furthermore, a requirement decomposition is performed for the Active Source with QM(D) and the Passive Source with ASIL B(D) so that the existing redundancy can be used for reducing the requirements for the systematic design and development process of the Active Source.

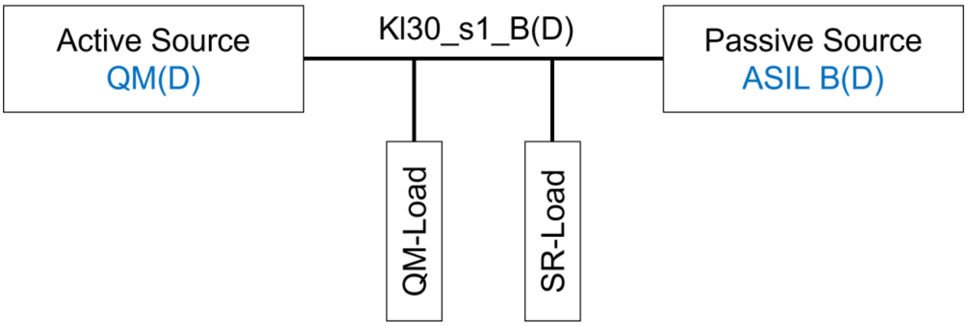


Fig. 3: Outline of a simplified single, decomposed EBN channel, e.g. terminal Kl30_s1_B(D)

For a complete safety case, proof of at least the requirements described in the subsequent three scenarios must be performed according to guidelines contained in Annex B:

Scenario A (faultless operation): Both sources of terminal Kl30_s1 (passive and active) each supply the specified minimum power/energy from the perspective of functional safety. ASIL B(D) must be used to avoid the occurrence of critical interference when both sources are available.

Note 1: As both sources are available in this operational state, interference can be compensated for better than in the following scenarios.

Scenario B (first fault in Passive Source): Only the Active Source supplies the specified minimum power/energy from the perspective of functional safety. The Passive Source is not available. In this scenario, interference that violates the safety requirement after a first fault must be avoided with QM(D).

Note 2: As only the QM(D) Active Source is available in this operational state and has a lower performance than a combination of the two sources in Scenario A, interferences can only be compensated for in a very limited fashion. Therefore, the power consumption of the consumers must be restricted more than in Scenario A to ensure freedom from interference.

Scenario C (first fault in Active Source): Only the Passive Source provides the specified minimum power/energy from the perspective of functional safety. The Active Source is not available. In this scenario, interference that violates the safety requirements must be avoided after the first fault, with an ASIL B(D) rating.

Note 3: As only the ASIL B(D) Passive Source is available in this operational state and has a lower performance than a combination of the two sources in Scenario A, interferences can only be compensated for in a very limited fashion. Therefore, the power consumption of the consumers must be restricted more than in Scenario A to ensure freedom from interference.

Note 4: Due consideration must be given to the fact that due to non-availability of the Active Source the operational status is subject to time limitations. For the MRM to be initiated, an energy reserve with ASIL B(D) must be provided for. The EOTTI described in chapter 4.2.4.4 must be subject to a time limit, in line with the energy reserve, to avoid occurrence of systematic failures caused by a discharged battery.

In respect of the requirement to avoid interferences, the requirement resulting from scenario C is dominant in this example, compared to the requirement resulting from scenario A, as interference has to be proven with the same ASIL integrity but at a lower source power. By implementing the requirement arising from scenario C, the requirement arising from scenario A can therefore also be fulfilled automatically.

From this general definition, different ASILs are derived for avoiding interference, if the active and Passive Sources mentioned above differ in their ability to supply electricity.

If the power reduction cannot be implemented within the FHTTI, the reduction of loads must be implemented preventively. Preventive load reduction means that the residual current in the EBN must not, at any time, be higher than the guaranteed power supply of the smaller source. This must be ensured by the initial ASIL B(D) of the EBN channel.

Example: Load reduction to ensure independence of the source(s)

- Maximum guaranteed power supplied by the Active Source in the entire specification range, with QM(D): 200 A
- Maximum guaranteed power supplied by the Passive Source in the entire specification range, with ASIL B(D): 300 A
- Current EBN load: 400 A, of which
    - 300 A QM-Loads (degradable/can be switched off)
    - 100 A SR-Loads (minimum load to be supplied)
- Upon loss of the ASIL B(D) Passive Source: reduction of the QM current consumption (with QM(D)) by 200 A to 100 A within the FHTTI in order to reduce the total current consumption of the EBN (QM+SR) to the Active Source's current supply of 200 A.
- Upon loss of the QM(D) Active Source: reduction of the QM current consumption (with ASIL B(D)) by 100 A to 200 A within the FHTTI in order to reduce the total current consumption of the EBN (QM+SR) to the Passive Source's current supply of 300 A.

Note 5: For the maximum permissible current consumption of the QM-Loads, a reserve for interference must be taken into consideration if they are not avoided/and or controlled by means of centralized or decentralized safety mechanisms with sufficient ASIL. If the reserve is sufficient to avoid interference, and this is safeguarded by the corresponding ASIL, then these interferences can be classified as "safe" regarding Annex B step 1. For the design of the reserve, the criteria and boundary conditions contained in Annex B must be complied with.

For details of the proof of freedom from interference within an EBN channel, reference is hereby made to Annex B.

4.2.3.3 Freedom from Interference within an EBN Channel

As described in the introduction to chapter 4.2.3, the requirement to ensure freedom from interference within an EBN channel fundamentally arises from ISO 26262-9:2018, 6, when components with a different ASIL coexist in a system (coexistence of Elements). That means that vehicle components/functions

- that place no safety-relevant availability requirements on the EBN do not violate safety requirements of vehicle components/functions that place a safety-relevant requirement on the EBN, and
- that place safety-relevant availability requirements with low ASIL integrity on the EBN do not violate safety requirements of vehicle components/functions that place a safety-relevant availability requirement with a higher ASIL on the EBN.

Example 1: If a control unit implies no safety-relevant availability requirements on the EBN, it will typically not have a safety requirement - as described in ISO 26262:2018 – to ensure freedom from interference with the EBN. This poses the risk of the control unit violating safety-relevant availability requirements of another control unit on the EBN if a fault occurs due to interferences on terminal Kl30_s.

Note: If the function or malfunction or an Item during the HARA shows an S, E or C ranking of zero, it is classified as non safety-relevant and thus places no availability requirement on the EBN. Nevertheless, potential interferences of this Item on the respective EBN channel must be avoided and/or controlled by means of the corresponding ASIL.

Example 2: If a control unit place a lower safety-relevant availability requirement on the EBN than another control unit, the former will usually also have a requirement with a lower ASIL to ensure freedom from interference on the EBN. This poses the risk of the control unit violating safety-relevant availability requirements of another control unit on the EBN if a fault occurs due to interferences on terminal Kl30_s.

In both cases, safety-relevant interferences must be avoided and/or controlled with the highest ASIL of the safety requirements for the EBN channel. The requirement for the EBN channel is inherited from the SR function that places the highest safety-relevant availability requirement on this EBN channel.

For vehicle components/functions that place the same safety-relevant availability requirements on the EBN, additional safety measures are not usually necessary to achieve freedom from interference. Instead, care must be taken to ensure that the safety-relevant vehicle components/functions themselves achieve their freedom from interference at least at the same ASIL rating which they require for a safe supply from the EBN. This is due to the fact that a fault of a vehicle component/function that results in the loss of its power supply will also inevitably result in the loss of the SR function to be provided. If this fault is not safeguarded with at least the ASIL of the SR function to be provided, the vehicle component will violate the requirements placed on it.

In this case, relevant vehicle components are deemed to be all Elements which – alone or in combination with other, dependent vehicle components – may influence compliance with the safety requirements (e.g. compliance with the voltage requirement of the safety-relevant loads) of an EBN channel (e.g. control units with/without safety-relevant functions, sensors, actuators, cables, plugs, storage devices, sources etc.). In addition, the combination of interferences of several independent Elements must be considered within the scope of a quantitative error analysis, taking into consideration the respective occurrence. This is an MPF that must not be neglected due to the likelihood of its occurrence.

Example "Interference of vehicle components": If the ASIL-protected reserve of the source for controlling interference is 100 A and there are two independent consumers with a nominal current consumption of 10 A each, which consume a maximum of 60 A electricity each in a failure mode, these alone cannot exceed the reserve in case of a failure. However, the concurrent interference from both consumers results in the reserve being exceeded and thus in a violation of the safety requirement regarding freedom from interference.

Additional safety measures, such as ATVs as per chapter 6.3, must be provided for if:

- there is a dependency of the components
- the probability of the fault combination of sufficiently independent vehicle components exceeds the derived PMHF budget, taking into consideration all other inferences; cf. EBN-FSR 1.1.3 and EBN-FSR 1.2.3.

A systematic mutual dependency of vehicle components is deemed to exist if these components (or Elements thereof) were not designed completely independent of each other, e.g. when using identically constructed microcontrollers in four different door control units. If their independence cannot be proven by means of a DFA, the combination of simultaneously occurring faults of all four control units must be taken into consideration when analyzing interferences.

4.2.4 Emergency Operation and Safe State

The safety concept of the EBN must ensure, inter alia, that at least one Emergency Operation is possible after a fault to achieve a safe state.
Consequently, the safety concept for the EBN constitutes a Fail-Active concept. SPFs (e.g. also "dependent failures") that lead to a direct loss of the SR-Vehicle-Function are only permissible with a sufficiently low probability (cf. in particular ISO 26262-5:2018, 9.4.1).

Fail-Active safety concepts for the power supply of safety-relevant functions require a special focus on the adoption of a safe state after a first fault was detected. ISO 26262:2018 presents a few underlying conditions already. However, in their concrete application to the power supply system as a "Shared Resource" for several SR functions they require interpretation. Within the scope of the definition, this recommendation constitutes a coordinated minimum requirement for the interpretation of the respective passages in ISO 26262:2018.

The Emergency Operation is executed whenever there is a first fault in the electrical power supply which impairs integrity. Due consideration must be given to the fact that operations outside the permissible operating range may also be classed as a potential first fault and subsequently be referred to as such.

Note: Regarding the operating ranges, the EOTTI shall only be used if the anticipated typical environment and user profiles of the relevant operating conditions are not met. Frequent or multiple exceedances of inadmissible operating conditions shall be considered as a systematic development fault.

4.2.4.1 Strategies for Reaching a Safe State

Generally, the safe state and transitioning of the system to the safe state during Emergency Operation are predetermined by the safety concept of the SR-Vehicle-Function. However, in case of a safe power supply, several SR-Vehicle-Functions resort to the EBN system.

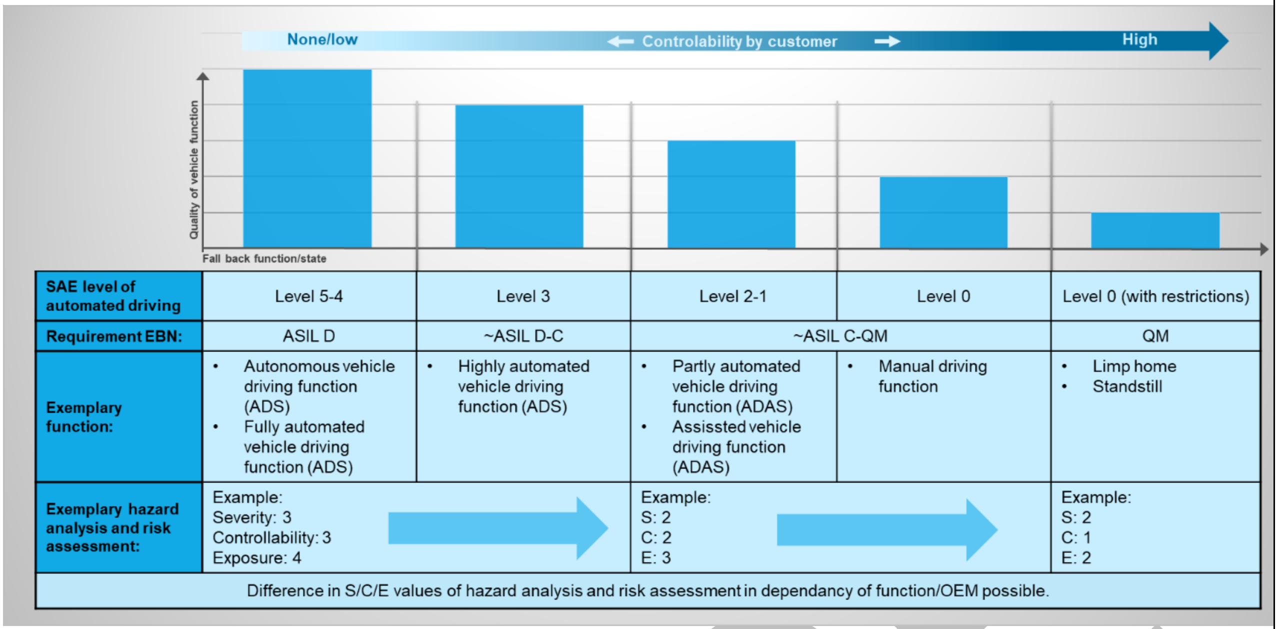
Therefore, several safety concepts with different integrity ratings and safety requirements for the EBN may coexist. Thus, the EBN constitutes a Shared Resource for several safety concepts.

This leads to specific features of the EBN safety concept that need to be taken into consideration for the design, development and during operation.

Usually, a vehicle is not developed for just one operation mode. In addition to autonomous, fully-automated and partly-automated driving, manual operation also places safety requirements on the EBN and is thus an SR-Vehicle-Function.

Several SR-Vehicle-Functions can be implemented in a vehicle, each with its own safety concept. These SR-Vehicle-Functions can have different integrity levels. Depending on the function characteristics and consideration within the safety concept, SR-Vehicle-Functions with lower integrity level can be used as a fallback function or as a Safe State for a higher rated SR-Vehicle-Function. The prerequisite is that the corresponding fault cases in the nominal function do not affect the safety concept of the fallback function.

Example: An SR-Vehicle-Function ADAS can be used as a fallback function or Safe State of an SR-Vehicle-Function ADS.



SAE level of automated driving	Level 5-4	Level 3	Level 2-1	Level 0	Level 0 (with restrictions)
Requirement EBN:	ASIL D	~ASIL D-C	~ASIL C-QM		QM
Exemplary function:	• Autonomous vehicle driving function (ADS) • Fully automated vehicle driving function (ADS)	• Highly automated vehicle driving function (ADS)	• Partly automated vehicle driving function (ADAS) • Assissted vehicle driving function (ADAS)	• Manual driving function	• Limp home • Standstill
Exemplary hazard analysis and risk assessment:	Example: Severity: 3 Controllability: 3 Exposure: 4		Example: S: 2 C: 2 E: 3		Example: S: 2 C: 1 E: 2
Difference in S/C/E values of hazard analysis and risk assessment in dependancy of function/OEM possible.					

Fig. 4: Illustration of the interaction of different vehicle functions and exemplary integrity levels

Due to its high severity, low controllability and high exposure, a function with a very high degree of automation has a high integrity level. A lower degree of automation and thus a greater involvement of the driver or the use of other technologies to supply power (e.g. hydraulic systems with manual operability) can influence both controllability and severity. Temporal and geographic restrictions (ODD) can influence the exposure factor. This reduces the safety requirements for the SR-Vehicle-Function and consequently also the requirements allocated to the EBN.

If faults occur in the Electrical Power Supply System, which affect the EBN safety concept and result in a reduction of the system integrity (e.g. loss of an electrical power supply channel), safe operation may still be possible if the function with the lower integrity level has been designed accordingly. In this case, the function with the lower level of integrity is still deemed to be a safe state.

Usually, a standstill of the vehicle is the condition with the lowest requirements placed on the Electrical Power Supply System. This idle state is commonly also referred to as the "safe state" although several safe states are conceivable or possible.

According to ISO 26262:2018, though, the safe state must be defined specifically for each respective safety concept of an SR-Vehicle-Function. (Cf. chapter 4.2.4.3)

To be able to use a function with a lower integrity level as a safe state, both SR-Vehicle-Functions must have been subjected to a separate HARA and corresponding, separate safety requirements for the electrical power supply must have been specified.

The subfunction that takes over transitioning from the faulty nominal function to the respective safe state is part of the safety concept of the nominal SR-Vehicle-Function. Therefore, a classification of hazards and risks is performed in the context of the HARA for the nominal SR-Vehicle-Function.

In this case, the maximum exposure time of the subfunction is limited by the Emergency Operation Tolerance Time Interval (EOTTI), which must be defined and predetermined in the safety concept of the SR-Vehicle-Function.

The safe state(s) in case of electrical power supply failures must be established both in the safety concept of the SR-Vehicle-Function and of the EBN and be defined in the Condition of use.

To transition the SR-Vehicle-Function with the higher level of integrity to the SR-Vehicle-Function at the lower level after a fault has occurred, an Emergency Operation will be performed if the respective Safety Mechanism is not completed within the FTTI. During the Emergency Operation, a shortfall of the system integrity compared to the integrity determined during HARA is permissible. (Cf. chapter 4.2.4.2).

4.2.4.2 Integrity during the Emergency Operation

For the operational requirements during the Emergency Operation, there are several passages that are relevant for the EBN safety concept.

In this context, the design of the system regarding the integrity level after occurrence of a first fault and the underlying conditions needed for Emergency Operation require particular attention.

Reference 1: ISO 26262-10:2018, 12.2.4.1 - Emergency Operation

During Emergency Operation, the Item is still free from unreasonable risk even though the ASIL capability of the Item is lower than the ASIL rating of the possible hazard. To address this situation, the operational time in this state is limited, such that it is unlikely that an additional fault occurs which leads to violation of the Safety Goal.

Note 1: The Emergency Operation Tolerance Time Interval is defined and verified from the probability of a next fault in accordance with 12.3.1.

Note 2: The transition to the Emergency Operation is defined and verified to be safe.

Reference 2: ISO 26262-10:2018, 12.2.4.2 - Safe states for fault-tolerant Item

Note 6: The Safety Mechanism implementing the restrictions of the possible vehicle operation states inherits the original ASIL of the Safety Goal. If the safe state is reached or maintained with the support of functions of other items, these are identified as safety requirements on those items.

Reference 3: ISO 26262-10:2018, 12.2.5.4 - System architecture description of the Item

Each one of channel A and channel B can, by itself, fulfil the safety requirements on an ASIL D level as far as systematic faults are concerned.

The combination of channel A and channel B can fulfil the safety requirements on an ASIL D level as far as random hardware faults (e.g. <= 1% of the random hardware faults can lead to a significant loss of functionality) are concerned.

Reference 4: ISO 26262-10:2018, 12.2.5.4 -System architecture description of the Item

The vehicle speed is reduced to less than v_2 by other items and this function is an additional safety requirement for such Item with ASIL D. This is a prerequisite for implementing Channel B in strategy 2.

Reference 5: ISO 26262-10:2018, 12.2.5.5 - Flow of events for this example

Note: The safety requirement to reduce the vehicle speed to v_2 has an ASIL D rating. Therefore, the function to reduce and maintain the vehicle speed to v_2 needs an ASIL D capability.

The referenced ISO passages are particularly relevant to the power supply, since its corresponding structure has strong interactions with the functional partitioning of the SR function.

If the functional concept of the SR function includes two redundant, decomposed channels, this often applies to the EBN, too. In this case, there are two redundant electrical power supply channels.

If the fault is restricted to just one electrical power supply channel and this fault results in the loss of one of the electrical power supply channels, the current rating of the system's integrity and of the SR function is automatically reduced to the integrity of the remaining channel for all functions that require power for their performance.

The requirement for integrity during the Emergency Operation (i.e. after occurrence of a first fault until the safe state has been reached) and the specification of the transition function to the safe state of the SR-Vehicle-Function therefore determines whether a power supply must be available with a simple or multiple redundancy.

Regarding the integrity requirements after occurrence of a first fault, ISO 26262:2018 allows for two general interpretations:

Interpretation option 1:

After a first fault, a transition to a safe state / degraded driving operation must be performed with a function that also receives the initial ASIL rating. Reference 2, 3, 4 and 5 refers to this.

Example: After a first fault within an ASIL D classified system, there is still another electrical power supply channel with ASIL D capability (regarding systematic failures). This does not affect hardware metrics.

Interpretation option 2:

After a first fault, the system may be operated with a lower ASIL integrity for a limited period of time when transitioning to a state with a lower ASIL rating. This limited period of time must not exceed the Emergency Operation Tolerance Time Interval (derived from the random hardware failures) established in accordance with ISO 26262:2018.

Example: Loss of a decomposed electrical power supply channel with an ASIL B(D) rating leads to a state where, temporarily, there is only one channel with ASIL B(D), while the vehicle is still in an ASIL D rated state. This status is only permitted during the temporary transition in a state with ASIL B rating.

This is referred to by reference 1 (12.2.4.1). In this example, reference 3 (12.2.5.4) is simply considered an implementation example and reference 5 (12.2.5.5) a Fail-Passive function (vehicle rolls until it has fallen below v_2).

In the context of a safety standard, interpretation 2 of ISO 26262:2018 is adopted here.

ISO 26262:2018 defines no clear requirements and guidelines for the integrity to be applied to implementing the EO in case of faults that do not have the potential to directly violate the SG. A possible implementation is introduced below:

The fault detection mechanisms for each EBN channel, which lead to the MRM being initiated, must be implemented in accordance with the integrity of the EBN channel. Usually, that includes fault avoidance or fault handling according to ASIL B(D). Furthermore, mechanisms to detect latent multiple faults are used, which can be implemented with a reduced ASIL as described in ISO 26262-4:2018, 6.4.2.5.

In addition, the loss of an SR function allocated to an EBN channel is detected by an SR-Vehicle-Function with a specified integrity and the MRM is initiated.

Since both detection paths access the same safety reaction to initiate the MRM, this initiation must be implemented in accordance with the initial ASIL.

The MRM may, for example, be initiated by a Fail-Passive function, thus requiring no additional availability requirement with ASIL D placed on the EBN during the EO. Adherence to the EOTTI must be ensured in accordance with ASIL D. After expiry of the EOTTI, the further execution of the SR-Vehicle-Function must be avoided with the initial ASIL, which can also be ensured without an additional ASIL D availability request for the EBN. According to interpretation 2, the general transition of the vehicle to a safe state can also be performed with a reduced integrity for the limited duration of the EOTTI.

Adherence to the EOTTI ensures that the MRM exposure duration is very low. This ensures that the probability of a random HW failure violating a Safety Goal is sufficiently low. Due to the independence of the remaining EBN channel, the occurrence of systematic second faults during the EOTTI is unlikely. Accordingly, a reduced integrity due to a faulty system is acceptable for exercising the MRM.

In summary, the Higher-Level Instance of the SR-Vehicle-Function must be designed to ensure that in case of the absence of active feedback about the EBN's freedom from faults, the trigger for transitioning to a safe state / the Emergency Operation can be activated automatically (and without power).

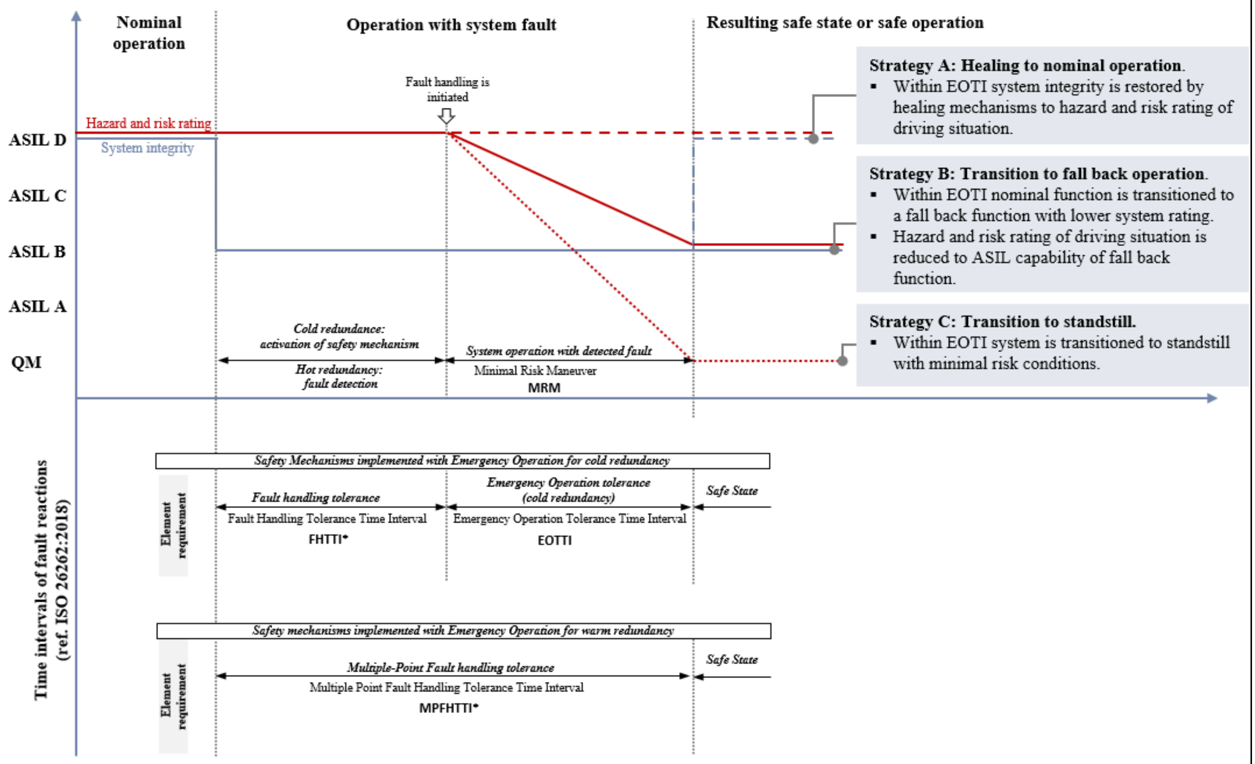
When using a hot redundancy, an existing backup path is already connected to the system. The fault reaction is limited to initiating the adoption of a safe state by informing the Higher-Level

Instance. By contrast, using a cold redundancy first requires warding off a failure within the FTTI, before a safe state can then be achieved within the EOTTI.

In case of a hot redundancy that has not implemented full independence requirements (e.g. when using a QM-DCDC converter in combination with a safety-relevant Passive Source in an EBN channel), due consideration must be given to the fact that the MPFDTI has already expired in case of a detected MPF. Therefore, the MPFDTI must be deducted from the EOTTI when using a hot redundancy to calculate how much time remains for transitioning to a safe state.

In both fault scenarios, an Emergency Operation can occur within the EOTTI. In case of single-point faults this is the case, for example, when a system failure was avoided during the FHTI but the system's integrity does not yet match the integrity rating of the driving situation.

4.2.4.3 Timing of the Transition to a Safe State


Nominal operation
Operation with system fault
Resulting safe state or safe operation
Fault handling is initiated
Hazard and risk rating
System integrity
ASIL D
ASIL C
ASIL B
ASIL A
QM
Cold redundance: activation of safety mechanism
Hot redundancy: fault detection
System operation with detected fault
Minimal Risk Maneuver
MRM
Time intervals of fault reactions (ref. ISO 26262:2018)
Safety Mechanisms implemented with Emergency Operation for cold redundancy
Element requirement
Fault handling tolerance
Fault Handling Tolerance Time Interval
FHTTI*
Emergency Operation tolerance (cold redundancy)
Emergency Operation Tolerance Time Interval
EOTTI
Safe State
Safety mechanisms implemented with Emergency Operation for warm redundancy
Element requirement
Multiple-Point Fault handling tolerance
Multiple Point Fault Handling Tolerance Time Interval
MPFHTTI*
Safe State

Strategy A: Healing to nominal operation.

- Within EOTI system integrity is restored by healing mechanisms to hazard and risk rating of driving situation.

Strategy B: Transition to fall back operation.

- Within EOTI nominal function is transitioned to a fall back function with lower system rating.
- Hazard and risk rating of driving situation is reduced to ASIL capability of fall back function.

Strategy C: Transition to standstill.

- Within EOTI system is transitioned to standstill with minimal risk conditions.

Fig. 5: Timing of the transition to the Safe State

The illustration shows the integrity of the power supply system in relation to the time.

It depicts a scenario in which the vehicle is in a driving situation that received an ASIL D rating during a HARA due to its environment and current speed. A first fault (e.g. loss of a safety-relevant source in a two-source system) leads to a reduction of the system integrity.

A fault diagnosis and fault reaction avoid a system failure or a single/multiple-point failure. The power supply function is upheld while the system integrity and the integrity rating of the driving situation are aligned during the course of the Emergency Operation.

The EO has come to an end when the system integrity once again matches or even exceeds the integrity rating of the driving situation.

For this purpose, different strategies (cf. Fig. 5) can be employed:

Strategy A "Restoration (healing of the system)": With the help of a fault reaction mechanism, the original integrity can be restored after occurrence of an MPF. In a two-source system, for example, consisting of an active and Passive Source, heating or charging strategies can increase the capacity of the Passive Source if insufficient capacity has been detected beforehand. In this case, there would be a brief shortfall in the system's integrity as the source would be unable to provide the power for the Minimal Risk Maneuver (MRM) that might have to be performed.

However, the EOTTI shall only be applied in case of a deviation from the expected typical environment and user profiles within the relevant operating conditions. In any other case, it is usually an error in the systematic design of the Passive Source.

Strategy B "Transition to another SR-Vehicle-Function state": With the help of a fault reaction mechanism, the integrity rating of the driving situation can be reduced and the nominal function can be transitioned to an SR-Vehicle-Function with a lower system integrity rating. By reducing the speed or integrating a driver in a new SR-Vehicle-Function state, for example, the severity or controllability of the driving situation can be influenced.

Strategy C "Transition to standstill": This strategy presents a special case of strategy B and describes the transition to standstill and the subsequent immobilization of the vehicle at an acceptable safe place (minimal risk condition).

4.2.4.4 Possible Derivation for Temporal Restrictions of the Emergency Operation (EOTTI)

If the necessary integrity cannot be ensured for a longer period than the FHTTI due to faults in the Electrical Power Supply System, the system must be transitioned to a safe state within the EOTTI and with the ASIL integrity of the residual system (cf. chapter 4.2.4.2 and chapter 4.2.4.3).
The maneuver-specific EOTI must be less than the EOTTI to be defined for the system, which in turn must be defined in due consideration of the physical constraints, other safety requirements, Common Cause Failure potential etc. (ISO 26262-10:2018, 12.2.4.3). Therefore, a detailed analysis of dependent failures is particularly important.

ISO 26262-10:2018 describes two calculations methods for determining the EOTTI (cf. ISO 26262-10:2018, 12.3.1.1 and 12.3.1.2).

The two calculation methods serve to provide an approximate evaluation of the EOTTI by means of a fault tree. Depending on the method of calculation, the EOTTI results vary. Both calculation methods are relevant; however, the applicability of the calculations must be checked depending on the respective case under consideration and the problem.

The calculation methods do not constitute a target for the derivation of the EOTTI. The correct method for determining the EOTTI is the quantitative analysis of random HW failures. In doing so, the probability of a failure of the faulty system during an Emergency Operation must be taken into consideration, in combination with the respective first fault. Within the quantitative safety analysis, the EOTTI can be chosen freely (without limitations imposed by the stated calculation methods) and is included in the respective failure probability. An important issue in the choice of the EOTTI is compliance with the target metrics of the quantitative safety analysis in total.

However, the EOTTI is not just restricted by the quantitative safety analysis but also by systematic safety analyses. Proof must be provided that the system will be free from unreasonable risks during Emergency Operation.

In concrete terms this means that for an Emergency Operation following a first fault, a pertinent analysis must be performed which identifies the risk potential of systematic second faults.

Due consideration must be given to the fact that the EOTTI is calculated across the life cycle/service life and averaged across the entire vehicle fleet. If a fault can therefore occur repeatedly, this must be taken into consideration for the design, as the cumulated duration of all emergency operations regarding this fault must not exceed the EOTTI. This applies in particular if the fault strategy aims to restore nominal operation after an Emergency Operation.

Monitoring adherence to the EOTTI for faults that can occur repeatedly during the vehicle's life cycle, is therefore recommended.

Example: A diagnosed non-capability of safety-relevant energy storage devices constitutes a fault condition for the EBN. However, if a further energy source has been installed, no system failure is deemed to exist. Nevertheless, since the probability of the EBN's failure is increased in this state and full system integrity is not available, a fault condition is deemed to exist. This fault condition of the Passive Source can be lifted by charging the battery or heating the battery, for example, until full system integrity has been restored.

Unexpected cold temperatures or very long immobilization times can result in a Passive Source with insufficient performance. Therefore, unfavorable driving behavior in combination with pertinent geographical conditions may result in a repeated exposition of a storage device unable to provide energy. Adding up the specific EOTI in each event of this fault ensures that the risk in connection with random hardware failures of the faulty system does not increase to an unreasonable level.

Note: As addressed in the previous example, transient fault conditions of electro-chemical energy storage devices caused by a temporary incapacity due to the temperature or the state of charge are of particular relevance for a repeated exposition of the EOTTI. The probability of exceeding a parameter due to an unpredicted use cannot usually be avoided altogether.

Therefore, the specific operating temperature and state-of-charge ranges of active and Passive Sources must be monitored in terms of adherence to the EOTTI and taken into consideration in the context of a multiple transient performance of an Emergency Operation.

4.2.4.5 Requirements for the Operating and Control Concept in Connection with EOTTI

The power supply by itself does not constitute a function that requires a direct interface with the driver and/or passenger. Nevertheless, there are pertinent norms, standards and legal provisions that demand a corresponding indication in case of a failure or restriction of the power supply.

Usually, the interface with the driver and/or passenger is defined in the respective SR-Vehicle-Function. That means there is no direct connection between the power supply and the customer interface and a notification regarding the EBN would be communicated via the SR-Vehicle-Function.

Due to legal requirements, the historic development of the EBN and in light of the use of the EBN as a Shared Resource, it may be sensible to partially connect the display concept directly with the power supply safety concept and to display certain faults and failures directly from within the electrical power supply function. (Cf. EBS-LR 11)

This document does not intend to give a clear recommendation for implementation options. However, it is advisable to make a note of this issue within the scope of the Conditions of Use between the SR-Vehicle-Function and the electrical power supply.

However, irrespective of the technical implementation it is advisable – in case of a first fault and an exceedence of the EOTTI – to inform the Higher-Level Instance about this.

Depending on the integration of the driver and/or passenger in the SR-Vehicle-Function, an effective acoustic and visual display concept is also recommended, which prompts the driver and/or passenger – if integrated in the MRM or the direct exercise of functions (e.g. for L3 functions) – to reach the Safe State. This must be coordinated with the respective SR-Vehicle-Functions within the scope of the requirements coordination.

In terms of the operating and control concept, it is also advisable to still permit a restricted driving operation - even if the EOTTI is exceeded – while maintaining the warning, as an operating mode of its own, independent of the prior nominal SR-Vehicle-Functions, thus allowing potential secondary hazards (e.g. emergency stop in an ambulance or on railway lines etc.) to be defused quickly and simply or allowing for a simplified recovery of the vehicle under safe conditions (e.g. use of emergency services) by means of manual intervention.

4.2.4.6 Return to the Nominal Function

After occurrence of a first fault, a system repair may be a sensible mechanism, depending on the situation, to increase safety and availability.

Example: Topology with a two-channel system. The electrical power supply channel Kl30_s1 fulfills the function of providing power by means of passive energy storage and a DCDC converter. The safety load is decomposed equally homogenous on both Elements.

A first fault within the DCDC converter leads to a failure of the power supply. Consequently, the power supply channel Kl30_s1 and thus the entire system falls short of the integrity. By means of a diagnosis and performance of a Safety Mechanism (e.g. reset), the fault can be remedied and the power supply be resumed. The original integrity of the power supply system is restored.

Note: Initially, the first fault is to be avoided with the ASIL integrity of the allocated or decomposed safety-relevant availability requirement. If the fault can be remedied within the MPFHTTI, the original ASIL capability of the system is restored and a safe state has been achieved. By restoring (healing) the system, the journey can be continued, cf. chapter 4.3.3.

A repair mechanism is part of the safety concept and must be subject to both a systematic and a quantitative analysis.

The frequency of exposition and the duration of the repair mechanism define the non-availability of a function of the safety concept. For a quantitative analysis, the probability must be quantified in the fault tree.

The repair function itself is part of the safety concept and subject to the restrictions of ISO 26262:2018. Therefore, a systematic design and development must take place in accordance with the derived integrity requirement.

Since carrying out the repair function takes a certain period of time during which the required integrity of the SR function is too low, the repair function must be completed within the time window of the Emergency Operation. In case of the same repair function being carried out repeatedly within the product's life cycle, the temporal restrictions of the Emergency Operation Tolerance Time Interval must be taken into consideration (cf. chapter 4.2.4.4).

It is advisable to document pertinent repair mechanisms in terms of the duration and frequency of their activity and to check them in the context of field monitoring.

4.2.5 Predictable Misuse

Predictable misuse is a relevant aspect within the scope of developing EBN safety concepts and must be avoided as described in the guidelines of ISO 26262:2018. While a recommendation within the scope of a safety standard may be useful, it is not dealt with in this version of VDA 450.

5. Functional Safety Concept EBN

In chapter 5, the functional safety concept for the EBN is derived. The objective of the chapter is to derive the requirements both for the EBN components and the loads supplied by the EBN from the requirements of the safety-relevant vehicle functions identified in chapter 4.

5.1 Classification of the EBN in the ISO 26262:2018 Context

To develop the Electrical Power Supply System in accordance with ISO 26262:2018, the Electrical Power Supply System must be aligned with the technical terms of the standard (e.g. Item, System, Subsystem, Element). The correct classification of the Electrical Power Supply System in these technical terms can lead to different results due to the generic definition of the terms. However, these different results are not inconsistent with each other; instead, they each constitute autonomous solutions with individual advantages and disadvantages.

5.2 Concept Classification

In the context of this recommendation, two different classifications of the Electrical Power Supply System in the context of ISO 26262:2018 were studied in detail. In the first concept, the electrical power supply is defined as an Item. In the second concept, the electrical power supply is not defined as an Item but as a Subsystem.

The most important features of both concepts are compared in Table 2.

Features	EBN as item	EBN as subsystem of one or more items
EBN = Shared Resource	Applicable	Applicable
EBN = SEooC	Possible	Possible
HARA	HARA is performed at Entity level. Defined Entity Safety Goals are broken down into associated Items (cf. chapter 5.2.1). Assessment of the intrinsic safety for the EBN in HARA of the Item EBN.	HARA is performed at Item level (SR-Vehicle-Function). The assessment of the scenario must take into account a failure of the EBN as well as the interference with other safety-relevant functions (steering assistance, braking assistance, …). Assessment of the intrinsic safety for the EBN in a separate safety analysis.
PMHF	The PMHF budget is defined at Item level, cf. chapter 3.2.3. The target PMHF budget is defined by the lowest budget of the respective safety-relevant functions.	Allocation of a PMHF budget for the electrical power supply / the EBN channel from the respective Items of the safety-relevant functions. The target PMHF budget is defined by the lowest budget of the respective safety-relevant functions.
Direct provider of requirement for the EBN	HARA of the higher-level Entities, EBN HARA & Conditions of Use incl. allocation of functions and technical safety requirements.	Higher-level system Elements & Conditions of Use. Allocated safety-relevant subfunctions necessary for carrying out a Safety-Relevant Function (e.g. actuator for ADS, logic for ADS, …).
Freedom from interference	Merger of analysis & proof at Item-EBN level explicitly for the EBN scope.	Merger of analysis & proof at Item level (SR-Vehicle-Function) with EBN scope as part of the analysis.
Test cases in the safety case	System tests at Item-EBN level. Requirements based testing for Item EBN.	System tests at Item level (SR-Vehicle-Function). Requirements based testing for the Subsystem EBN.
Necessary documents for the EBN	Own Safety Case necessary. Less complex documentation for the Item of the SR-Vehicle-Function (reference to Safety Case EBN).	Less complex documentation for the organizational unit EBN, as the EBN does not constitute an Item of its own. The complete documentation is performed at Item level of the SR-Vehicle-Function.

Tab. 2: Comparison of the most important features for the development of the electrical power supply as an item and as a subsystem

Both concepts are described in more detail in the subsequent chapters and comply with ISO 26262:2018. There is no simple answer to which concept is better suited to a development project. This question must be evaluated for each case individually, taking into account influencing factors such as the organizational structure of the companies involved, systems already developed (so-called legacy systems) and functions that are not restricted to the vehicle level (e.g platooning, V2X communication).

Classifying the EBN as an Item of its own (cf. chapter 5.2.1) is particularly appropriate when it is developed within a separate organizational unit that is largely separated from the SR-Vehicle-Function. In this case, the reduced coordination effort between the organizational units – due to clear agreements by means of the Conditions of Use – reduces the probability of systematic design and development errors. Responsibility for the documentation in the context of the safety cases rest with the organizational unit EBN.

5.2.1 EBN as an Item

The electrical power supply is defined as an Item to bundle the requirements – at this level - of different Entities (e.g. AD, Steer-by-Wire, Platooning) or other Items (e.g. drive, brake, steering, light and visibility) for the electrical power supply by means of the "Conditions of Use" in chapter 3.2.3. The item Electrical power supply can be subdivided in further (sub-)system that are not defined as Items of their own here. This serves to minimize the interfaces and makes it possible to assess the specific hazards of the electrical power supply in a separate HARA of the item Electrical power supply.

The following requirement sources must be taken into account for the Item EBN:

- At **Entity level,** a HARA is performed, based on which Safety Goals for the Entity level are defined. From these Safety Goals, Safety Goals will be derived for the EBN Item level, if the Safety Goal at Entity level can be violated by a pertinent malfunction or if the Item contributes to fulfilling the Safety Goal at Entity level.
- At **Item level,** all items that place safety-relevant availability requirements on the power supply must collate their dependencies on the Electrical Power Supply System for each channel and document those in the Conditions of Use.
- Optionally, a HARA can be performed at the **item level Electrical power supply** and integrated in the safety concept to identify hazards posed by the components of the Electrical Power Supply System. Alternatively, this HARA must be performed in a separate safety concept and the correlations with the EBN safety concepts shall be considered in additional requirements and Conditions of Use.

The following minimum information must be provided to the item EBN:

- From the **Entity level:**
  - Safety Goals incl. ASIL, FTTI, Safe State
  - SR-Vehicle-Function with associated SR-Maneuvers (e.g. evasive maneuver, Minimal Risk Maneuver)
  - Preliminary technical concept for the implementation of the SR-Vehicle-Function / SR function, e.g. description of the system architecture (preliminary architectural assumption)
- From **other Items**:
  - Channel-specific integrity requirements based on the Item SG and the preliminary system architecture
  - Time-dependent undervoltage and overvoltage thresholds of the SR-Loads
  - Required power demand and energy demand of the SR-Loads in the SR-Maneuvers
- From **own HARA**:
  - Additional SG for dealing with Item-inherent hazards, such as fire risk caused by thermal runaway or chemical risks associated with outgassing batteries
  - Definition of the metrics requirements for the Item-related Safety Goals (SG)

According to chapter 3.2.3, the quantitative proof (PMHF, SPFM, LFM) in the Entity concept must be performed at Item level, analogous to ISO 26262-5:2018, 8.2 & 9.4.2.2.

Bundling the aforementioned requirement sources results in a complete set of requirements for the Item Electrical power supply. This, in turn, serves as the basis for deriving further requirements.

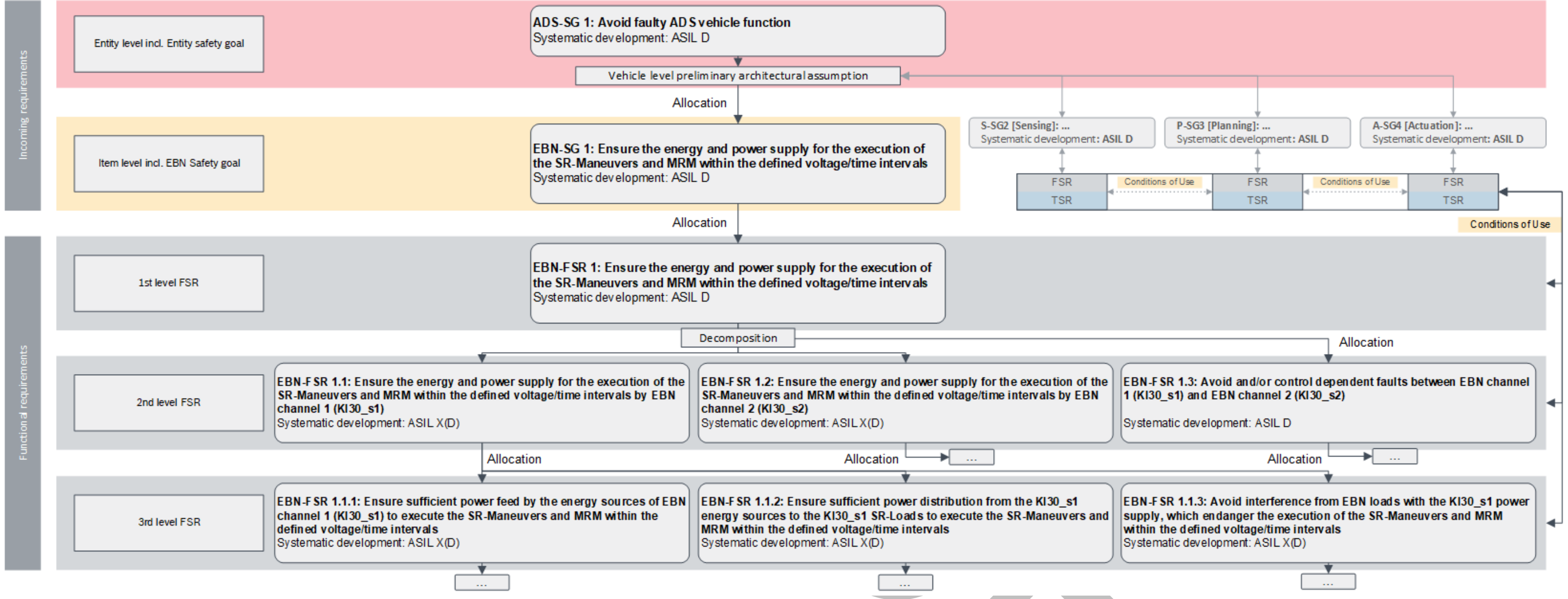

Incoming requirements
Functional requirements
Entity level incl. Entity safety goal
Item level incl. EBN Safety goal
1st level FSR
2nd level FSR
3rd level FSR
ADS-SG 1: Avoid faulty ADS vehicle function
Systematic development: ASIL D
Vehicle level preliminary architectural assumption
Allocation
S-SG2 [Sensing]: ...
Systematic development: ASIL D
P-SG3 [Planning]: ...
Systematic development: ASIL D
A-SG4 [Actuation]: ...
Systematic development: ASIL D
FSR
TSR
Conditions of Use
EBN-SG 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
EBN-FSR 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
Decomposition
EBN-FSR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 1 (KI30_s1)
Systematic development: ASIL X(D)
EBN-FSR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 2 (KI30_s2)
Systematic development: ASIL X(D)
EBN-FSR 1.3: Avoid and/or control dependent faults between EBN channel 1 (KI30_s1) and EBN channel 2 (KI30_s2)
Systematic development: ASIL D
EBN-FSR 1.1.1: Ensure sufficient power feed by the energy sources of EBN channel 1 (KI30_s1) to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
EBN-FSR 1.1.2: Ensure sufficient power distribution from the KI30_s1 energy sources to the KI30_s1 SR-Loads to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
EBN-FSR 1.1.3: Avoid interference from EBN loads with the KI30_s1 power supply, which endanger the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
...

Fig. 6: Example of FSR derived from the Safety Goals of the Entity

When designing and developing the Electrical Power Supply System, functional safety requirements arise which serve to comply with the Safety Goals. Figure 6 illustrates how Safety Goals are derived from the Entity level to the Item Electrical power supply and how these Safety Goals can be specified as functional safety requirements. In this publication, the starting point is the generic Safety Goal

ADS-SG 1: " Avoid faulty ADS vehicle function"

with ASIL D, as derived in chapter 4.1.1. In the process, the electrical power supply must ensure the energy and power supply of all items with a functional dependency on the EBN, with sufficient integrity.

After specifying the functional safety requirements for the Electrical Power Supply System, in this case

EBN-FSR 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals,

a decomposition of the safety requirements for the electrical power supply on the EBN channels can be performed on the basis of the "preliminary technical concept" – comparable to the "preliminary architectural assumptions" in ISO 26262:2018 – in line with

EBN-FSR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 1 (Kl30_s1)

and

EBN-FSR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 2 (Kl30_s2).

In doing so, the requirement of independence of the channels must be taken into consideration, analogous to

EBN-FSR 1.3: Avoid and/or control dependent faults between EBN channel 1 (Kl30_s1) and EBN channel 2 (Kl30_s2),

cf. chapter 4.2.2. The safety requirements EBN-FSR 1.1, EBN-FSR 1.2 and EBN-FSR 1.3 are derived analogously in chapter 5.2.2 in the concept "EBN as a Subsystem". Therefore, the further derivation of safety requirements within the individual EBN channels is described in chapter 5.3, based on the higher-level safety requirements.

5.2.2 EBN as a Subsystem of one or more Items

Apart from the concept of classifying the EBN as an Item, the EBN can also be classified as a Subsystem, as the EBN has no functions that can be directly experienced by the customer in terms of its tasks (such as energy and power supply and voltage supply). The HARA evaluates malfunctions whose effects can only be evaluated through the function itself. As the EBN does not constitute a function that can be experienced by the customer, a HARA directly related to the EBN is not applicable. Instead, the safety requirements for the EBN as a subsystem are derived from the individual systems (steering, light, etc.) (ISO 26262-9:2018, 7.4.4g). As a subsystem, the EBN must also ensure freedom from interference between the individual systems, cf. chapter 4.2.1.

Note: According to ISO 26262-3:2018, 6.4.2.6, the vehicle's power supply must be included in the HARA for deriving the Safety Goals of the Vehicle-Functions.

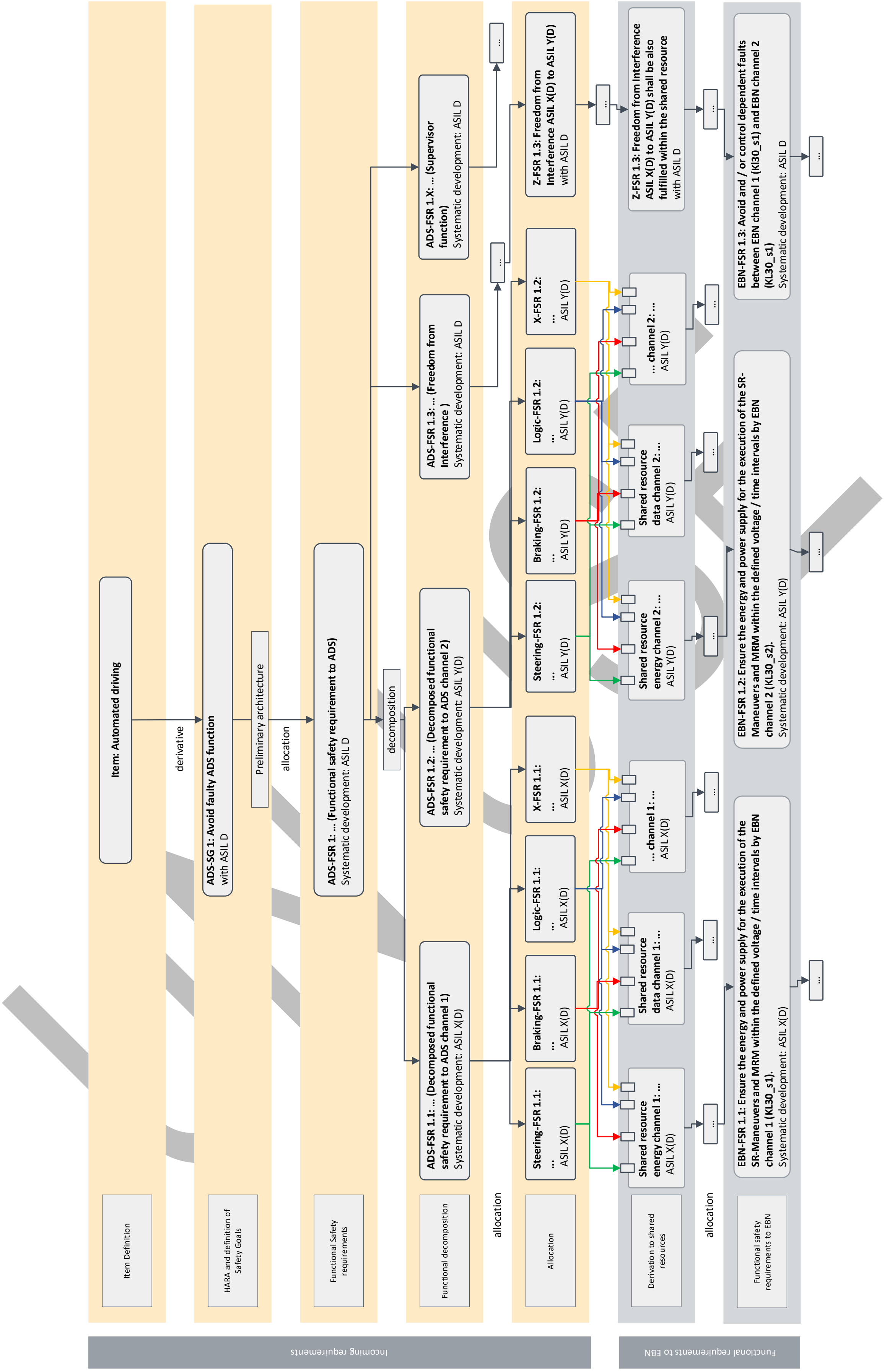

Item Definition
HARA and definition of Safety Goals
Functional Safety requirements
Functional decomposition
allocation
Allocation
Derivation to shared resources
allocation
Functional safety requirements to EBN
Incoming requirements
Functional requirements to EBN
Item: Automated driving
derivative
ADS-SG 1: Avoid faulty ADS function with ASIL D
Preliminary architecture
allocation
ADS-FSR 1: ... (Functional safety requirement to ADS) Systematic development: ASIL D
decomposition
ADS-FSR 1.1: ... (Decomposed functional safety requirement to ADS channel 1) Systematic development: ASIL X(D)
ADS-FSR 1.2: ... (Decomposed functional safety requirement to ADS channel 2) Systematic development: ASIL Y(D)
ADS-FSR 1.3: ... (Freedom from Interference) Systematic development: ASIL D
ADS-FSR 1.X: ... (Supervisor function) Systematic development: ASIL D
...
Steering-FSR 1.1: ... ASIL X(D)
Braking-FSR 1.1: ... ASIL X(D)
Logic-FSR 1.1: ... ASIL X(D)
X-FSR 1.1: ... ASIL X(D)
Steering-FSR 1.2: ... ASIL Y(D)
Braking-FSR 1.2: ... ASIL Y(D)
Logic-FSR 1.2: ... ASIL Y(D)
X-FSR 1.2: ... ASIL Y(D)
Z-FSR 1.3: Freedom from Interference ASIL X(D) to ASIL Y(D) with ASIL D
Shared resource energy channel 1: ... ASIL X(D)
Shared resource data channel 1: ... ASIL X(D)
... channel 1: ... ASIL X(D)
Shared resource energy channel 2: ... ASIL Y(D)
Shared resource data channel 2: ... ASIL Y(D)
... channel 2: ... ASIL Y(D)
Z-FSR 1.3: Freedom from Interference ASIL X(D) to ASIL Y(D) shall be also fulfilled within the shared resource with ASIL D
EBN-FSR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage / time intervals by EBN channel 1 (KL30_s1). Systematic development: ASIL X(D)
EBN-FSR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage / time intervals by EBN channel 2 (KL30_s2). Systematic development: ASIL Y(D)
EBN-FSR 1.3: Avoid and / or control dependent faults between EBN channel 1 (Kl30_s1) and EBN channel 2 (KL30_s1) Systematic development: ASIL D
...

Fig. 7: Example of a hierarchical approach to deriving requirements for the subsystem EBN

Figure 7 illustrates, by way of example, the hierarchical procedure for deriving requirements for the subsystem EBN. Through the strictly hierarchical procedure in this approach, inconsistencies in the safety concepts are avoided. The validation, verification and analyses can be performed at the individual levels of the Elements. To ensure the Safety Goals, an FIT budget is required for each case, as provided for by chapter 5.4.

The resulting safety requirements EBN-FSR 1.1, EBN-FSR 1.2 and EBN-FSR 1.3 are identical to those described in chapter 5.2.1 in the concept "EBN as an Item". Only the structure for the derivation and thus also the structure of the safety concept and the responsibilities differ. A further derivation of safety requirements within the individual EBN channels, based on the higher-level safety requirements, is described in chapter 5.3.

5.3 Adopted Safety Goals and Requirements for the EBN

This chapter describes how the Safety Goals of the SR-Vehicle-Function ADS are broken down by means of ASIL decomposition and allocation to the functional safety requirements of the EBN components. Within the described safety concepts, the ASIL decomposition is performed in different places. If the EBN is defined as an Item, decomposition takes place at EBN level. In this case, decomposition is based on the functional safety requirements for the electrical power supply. If the EBN is treated as a Subsystem, decomposition takes place at the level of the SR-Vehicle-Function ADS instead. After the requirements decomposition, the functional safety requirements for the electrical power supply from both development concepts are identical. They are:

- EBN-FSR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 1 (Kl30_s1)
- EBN-FSR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 2 (Kl30_s2)
- EBN-FSR 1.3: Avoid and/or control dependent faults between EBN channel 1 (Kl30_s1) and EBN channel 2 (Kl30_s2)

Note 1: It is imperative to always have sufficient power available to ensure that the defined SR-Maneuvers of the respective operating conditions can be executed.

Note 2: It is imperative to always have sufficient power available to ensure that the vehicle can be transitioned to a safe state by means of a defined MRM, as described in chapter 4.2.3.

Note 3: The energy and power reserves, for example, must be implemented with a prediction function at an appropriate ASIL integrity and a prediction horizon as per MRM.

The aforementioned, decomposed functional safety requirements are independent of the selected structure of the safety concept. In other words: Their validity does not depend on whether the EBN is treated as an Item or a Subsystem.

In the next step, the decomposed Functional Safety Requirement for each EBN channel – e.g. channel 1 with Kl30_s1 and Kl30_q and channel 2 with Kl30_s2 – is specified. The following three channel-specific requirements arise as a result and are allocated based on EBN-FSR 1.1.:

- EBN-FSR 1.1.1 / 1.2.1: Ensure sufficient power feed by the energy sources of EBN channel 1/2 (Kl30_s1 / Kl30_s2) to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
- EBN-FSR 1.1.2 / 1.2.2: Ensure sufficient power distribution from the Kl30_s1 / Kl30_s2 energy sources to the Kl30_s1 / Kl30_s2 SR-Loads to execute the SR-Maneuvers and MRM within the defined voltage/time intervals

- EBN-FSR 1.1.3 / 1.2.3: Avoid interference from EBN loads with the Kl30_s1 / Kl30_s2 power supply, which endangers the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals

Note 1: For the implementation of the functional safety requirements EBN-FSR 1.1.1 and EBN-FSR 1.2.1 and EBN-FSR 1.1.2 and EBN-FSR 1.2.2, the defined SR-Maneuvers of the respective operating conditions must be taken into account analogous to EBN-FSR 1.1 and EBN-FSR 1.2.

Note 2: The selected ASIL decomposition or the original safety requirements on two sufficiently independent EBN channels provides an example for the purpose of explaining the structure. The ASIL decomposition and allocation of safety requirements must always be performed individually for each specific project.

Note 3: The structure selected here – power feed, power distribution and freedom from interference – presents a possible, exemplary structural concept. It results from a common structure used by companies, using a breakdown by HW components. Other structures, e.g. by functions, faults or chains of effects, are also conceivable. In the final analysis though, all structural concepts allocate the functional safety requirements to components. Therefore, the final component requirements are independent of the selected substructure.

Note 4: As described in chapter 4.2.3, the requirement to ensure freedom from interference within an EBN channel according to EBN-FSR 1.1.3 and EBN-FSR 1.2.3 fundamentally arises from ISO 26262-9:2018, 6.

At the next level of detail in the requirement derivation, the functional safety requirements of the source capability as per EBN-FSR 1.1.1, the power distribution as per EBN-FSR 1.1.2 and the avoidance of interference as per EBN-FSR 1.1.3 are refined further. In doing so, a distinction must be made between systematic and random faults. Systematic faults whose origin can usually be traced back to an insufficient design process and which are reproducible, must be avoided in the design process and/or by means of suitable safety mechanisms at a corresponding ASIL integrity during operation. They are therefore not taken into consideration in the target metrics of ISO 26262:2018. The derived metrics (PMHF_bud, SPFM_bud, LFM_bud) refer to random HW faults. The unavoidable residual risk posed by random HW faults can be reduced by a selection of suitable safety mechanisms, such as the introduction of Active Separating and Connecting Elements and/or prediction mechanisms in line with a failure prediction. The need to introduce safety mechanisms – in addition to the condition of implementing the required systematic integrity - arises from the target values of the derived metrics, which can usually not be achieved without safety mechanisms. An alternative option for achieving the target values regarding random hardware faults is the introduction of redundancy structures.

Chapter 5.4. below describes how the functional safety requirements at component level can be derived from the functional safety requirements at the level of the electrical power supply. The decomposition and allocation of the functional safety requirements to the components of the electrical power supply is performed on the basis of a specifically selected electrical power supply topology as described in the example in Annex D. In doing so, a component can be allocated functional safety requirements from various functional safety requirements of the electrical power supply.

5.4 Allocation of the Requirements and Goals to the EBN Elements and Components

In this chapter, the safety requirements at component level are derived from the functional safety requirements at the electrical power supply level. Table 3 contains an overview of the requirements allocation and decomposition for the components of the EBN. This overview reveals that the components are usually allocated functional safety requirements from various functional safety requirements of the electrical power supply. For Active and Passive Sources, requirements from

EBN-FSR 1.3 Independence may have to be taken into account, despite the fact that these are only available in one of the channels respectively. This requirement means that a DFA must be used to check whether the sources of the EBN channels are sufficiently independent of each other. The requirement of a DFA may, in turn, result in the need for a diverse implementation of the components. Alternatively, a requirements decomposition may be dispensed with and the initial ASIL be allocated to both homogenous redundant sources of the EBN channels.

Component looked at	EBN-FSR 1.1.1 power feed	EBN-FSR 1.1.2 power distribution	EBN-FSR 1.1.3 freedom from interference	EBN-FSR 1.3 independence
Active Sources (6.1)	X	-	X	X
Passive Sources (6.2)	X	-	X	X
Active Separating and Connecting Elements (6.3)	-	X	X	X
Passive separating and connecting Elements (6.4)	-	X	X	X
QM and SR-Loads (6.5)	-	-	X	X
Energy Management (6.6)	X	X	X	X

Tab. 3: Overview of the allocation and decomposition of functional requirements at component level for EBN channel 1

Below, the individual components of the Electrical Power Supply System are described in more detail:

Active Sources [AQ] (cf. chapter 6.1):

Active Sources derive their requirements from EBN-FSR 1.1.1 for the safe provision of energy and power for SR-Maneuvers of the respective operating condition, e.g. to implement the Minimal Risk Maneuvers (MRM) or a double lane change. Furthermore, requirements to avoid interference from EBN-FSR 1.1.3 must be taken into consideration. If the same Active Sources are used for both EBN channels, additional requirements from EBN-FSR 1.3 must be taken into account due to the existence of a homogeneous redundancy.

Note: In case of a homogeneous redundancy of the Active Sources of both EBN channels, a decomposition of the requirement to provide energy and power may not be possible, cf. chapter 4.2.2.

Passive Sources [PQ] (cf. chapter 6.2):

Passive Sources draw their requirements also from EBN-FSR 1.1.1 for the safe provision of energy and power for SR-Maneuvers of the respective operating condition, e.g. to implement the Minimal Risk Maneuver (MRM) or a double lane change. Furthermore, requirements to avoid interferences from EBN-FSR 1.1.3 must be taken into consideration. If the same Passive Sources are used for both EBN channels, additional requirements from EBN-FSR 1.3 must be taken into account due to the existence of a homogeneous redundancy.

Note: In case of a homogeneous redundancy of the Passive Sources of both EBN channels, a decomposition of the requirement to supply energy and power may not be possible, cf. chapter 4.2.2.

Active Separating and Connecting Elements [ATV] (cf. chapter 6.3):

ATVs draw their requirements path-specifically from the electrical power supply requirement for safe power distribution, cf. EBN-FSR 1.1.2. The ASIL integrity for the safe supply must be assessed path-specifically, depending on the connected SR-Loads. A safety-relevant vehicle with integrity ASIL B(D) connected via one channel, for example, passes this requirement on to both the path-selective active separating and connecting Element and to the corresponding wire, the passive separating and connecting Element. Furthermore, requirements for the avoidance of interferences from EBN-FSR 1.1.3 must be taken into consideration.

If ATVs are used to ensure sufficient independence of both electrical power supply channels – e.g. the terminals Kl30_s1 and Kl30_s2 –, additional requirements from EBN-FSR 1.3 Independence must be taken into consideration (cf. chapter 4.2.1).

Passive separating and connecting Elements [PTV] (cf. chapter 6.4):

Passive separating and connecting Elements draw their requirements path-specifically from the electrical power supply requirement for safe power distribution, cf. EBN-FSR 1.1.2. The ASIL integrity for the safe supply must be assessed path-specifically, depending on the connected SR-Loads. A safety-relevant vehicle with integrity ASIL B(D) connected via one channel, for example, passes this requirement on to both the path-selective active separating and connecting Element and to the corresponding wire, the passive separating and connecting Element. Furthermore, requirements for the avoidance of interferences from EBN-FSR 1.1.3 must be taken into consideration.

QM and SR-Loads [BNL] (cf. chapter 6.5):

QM and SR-Loads constitute both a requirements provider and a requirements receiver for the EBN. QM and SR-Loads draw their requirements from EBN-FSR 1.1.3 Freedom from Interference. As a result, due consideration must be given to the fact that SR-Loads should implement freedom from interference at the same level of ASIL integrity at which they demand a safe supply from the EBN, cf. chapter 4.2.3.3. If the loads are connected to both electrical power supply channels – e.g. the terminals Kl30_s1 and Kl30_s2 -, additional requirements from EBN-FSR 1.3 must be taken into account as faults of the control unit may lead to a violation of the requirement of sufficient independence of both EBN channels, cf. chapter 4.2.2.

Energy Management [EM] (cf. chapter 6.6):

The Energy Management usually consists of many functional modules whose implementation is OEM-specific. Therefore, no general statement can be made within the scope of this document. A function-specific effects analysis of the Energy Management must be performed.

Note on competing safety requirements:

A closer look at the component requirements may reveal competing safety requirements for individual components, depending on the operating conditions. It is important to ensure that the safe state can be upheld for all safety requirements. In situations where this is not possible, rephrasing the safety requirements or a timely reaction at system level, such as a warning or a change of the operating condition to an operating condition with lower availability requirements placed on the EBN, may result in an inevitable Safety Goal violation no longer constituting a hazard.

Example: An ATV receives a safety requirement from EBN-FSR 1.1.2 to ensure power distribution with ASIL B and a safety requirement from EBN-FSR 1.1.3 to ensure freedom from interference with ASIL C. These initially conflicting requirements can be resolved by differentiating the operating conditions by means of the measured current value:

- The safety requirement to ensure power distribution only applies in a closely specified current value range
- Ensuring freedom from interference only applies when a much higher threshold value is exceeded.

Consequently, the safe state is dependent on the current and can be defined consistently for all safety requirements.

In chapter 6 below, the functional safety requirements of the aforementioned components are specified as generic component requirements. In doing so, requirements are distinguished according to the requirement sources introduced in chapter 5.2.

- EBN-FSR 1.1.1 Power feed
- EBN-FSR 1.1.2 Power distribution
- EBN-FSR 1.1.3 Freedom from interference
- EBN-FSR 1.3 Independence

In chapter 5.5 and Annex E, quantitative target metrics are derived in accordance with ISO 26262:2018 for the functional safety requirements derived in this chapter.

5.5 Budgeting / Determination of the Target Value of Failure Rates and Metrics

In chapters 5.1 to 5.4, the focus is on the qualitative derivation of systematic ASIL requirements. In addition to the requirements placed on the systematic design and development process, requirements for adherence to the target metrics of random hardware faults must be taken into account. According to ISO 26262-5:2018, the metrics PMHF, SPFM and LFM or PMHF_bud, SPFM_bud and LFM_bud must be allocated as attributes of the Safety Goals and safety requirements.

The derivation of the target metrics follows the scheme of the qualitative derivation of systematic ASIL requirements:

- In case of an allocation (without use of redundancy), the PMHF of a requirement will be divided, in a first approximation, between its subrequirements in such a way that the sum of the PMHF values of the subrequirements matches the PMHF of the original requirement. In case of allocations, the requirements regarding relative metrics (SPFM and LFM) are typically passed on unchanged from the original requirement to the subrequirements.
- In case of decomposition, the original requirement is implemented according to chapter 4.2 by sufficiently independent subrequirements. Through this redundancy, a higher PMHF budget can usually be reserved for the subrequirements. In the course of the decomposition, the LFM of the original requirement usually becomes the SPFM of the subrequirement. The LFM of the subrequirement cannot be derived generically from the original requirement and will therefore not be looked at in detail.

According to ISO 26262-9:2018, 5.4.5, due consideration must be given to the fact that the target metrics of the original requirement must still be achieved both by the application of the ASIL allocation and the ASIL decomposition. As this constitutes the only requirement placed on budgeting the ISO 26262:2018 metrics, there are degrees of freedom within the scope of developing the safety concept. Therefore, the component requirements for the EBN components described in chapter 6 are not just dependent on the EBN architecture but also specific to vehicle manufacturers and individual projects.

Note: If a fault is detected in one of the redundant EBN channels and a transition to a safe state has been initiated, the probability of a fault in the faultless EBN channel must be sufficiently unlikely for the duration of the transition to a safe state (EOTTI), cf. chapter 4.2.3.5.

In order to allow for the development of industrial standard EBN components, proposals are submitted in Annex E for allocating the ISO 26262:2018 target metrics to the Safety Goals and requirements described in chapter 5.2. In doing so, a distinction is made as to

- whether the focus is exclusively on the capability of the EBN for the ASIL D compliant supply of the SR-Vehicle-Function ADS according to ADS-SG 1 or
- whether, in addition, the basic EBN has ASIL B or ASIL C capability.

The strategy of providing the basic EBN with ASIL B or ASIL C capability allows, on the one hand, for synergies between manual and automated driving for joint use of the basic EBN Kl30_s while, on the other hand, allowing for manual driving after failure of the redundant ADS terminal Kl30_s2.

Note: The "basic EBN" is the electrical power supply for implementation of manual driving vehicle functions. This electrical power supply typically has only one safety-relevant terminal Kl30_s to supply consumers that also place safety-relevant availability requirements on the electrical power supply during manual driving (e.g. electronic steering and braking assistance, lights & visibility).

6. Functional Safety Requirements for Elements and Components

In chapter 6, the functional safety requirements are specified as generic requirements for the Elements and components of an electrical power supply. In the process, competing safe states may arise in the FSRs that are allocated to an Element or a component. These competing target conditions can occur both within the EBN safety concept and in the interaction with other safety concepts (e.g. intrinsic protection of the component).

These competing safe states must be assessed in the safety concept.
Ideally, different operating conditions and ambient conditions can be defined in which an unambiguous safe state of the Element can be allocated. Thus, a conflict of the competing safe states can be resolved. If the ambient condition cannot be clearly defined due to faults, this must be taken into account in the context of the safety concept and the safe states of the Elements must be assessed for this case and prioritized.
In addition to the defined safe states of the Element, it may be necessary – from a safety concept perspective – to report the fault status of the Element to a Higher-Level Instance in order to initiate an EO. Using this fault detection and warning strategy ensures that the faulty operation with unclear operating/ambient conditions is limited in time by the EOTTI, thus staying below the acceptable residual risk.
In case of FSRs that include availability requirements, a determination of the safe state at Element/component level is not possible. A violation of the FSR always results in an impairment of the Safety Goal or the overall system integrity and requires an EO. Therefore, Element-specific requirements that are relevant to availability always require the nominal function as a safe state. In case of FSRs regarding freedom from interference, a safe state will be specified analogous to classic Fail-Passive safety concepts.

In this chapter, FSRs will be described for the following Elements and components:

- Active Sources (6.1),
- Passive Sources (6.2),
- Active Separating and Connecting Elements (6.3),
- Passive separating and connecting Elements (6.4),
- QM and SR-Loads (6.5) and
- Energy Management (6.6).

In doing so, functional safety requirements are distinguished in accordance with the requirement sources introduced in chapter 5.2:

- EBN-FSR 1.1.1 Power feed,
- EBN-FSR 1.1.2 Power distribution,
- EBN-FSR 1.1.3 Freedom from interference, and
- EBN-FSR 1.3 Independence.

The FSRs are presented in the following uniform structure:

Attribute	Explanation
Requirement	Functional Safety Requirement placed on the Element (nominal function)
Time interval	Timing requirement placed on the Element for the nominal function, e.g. FHTTI or MPFHTTI
Safe state of the Element	Safe state of the Element from the perspective of this FSR. Competing FSRs and the resulting competing target conditions of the Element are not taken into account here (cf. chapter 5.4 and introduction to chapter 6).
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Reaction to be produced by the Element to transition the EBN to a safe state, after the original function of the Element can no longer be fully implemented. The timing requirement for this is defined in the safety concept and is part of the budget of the EOTTI.
Integrity	Recommendation for the minimum integrity level (ASIL) of the nominal function
Mode	Driving condition in which the requirement is valid
Applicability to variants	Variants for which the requirement is valid
Derived from	Reference to the higher-level requirement of the safety concept
Comment	Additional notes

6.1 Active Sources

Active Sources are fundamental to the EBN safety concept for SR-Vehicle-Functions. At this point, the generic functional safety requirements are specified in such a way that an Active Source with capability according to the requirements is essentially suitable for use in the context of safety concepts developed on the basis of the VDA 450 recommendation.

6.1.1 Definition

Active Sources are components that provide energy to the electrical power supply (channel). This includes, inter alia:

- Generators
- DC/DC converters

6.1.2 Types/Variants

In the recommendation, a distinction is made between four different Active Sources in respect of their use cases.

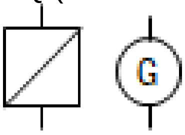
#	Type	Freedom from interference	Availability
1	AQ	Yes (inherent due to design or location)	No

2	AQ-R	Yes (through Safety Mechanism)	No
3	AQ[SR]-ON	Yes	Yes, active in nominal operation, e.g. for hot redundancy
4	AQ[SR]-SBY	Yes	Yes, inactive in nominal operation, e.g. for cold redundancy

Tab. 4: Types/variants of Active Sources

Type 1)
Non availability-relevant Active Source, which is free from interference due to its design or location.

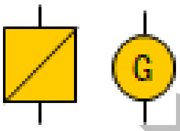
AQ (Active Source)



This variant represents Active Sources, whose supply of energy or power is not included in an energy or power balance for safety-relevant functions and which, due to their design or location, do not include sources of faults within the scope of the EBN safety concept.

Type 2)
Non availability-relevant Active Source, which implements technical safety mechanisms for freedom from interference.

AQ-R (Active Source, free from interference)

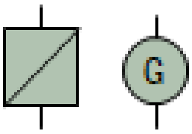


This variant represents Active Sources, whose supply of energy or power is not included in an energy or power balance for safety-relevant functions. However, due to its capability a fault (e.g. Short Circuit) may lead to the Active Source having a detrimental effect on the safety-relevant electrical power supply, thus potentially resulting in a violation of a Safety Goal.

The corresponding fault modes and sources of faults must be determined by means of a pertinent safety analysis and be remedied accordingly.

Type 3)
Availability-relevant Active Source, permanently switched on.

AQ[SR]-ON (Active Source, relevant to availability, default "On")

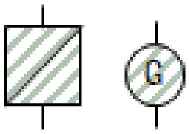


This variant of Active Source is characterized by being an availability-relevant Element of the safety concept. The supply of power and the capability are included in the power and energy balances for the safety-relevant functions.

Active Sources of this variant must ensure their freedom from interference with the power supply.

Type 4)
Availability-relevant Active Source as a switchable system.

AQ[SR]-SBY (Active Source, relevant to availability, default "Standby")



This variant of Active Sources is characterized by being an availability-relevant Element of the safety concept. The supply of power and the capability are included in the power and energy balances for the Safety-Relevant Function.

During operation, the Active Source is not switched on. Within the scope of the safety concept, it is switched on within the FHTI of a fault requiring compensation. An AQ[SR]-SBY therefore constitutes a cold redundancy.

Active Sources of this variant must ensure freedom from interference with the power supply, both in standby and when activated, i.e. switched on.

6.1.3 Functional Requirements

The safety requirements listed here for the Active Sources (DC/DC converter and generators) are described generically and may have to be amended and/or extended for the concrete architecture and the respective safety concept.

When using generators, it is expedient to allocate the safety mechanisms to other Elements such as higher-level diagnosis and control units (e.g. engine control unit) and/or to external separating Elements.

6.1.3.1 Requirements resulting from Availability

Active Sources may be part of interconnected sources within an electrical power supply channel. In this case, the function "supply power" can be decomposed to subfunctions.

Fulfilling the Safety Goal "power feed" is usually subordinate to other protective Safety Goals (e.g. avoidance of overvoltage on safety-relevant electrical power supply). When designing the component safety concept, this must be taken into consideration for both the systematic and the quantitative analysis of faults.

AQ-FSR 1:	When the operation of an SR-Vehicle-Function or corresponding operational parameters are communicated, the AQ shall supply a defined power at the safety-relevant power interfaces for a defined period of time. Note 1: The power to be supplied and the corresponding period of time is to be defined by the respective safety concept. Note 2: The basis for the implementation is the Functional Safety Requirement AQ-FSR 2 (notification regarding capability, detection of latent faults).

	Note 3: The defined profile of the power to be supplied contains various load scenarios such as energy and power requirements (e.g. Continous, Peak and MRM). Note 4: In case of a DC/DC converter, it is assumed that the corresponding amount of energy and power is available at the input interface in the specified functional range, with the pertinent level of integrity. Note 5: Possible restrictions of the dynamics (e.g. when using a generator) must be taken into account.
Time interval	FHTTI of the Element according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3)
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Supply of the available residual power/energy and notification of restricted functionality to the Higher-Level Instance within a timeframe defined in the safety concept
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	AQ[SR]-ON, AQ[SR]-SBY
Derived from	EBN-FSR 1.1.1
Comment	*Always necessary in case of availability requirement

AQ-FSR 2:	The Active Source must monitor its ability to supply the required power at the safety-relevant power interfaces and predict any restrictions in the power feed (e.g. by thermal derating) and notify the Higher-Level Instance within the defined prediction period.
Time interval	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3)
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of a loss of the prediction Note 1: The required power supply ensues from the system design regarding the time-power requirement for the MRM and the other defined SR-Maneuvers Note 2: In case of a generator without a communication interface, this requirement applies to the control unit of the generator.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode

Applicability to variants	AQ[SR]-ON, AQ[SR]-SBY
Derived from	EBN-FSR 1.1.1
Comment	The definition of the prediction period must be derived from the safety concept of the vehicle. The report to the Higher-Level Instance should contain not just the predictive information regarding the power feed, but also the current status. Unpredictable faults and reactions of competing Safety Goals cannot be part of the prediction. *Always necessary in case of availability requirement

6.1.3.2 Requirements resulting from Freedom from Interference

AQ-FSR 3:	The Active Source must restrict the power consumption from the safety-relevant power interfaces to a maximum value, if it is notified of safety-relevant vehicle functions being exercised or receives the corresponding operating parameters (e.g.: boost avoidance / restriction, faulty power consumption). Note 1: The restriction of the power consumption is to be defined by the respective safety concept. Note 2: It may be necessary to also restrict the power consumption at potential interfaces with the logic supply, if the safety-relevant Electrical Power Supply Systems require balancing of the capability to consume and provide power.
Time interval	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3)
Safe state of the Element	Interruption of the power consumption Note: The prevention of a faulty power consumption can be implemented by setting up an Emergency Operation strategy, which guarantees a power feed on the safety-relevant interfaces, or alternatively by interrupting operations. The concrete strategy must be coordinated in the context of the safety concept.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to other variants	AQ-R, AQ[SR]-ON, AQ[SR]-SBY
Derived from	EBN-FSR 1.1.3
Comment	N/A

AQ-FSR 4:	The Active Source shall prevent an exceedance of the maximum permissible voltage at its safety-relevant voltage interfaces caused by AQ internal faults.
Time intervals	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3)
Safe state of the Element	Shutdown of the power feed
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	AQ-R, AQ[SR]-ON, AQ[SR]-SBY
Derived from	EBN-FSR 1.1.3
Comment	Overvoltage may be caused by internal or external faults. The corresponding safety concept of the component can only take into account the internal sources of faults when analyzing faults. However, the coordination of the EBN safety concept should also take into account the general reaction to high voltages at the safety-relevant voltage interfaces. For this purpose, this requirement can be implemented at multiple levels for different permissible voltage and time values.

AQ-FSR 5:	The Active Source shall prevent a voltage below the minimum permissible threshold at its safety-relevant voltage interfaces caused by AQ internal faults. Note 1: Switching off the power consumption (e.g. in case of low voltage caused and detected by the Active Source) ensures a restriction to a value above the minimum value. Note 2: This also includes a prevention of exceeding a specified energy flow to ground.
Time interval	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Safe state of the Element	Fault-specific, either separation or shutting down (cf. Note 1 and Note 2 in AQ-FSR 5)
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)

Mode	Driving Mode
Applicability to variants	AQ-R, AQ[SR]-ON, AQ[SR]-SBY
Derived from	EBN-FSR 1.1.3
Comment	Low voltage may be caused by internal or external faults. The corresponding safety concept of the component can only take into account the internal sources of faults when analyzing faults. However, the coordination of the EBN safety concept should also take into account the general reaction to low voltages at the safety-relevant voltage interfaces. For this purpose, this requirement can be implemented at multiple levels for different permissible voltage and time values.

AQ-FSR 6:	The Active Source must prevent the generation of an output frequency or amplitude outside the specification range, generated by itself.
Time interval	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Safe state of the Element	Shutdown of the power feed
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	AQ-R, AQ[SR]-ON, AQ[SR]-SBY
Derived from	EBN-FSR 1.1.3
Comment	N/A

6.2 Passive Sources

Passive Sources are fundamental to the EBN safety concept for SR-Vehicle-Functions. At this point, the generic functional safety requirements are specified in such a way that a Passive Source, with capability according to the requirements, is essentially suitable for use in the context of safety concepts developed on the basis of the VDA 450 recommendation.

6.2.1 Definition

Passive Sources are components of the electrical power supply system that are used to store energy. This includes, inter alia:

- Batteries (e.g. rechargeable accumulators such as lead-acid batteries, lithium-ion-batteries),
- Power capacitors (e.g. SuperCaps, EDLC),

6.2.2 Types/Variants

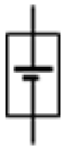
In this recommendation, a distinction is made between four different Passive Sources in terms of their use cases.

#	Type	Freedom from interference	Availability
1	PQ	Yes (inherent by design)	No
2	PQ-R	Yes (by Safety Mechanism)	No
3	PQ[SR]-ON	Yes	Yes, active during nominal operation, e.g. for hot redundancy
4	PQ[SR]-SBy	Yes	Yes, active during nominal operation, e.g. for cold redundancy

Tab. 5: Types/variants of Passive Sources

Type 1)
Non availability-relevant Passive Source, which is free from interference due to its design.

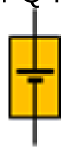
PQ (Passive Source)



This variant represents sources, whose supply of energy or power is not included in an energy or power balance for safety-relevant functions and which, due to its design, does not include failure modes within the scope of the EBN safety concept.
A failure mode can usually be excluded if the capability and energy capacity are considerably lower than the power or energy requirement of the consumer collective. This can be ensured, for example, by low power in the mW range and a corresponding connection with a small cable cross-section.
Freedom from interference must be determined by means of suitable fault analyses.

Type 2)
Non availability-relevant Passive Source, which implements technical safety mechanisms for freedom from interference.

PQ-R (Passive Source, free from interference)

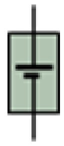


This variant represents Passive Sources whose supply of energy or power is not included in an energy or power balance for safety-relevant functions. However, due to its capability a fault (e.g. Short Circuit) may lead to the Active Source having a detrimental effect on the safety-relevant electrical power supply. This category also includes Passive Sources that may generate a sudden load increase for the respective safety-relevant source due to an unplanned shutdown.

The corresponding failure modes must be determined by means of a pertinent safety analysis.

Type 3)
Availability-relevant Passive Source permanently switched on

PQ[SR]-ON (Passive Source, relevant to safety, default "On")



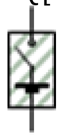
This variant of Passive Sources is characterized by being an availability-relevant Element of the safety concept. The capabilities to supply energy and power are considered in the power and energy balances for the safety-relevant functions.

Due to the availability requirements, requirements for the avoidance of interferences automatically arise, too.

Passive Sources of this variant must ensure their freedom from interference with the power supply.

Type 4)
Availability-relevant Passive Source as a switchable system

PQ[SR]-SBY (Passive Source, safety-relevant, default "Standby")



This variant of Passive Sources is characterized by being an availability-relevant Element of the safety concept. The supply of power and the capability are included in the power and energy balances for the Safety-Relevant Function.
Due to the availability requirements, requirements for the avoidance of interferences automatically arise, too.
During nominal operation, the Passive Source is not switched on. Within the scope of the safety concept, it is switched on within the FHTI if a fault in the source occurs.

6.2.3 Functional Requirements

The safety requirements listed here for the Passive Sources are described generically and may have to be amended and/or extended for the concrete architecture and the respective safety concept.

6.2.3.1 Requirements resulting from Availability

Passive Sources that serve as Elements to ensure power availability within the scope of a safety concept and are therefore to be allocated to the variant PQ[SR]-ON or PQ[SR]-SBy must ensure not just freedom from interference but also availability requirements.
Passive Sources may be part of interconnected sources within an electrical power supply channel. In this case, the function "supply power" can be decomposed to subfunctions. The FHTI of a fault in interconnected sources is then dependent on the forecast horizon that is derived from the duration of the maneuver to adopt a safe state, the diagnostic interval and the Diagnostic Coverage of the individual elements supplying power.

PQ-FSR 1:	The Passive Source must forecast its power capability and its energy content regarding energy output and energy consumption and communicate those to the Higher-Level Instance at regular intervals. Note: The capability and energy content are predicted at least for the performance of the SR-Maneuver and the MRM plus the MPFDTI
Time interval	MPFDTI freely selectable, usually around 1 s.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of restricted functionality to the Higher-Level Instance or shutdown of communication
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	PQ[SR]-ON, PQ[SR]-SBy
Derived from	EBN-FSR 1.1.1
Comment	There are approaches in which the forecast functions are standardized (cf. Annex G). *Always necessary in case of availability requirement

PQ-FSR 2:	A Passive Source with an integrated separating Element must ensure that the transmission of the specified power and energy is not interrupted unintentionally. Note 1: An intentional separation must be announced with a predefined lead time and may only be performed after expiry of this lead time. Note 2: The predefined lead time usually covers the duration of the SR-Maneuver and the MRM.
Time interval	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3) Also applies to all subsequent requirements.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Transmission of the maximum possible power/energy and/or switch-on attempt after unplanned opening of the separating Element. Notification of functional restriction to the Higher-Level Instance or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode

Applicability to variants	PQ[SR]-ON, PQ[SR]-SBy Note: Passive Sources of the classification PQ[SR]-SBy always have a separating Element due to their operating mode and must implement this requirement as a matter of principle.
Derived from	EBN-FSR 1.1.1
Comment	* Always necessary in case of availability requirement

PQ-FSR 3:	The Passive Source shall supply power and energy on the basis of a communicated or diagnosed first fault in the interconnected sources within the FRTI of the interconnected sources. Note 1: A diagnosed first fault is deemed to exist when the specified operating range of the safe electrical supply is not met and this is detected by the Passive Source. Note 2: A communicated first fault can be signaled by a Higher-Level Instance via a communication bus. Note 3: The supply of energy and power by the PQ must be ensured within the FHTTI after a shortfall in the signaled specified voltage range.
Time interval	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3) Also applies to all subsequent requirements.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Transmission of the maximum possible power/energy and/or switch-on attempt after unplanned opening of the separating Element. Notification of functional restriction to the Higher-Level Instance or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode, after detection of first fault in the interconnected sources.
Applicability to variants	PQ[SR]-SBy
Derived from	EBN-FSR 1.1.1
Comment	N/A

6.2.3.2 Requirements resulting from Freedom from Interference

Passive Sources that are classified as variants PQ-R, PQ[SR]-ON or PQ[SR]-SBy must ensure freedom from interference with the power supply.
Note 1: The safety functions described refer to an energy storage device (accumulator) with a diagnostic unit and an optional separating Element, which is actuated directly by the diagnostic unit.

Note 2: The diagnostic unit and, if present, the separating Element may coexist in one common component (e.g. in case of lithium-ion batteries) or in separate components (e.g. in case of lead acid batteries).

PQ-FSR 4:	When a shutdown becomes necessary, the Passive Source must give advance notice to the Higher-Level Instance. The time interval between the advance notice and shutdown must be at least as long as the duration of the MRM. Note 1: Requirement applies if overvoltage/undervoltage may occur due to the shutdown. Note 2: A corresponding overvoltage/undervoltage can usually only occur if high load currents are drawn from the supply system.
Time interval	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3) Also applies to all subsequent requirements.
Safe state of the Element	Fault must be avoided by means of Element design.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Switched on for the maximum permissible duration or stepwise shutdown of the component. Report of functional restriction to the Higher-Level Instance or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	PQ-R
Derived from	EBN-FSR 1.1.3
Comment	N/A

PQ-FSR 5:	The Passive Source must prevent the occurrence of a voltage outside the specified voltage/time interval at its power interfaces, caused by the Passive Source itself.
Time interval	FHTTI of the Elements according to the timeframe of the performance requirements, taking into consideration the voltage drop via the wiring harness. (cf. chapter 4.1.3) Also applies to all subsequent requirements.
Safe state of the Element	Fault must be avoided by means of Element design.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	If possible, the fault should be separated or remedied. If a separating Element exists and a short-circuit was detected, the Passive Source must be shut down. Report of functional restriction to the Higher-Level Instance or shutdown of communication.

Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	PQ-R, PQ[SR]-ON, PQ[SR]-SBy
Derived from	EBN-FSR 1.1.3
Comment	N/A

6.3 Active Separating and Connecting Elements

ATVs are fundamental to the EBN safety concept for SR-Vehicle-Functions. At this point, the generic functional safety requirements are specified in such a way that an active separating and connecting Element, with capability according to the requirements, is essentially suitable for use in the context of safety concepts developed on the basis of the VDA 450 recommendation.

6.3.1 Definition

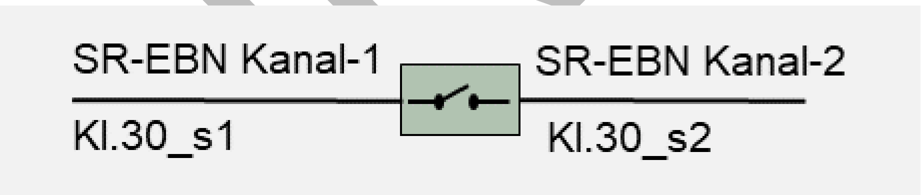
The ATVs are safety Elements added to the Electrical Power Supply System, which act as a Safety Mechanism to separate and connect the Elements in the Electrical Power Supply System with corresponding integrity.
This includes, inter alia:

- DCDC converter
- Semiconductor-based switches
- Relays

6.3.2 Types/Variants

In this recommendation, a distinction is made between six different ATVs.

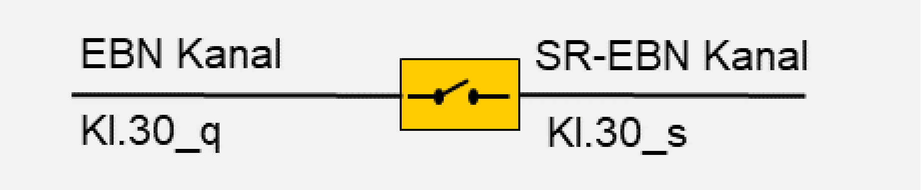
Type 1) Active separating and connecting Element EBN[SR]-EBN[SR]:
Separating and connecting Element between two safety-relevant EBN channels.



Requirement: Ensuring sufficient freedom from interference and independence between the safety-relevant EBN channels. Depending on the safety concept, the Element also serves to safely conduct energy.

Note: Use of this Element with a safety-relevant availability requirement of the connection is not possible in case of a decomposition between SR-EBN channel 1 and SR-EBN channel 2, as the independence requirements that this Element must implement with the initial ASIL rating compete with the safety requirements for availability.

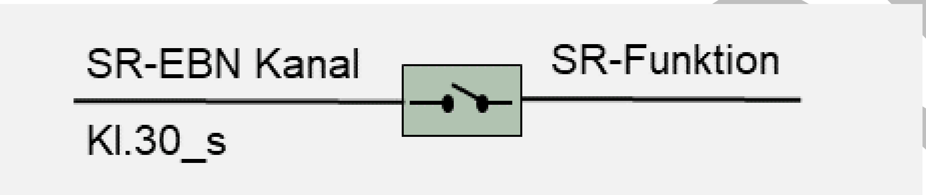
Type 2) Active separating and connecting Element EBN[QM]-EBN[SR]:
Separating Element between a QM-EBN channel and a safety-relevant EBN channel.



Requirement: Ensuring freedom from interference from the QM-EBN channel to the safety-relevant EBN channel.

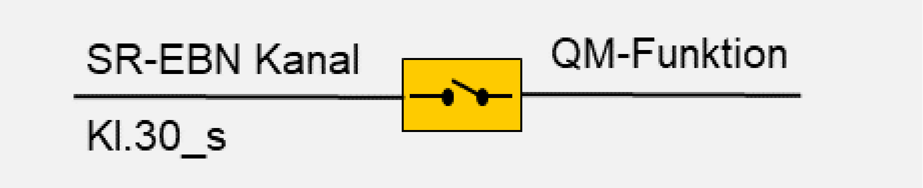
Note: If the QM-EBN Channel lays between two SR-EBN Channels, as illustrated in the use case in Annex D, the ATVs which are the interfaces to both SR-EBN Channels must ensure sufficient independence and freedom from interference between the safety-relevant EBN channels.

Type 3) Active separating and connecting Element EBN[SR]-L[SR]:
Separating and connecting Element between a safety-relevant channel and a safety-relevant load.



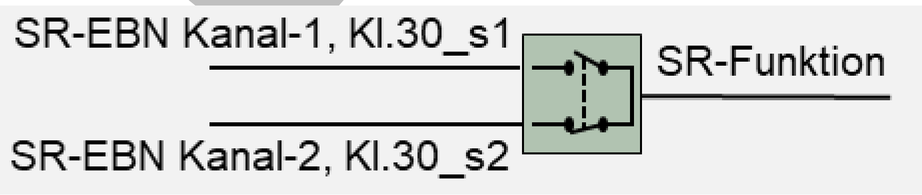
Requirement: Ensuring freedom from interference from the safety-relevant load incl. its connection (cf. chapter 6.4) to the safety-relevant EBN channel plus ensuring sufficient supply of the safety-relevant loads by the safety-relevant EBN channel.

Typ 4) Active separating and connecting Element EBN[SR]-L[QM]:
Separating Element between a safety-relevant EBN channel and a non safety-relevant load



Requirement: Ensuring freedom from interference of the non safety-relevant load incl. its connection (cf. chapter 6.4) on the safety-relevant EBN channel.

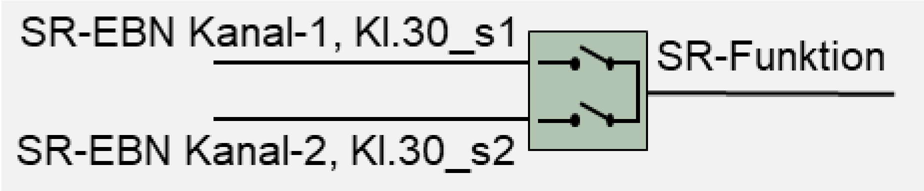
Type 5) Active separating and connecting Element EBN[SR]-L[SR]-EBN[SR]:
Connecting Element designated as Y1 between two safety-relevant EBN channels and a safety-relevant load.
Y1 switch EBN[SR]-L[SR]-EBN[SR]– only one power supply connection active during normal operation.



Requirement: Ensuring sufficient power supply of the safety-relevant load by means of one of the two safety-relevant EBN channels (only ever one connection to one of the two safety-relevant channels). In case of a fault of the supplying EBN channel, this connection to the load must be separated and the power supply for the load ensured by another EBN channel within the FTTI.

Furthermore, freedom from interference from the safety-relevant load incl. its connection (cf. chapter 6.4) to the safety-relevant EBN channels and the freedom from interference and sufficient independence of the safety-relevant EBN channels must be ensured.

Type 6) Active separating and connecting Element EBN[SR]-L[SR]-EBN[SR]:
Connecting Element between two safety-relevant EBN channels and a safety-relevant load.
Y2 switch EBN[SR]-L[SR]-EBN[SR] – both power supply connections simultaneously active during normal operation



Requirements: Ensuring sufficient power supply of the safety-relevant load by means of both safety-relevant EBN channels. In case of a fault of one of the two EBN channels, this connection to the load must be separated and the power supply for the load still be ensured by the other SR-EBN Channel.
Furthermore, freedom from interference from the safety-relevant load incl. its connection (cf. chapter 6.4) to the safety-relevant EBN channels and the freedom from interference and sufficient independence of the safety-relevant EBN channels must be ensured.

6.3.3 Functional Requirements

The safety requirements listed here for the ATVs are described generically and may have to be amended and/or extended for the concrete architecture and the respective safety concept.

6.3.3.1 Requirements resulting from Availability

ATV-FSR 1:	The ATV shall ensure the transition of energy and power between the safety-relevant interfaces, within the specified range.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply VDA recommendation: Cf. performance requirements in chapter 4.1.3
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Provision of the available residual power/energy* and Report of restricted functionality to the Higher-Level Instance within a timeframe specified in the safety concept
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	EBN[SR]-L[SR]; EBN[SR]-EBN[SR]**; Y1***; Y2
Derived from	EBN-FSR 1.1.2

Comment	* Always necessary in case of availability requirement ** If a topology is used that uses energy sources/ storage in the respective EBN channel which can supply power with a sufficient level of integrity, there is no need for a safety requirement of the active separating and connecting Element in respect of the power transmission. *** Switch over energy supply to the load, if a second EBN[SR] is within the specification

ATV-FSR 2:	A diagnosis is required to confirm that the active separating and connecting Element is still able to conduct energy (to avoid latent faults ISO 26262-04:2018, 6.4.2.5).
Time interval	N/A
Safe state of the Element	N/A
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	According to the table for avoiding latent faults (ISO 26262-04:2018, 6.4.2.5) and dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept Minimum: ASIL A
Mode	At least once per driving cycle and upon request
Applicability to variants	EBN[SR]-L[SR]; EBN[SR]-EBN[SR]*; Y1; Y2
Derived from	ATV-FSR 1
Comment	* If a topology is used that uses energy sources/ storage in the respective EBN channel which can supply power with a sufficient level of integrity, there is no need for a safety requirement of the active separating and connecting Element in respect of the power transmission.

6.3.3.2 Requirements resulting from Freedom from Interference

ATV-FSR 3:	In order to protect the SR-EBN Channel, the active separating and connecting Element shall prevent the transfer of power and energy to the connected Element (QM-Load / SR-Load / EBN load / SR-EBN Channel), if a specified short-circuit is detected at the connected Element. Note: Concrete values are derived from the Conditions of Use.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply VDA recommendation: 100-500 µs; cf. performance requirements in chapter 4.1.3
Safe state of the Element	open/non-conducting
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.

Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept. VDA recommendation: at least ASIL B(D)
Mode	Driving Mode
Applicability to variants	EBN[SR]-L[QM]; EBN[SR]-L[SR]; EBN[SR]-EBN[SR]; EBN[SR]-EBN[QM]; Y1; Y2
Derived from	EBN-FSR 1.1.3, EBN-FSR 1.3, Conditions of Use
Comment	N/A

ATV-FSR 4:	In order to protect the SR-EBN Channel, the ATV shall prevent the transfer of power and energy to the connected Element (QM-Load / EBN channel / SR-EBN Channel), if the voltage drops below the specified voltage limit. Note: Specific values are derived from the Conditions of Use
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply VDA recommendation: 100-500 µs; cf. performance requirements in chapter 4.1.3 Note: It is recommended to prioritise the over-current disconnect (ATV-FSR 3) to the undervoltage disconnect (ATV-FSR 4).
Safe state of the Element	Open/non-conductive
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept.
Mode	Driving Mode
Applicability to variants	EBN[SR]-L[QM]; EBN[SR]-EBN[SR]; EBN[SR]-EBN[QM]; Y1*
Derived from	EBN-FSR 1.1.3, EBN-FSR 1.3, Conditions of Use
Comment	* Switch over energy supply to the load, if a second EBN[SR] is within the specification

ATV-FSR 5:	In order to protect the SR-EBN Channel, the ATV shall prevent the transfer of energy and power to the SR-EBN Channel, if a specified voltage is exceeded. Note: Concrete values are derived from the Conditions of Use
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply. Cf. performance requirements in chapter 4.1.3
Safe state of the Element	Open/non-conductive*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.

Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept
Mode	Driving Mode
Applicability to variants	EBN[SR]-EBN[SR]; EBN[SR]-EBN[QM]
Derived from	EBN-FSR 1.1.3; EBN-FSR 1.3
Comment	* In case of competing safety requirements (e.g. due to availability requirements of the SR-Load), the target condition of the Element must be specified in the safety concepts and in accordance with vehicle modes.

ATV-FSR 6:	A diagnosis is required to check if the active separating and connecting Element is still able to prevent energy being conducted (to avoid latent faults ISO 26262-04:2018, 6.4.2.5).
Time interval	N/A
Safe state of the Element	N/A
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	According to the table for avoiding latent faults (ISO 26262-04:2018, 6.4.2.5) and dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept Minimum: ASIL A
Mode	At least once per driving cycle and upon request
Applicability to variants	EBN[SR]-L[QM]; EBN[SR]-L[SR]; EBN[SR]-EBN[SR]; EBN[SR]-EBN[QM]; Y1; Y2
Derived from	ATV-FSR 3, ATV-FSR 4, ATV-FSR 5, EBN-FSR 1.1.3, EBN-FSR 1.3
Comment	N/A

ATV-FSR 7:	In order to protect the electrical power supply, it shall be ensured that the ATV does not exceed a specified energy flow to ground.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply. Cf. performance requirements in chapter 4.1.3
Safe state of the Element	Fault must be avoided by means of Element design.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	N/A
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal, the system safety concept and the potential interference with an EBN channel or the entire electrical power supply

Mode	Driving Mode
Applicability to variants	EBN[SR]-L[QM]; EBN[SR]-V[SR], EBN[SR]-EBN[SR]; EBN[SR]-EBN[QM]; Y1; Y2
Derived from	EBN-FSR 1.1.3, EBN-FSR 1.3
Comment	N/A

ATV-FSR 8:	The ATV shall prevent transfer of energy from one electrical power supply to another electrical power supply, if a specified transverse current is exceeded.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply. Cf. performance requirements in chapter 4.1.3
Safe state of the Element	Open/non-conductive*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR.
Integrity	Dependent on the architecture of the electrical power supply / the initial Safety Goal and the system safety concept.
Mode	Driving Mode
Applicability to variants	EBN[SR]-EBN[SR]; EBN[SR]-EBN[QM]; Y1; Y2
Derived from	EBN-FSR 1.1.3, EBN-FSR 1.3
Comment	* In case of competing safety requirements (e.g. due to availability requirements of the SR-Load), the target condition of the Element must be specified in the safety concepts and in accordance with vehicle modes.

6.4 Passive Separating and Connecting Elements

Passive separating and connecting Elements are fundamental to the EBN safety concept for SR-Vehicle-Functions. At this point, the generic functional safety requirements are specified in such a way that a passive separating and connecting Element, with capability according to the requirements, is essentially suitable for use in the context of safety concepts developed on the basis of the VDA 450 recommendation.

6.4.1 Definition

The passive separating and connecting Elements are safety Elements that separate Elements in the electrical power supply as a Safety Mechanism and, if applicable, connect them with integrity.

6.4.2 Types/Variants

Type 1) Electric wires
Connecting Element for the transmission of energy
Requirement: Ensuring sufficient energy transmission from EBN Elements

Type 2) Electric plugs
Connecting Element for the transmission of energy
Requirement: Ensuring sufficient energy transmission from EBN Elements

Type 3) Passive fuses
Separating Element to prevent an energy flow and connecting Element for the transmission of energy
Requirement: Ensuring the separation of an energy flow if currents are outside the specification
Note: The original need for the integration of passive electric fuses is derived from the wire protection. Use for ensuring freedom from interference requires reliable separation within the FHTTI in respect of EBN-FSR 1.1.3 and EBN-FSR 1.2.3.

Type 4) Screw connections
Connecting Element for the transmission of energy
Requirement: Ensuring sufficient energy transmission from EBN Elements

Type 5) Nondetachable electric connections
Connecting Element for the transmission of energy
Requirement: Ensuring sufficient energy transmission from EBN Elements

6.4.3 Functional Requirements

The physical Electrical Power Supply System including the passive separating and connecting Elements constitute a part of the E/E system, whose failure modes can impair the functionality of the E/E system. Therefore, random and systematic faults of the passive separating and connecting Elements must be taken into account for the safety considerations of the E/E system. For this purpose, the failure modes of the separating and connecting Elements must be identified verifiably.

Concomitantly, the fulfillment of requirements for the components must be ensured by a suitable product development and manufacturing process.

The subsequently listed safety requirements for the passive separating and connecting Elements are described generically and may have to be amended for the concrete architecture and the respective safety concept and/or extended.

6.4.4 Requirements resulting from Availability

PTV-FSR 1:	The passive separating and connecting Elements shall ensure the transfer of energy from one safety-relevant Element to another safety-relevant Element, if the operating ranges are within the respective specifications (temperature, voltage, current, vibration, humidity, …). In the process, a maximum voltage drop must not be exceeded for the respective performance requirements (chapter 4.1.3)*.
Time interval	FHTTI dependent on the technical analysis; cf. performance requirements from chapter 4.1.3
Safe state of the Element	Maintaining the nominal function**
Substitute reaction of the Element to fulfill the safety requirements at EBN level	N/A
Integrity	Dependent on the electrical power supply architecture / the initial Safety Goal and the system safety concept
Mode	Driving Mode

Applicability to types	Type 1) Electric wires Type 2) Electric plugs Type 3) Passive fuses Type 4) Screw connections Type 5) Nondetachable electric connections
Derived from	EBN-FSR 1.1.2
Comment	As a recommendation, a derivation to a technical FHTTI should generally be avoided for passive connecting Elements. Open contacts, for example, are permitted on adjacent connecting Elements or their own Element for a certain period of time. *The maximum voltage drop across the specific Element is derived from the total maximum voltage drop across the wiring harness and the sum of the contained Elements for the specific load with the respective performance requirement. **Always necessary in case of availability requirement

6.4.5 Requirement resulting from Freedom from Interference

PTV-FSR 2:	The passive separating and connecting Element shall prevent the transfer of energy to ground or adjacent potentials, both individually and in combination.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply Cf. performance requirements in chapter 4.1.3
Safe state of the Element	Fault must be avoided by means of Element design.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	N/A
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal, the system safety concept and the potential interference with an EBN channel or the entire electrical power supply
Mode	Parking Mode Driving Mode
Applicability to types	Type 1) Electric wires Type 2) Electric plugs Type 3) Passive fuses Type 4) Screw connections Type 5) Nondetachable electric connections
Derived from	EBN-FSR 1.1.3; EBN-FSR 1.3
Comment	As a recommendation, a derivation to a technical FHTTI should generally be avoided for passive connecting Elements, e.g. permitting transfer of energy to adjacent connecting Elements or their own Element for a certain period of time.

6.5 QM and SR Loads

QM and SR-Loads are Elements of the EBN safety concept for SR-Vehicle-Functions that are particularly relevant to freedom from interference. At this point, the generic functional safety requirements are specified in such a way that a QM or SR-Load, with capability according to the requirements, is essentially suitable for use in the context of safety concepts developed on the basis of the VDA 450 recommendation.

6.5.1 Definition

Loads are consumers of electric energy and power in the EBN.

6.5.2 Types/Variants

Type 1) QM-Load

A QM-Load is an electric consumer that is supplied with energy and power from the electrical power supply for the purpose of fulfilling its functions. However, it does not place safety-relevant availability requirements on the power supply. One example of a QM-Load is a load that implements a Fail-Passive function or a non safety-relevant function.

Note: If QM and SR-Functions, whose reciprocal freedom from interference is ensured, are allocated to a load, this is an SR-Load from an EBN perspective.

Type 2) SR-Load:

A safety-relevant load is an electric consumer that implements a subfunction of a Fail-Active SR-Vehicle-Function, such as braking, steering or environment detection. Therefore, the SR-Load allocates a safety-relevant availability requirement to the power supply.

6.5.3 Functional Requirements

Note: The subsequently listed safety requirements for the QM and SR-Loads are described generically and may have to be amended and/or extended for the concrete architecture and the respective safety concept.

QM and SR-Loads can constitute direct E/E functions.

6.5.3.1 Requirements resulting from Availability

N/A

6.5.3.2 Requirements resulting from Freedom from Interference

BNL-FSR 1:	The load shall avoid the transfer of energy to ground or adjacent potentials outside the specification, both individually and in combination.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components for the electrical power supply.
Safe state of the Element	Fault must be avoided by means of Element design
Substitute reaction of the Element to fulfill the safety requirements at EBN level	N/A
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal, the system safety concept and the potential

	interference with an EBN channel or the entire electrical power supply / the use of additional safety Elements
Mode	Parking Mode Driving Mode
Applicability to types	Type 1) QM-Loads Type 2) SR-Loads
Derived from	EBN-FSR 1.1.3; EBN-FSR 1.3
Comment	N/A

BNL-FSR 2:	The load shall prevent/degrade its power consumption if it exceeds the specification or if commanded by a Higher-Level Instance.
Time interval	FHTTI dependent on the technical analysis and the requirements of the safety-relevant components on the electrical power supply.
Safe state of the Element	Switch off component
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the inability to fulfill the FSR
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal, the system safety concept and the potential interference with an EBN channel or the entire electrical power supply / the use of additional safety Elements
Mode	Parking Mode Driving Mode
Applicability to types	Type 1) QM-Loads Type 2) SR-Loads
Derived from	EBN-FSR 1.1.3
Comment	The integrity of the specified energy must be ensured. If a load cannot ensure this, other mechanisms in the vehicle Electrical Power Supply System (e.g. ATVs) must ensure adherence to the required amount of energy.

6.6 Energy Management

The Energy Management is an Element of the EBN safety concept for SR-Vehicle-Functions. At this point, the generic functional safety requirements are specified in such a way that an Energy Management, with capability according to the requirements, is essentially suitable for use in the context of safety concepts developed on the basis of the VDA 450 recommendation.

6.6.1 Definition

The Energy Management is a functional Element of the EBN that coordinates the energy and power supply of the source with the demand of the loads. In addition, it monitors the sources and loads as well as the power and energy distribution in the vehicle.

Whether or not the functional Element is also relevant within the scope of a safety concept for the EBN must be defined specifically in the respective safety concept. Usually, this makes sense in particular for more complex EBN systems where the potentially installed load consumption of an EBN channel is significantly higher than the power feeds (across the entire temperature and charge state range) by the SR sources.

The Energy Management is a SW unit that can access the sensor system and the actuating Elements, makes decisions based on aggregated information and then passes on the respective commands to the individual EBN Elements.

In the context of the EBN safety concept, this SW unit is also called a Higher-Level Instance, to which fault conditions of EBN Elements, for example, are reported.

In the overall system, the Energy Management thus constitutes an intermediate instance which aggregates all fault conditions of the electrical power supply and fault reactions and coordinates them. Accordingly, the next higher instance is a SW unit of an SR-Vehicle-Function, which receives the aggregated information on EBN faults and imitates system reactions that are outside the EBN scope of observation.

6.6.2 Types/Variants

The Energy Management is a very specific Element whose scope is highly dependent on the functional partitioning in the overall system. For this reason, a classification into variants or types is generally not useful.

6.6.3 Functional Requirements

The Energy Management assumes, inter alia, the following functions:

Activation/deactivation of the safety mechanisms:
Usually, monitoring functions of safety concept Elements are only active if there is a corresponding risk (e.g. during active driving). To activate and deactivate the monitoring of individual EBN Elements in a coordinated manner, a corresponding status management (system) is required.

Diagnosis of distributed multiple-point faults in the EBN system:
By aggregating multiple pieces of information from the Elements of the EBN, the Energy Management system can detect a first fault of multiple-point faults at an early stage and initiate a system response. Example: shortfall of the source's capability in case of maximum utilization of the EBN, exceeding the residual load consumption of the EBN Elements, exceeding the operating limits, …

Recording of fault conditions and clustering:
The Energy Management records the fault conditions of the safety concept Elements and sorts these into fault categories. The Energy Management decides which fault reaction is adopted.

Commanding central fault reaction mechanisms:
In a safety concept, the Energy Management can initiate central fault reactions based on its own central diagnoses or aggregated fault conditions (e.g. in case of several independent first faults of a higher order, MPF detected). Examples in case are the commanded load reductions of the consumers, the commanded initiation of single or several ATVs, …

Field monitoring:
The central processing of fault conditions enables the Energy Management to perform specific field monitoring, which aggregates not just the mere information on the faults but also the corresponding information of other control units.

The functions that the Energy Management performs in the process are respective subfunctions of individual safety mechanisms. The functions of the Energy Management often constitute a service that can be used by several safety mechanisms.

The services of the Energy Management also address potential fault patterns that affect the entire EBN system, i.e. freedom from interference as well as safety-relevant aspects. Therefore, a clear distinction between "requirements resulting from availability" and "requirements resulting from freedom from interference" is therefore not possible.

6.6.3.1 Requirements resulting from Availability

EM-FSR 1:	The Energy Management must ensure that all Elements required for a safe provision of energy and power are in a functioning and faultless condition in good time for activation and during the SR driving function operation. Likewise, the respective allocated safety mechanisms must be active and operational.
Time interval	MPFHTTI maximum EOTTI for the respective fault minus the duration of the MRM and the duration of the signal transmission time.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the EM's functional restriction until the nominal function has been restored or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal and the system safety concept
Mode	Driving Mode
Applicability to variants	N/A
Derived from	EBN-FSR 1.1.1, EBN-FSR 1.1.2, EBN-FR 1, EBN-FR 6
Comment	This requirement does not apply if the safety mechanisms of the components are active irrespective of the vehicle's operating mode. *Always necessary in case of availability requirement

EM-FSR 2:	The Energy Management must ensure that the non-availability of the EBN safety mechanisms is reported correctly to the Higher-Level Instance, based on the Element's (fault) condition.
Time interval	MPFHTTI maximum EOTTI for the respective fault minus the duration of the MRM and the duration of the signal transit time.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the EM's functional restriction until the nominal function has been restored or shutdown of communication.

Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal and the system safety concept
Mode	Driving Mode
Applicability to variants	N/A
Derived from	EBN-FR 1, EBN-FSR 1.1.1, EBN-FSR 1.1.2, EBN-FSR 1.1.3
Comment	This requirement does not apply if the safety mechanisms of the components are active irrespective of the vehicle's operating mode. The objective is to avoid false positive reports of the availability of safety mechanisms. *Always necessary in case of availability requirement

EM-FSR 3:	The Energy Management must monitor if the energy and power consumption of the loads is below the forecast energy and power supply of the sources, taking into consideration potential safety mechanisms. Examples of safety mechanisms: commanded degradation functions, voltage-dependent consumer degradation, voltage-dependent separation of consumers and/or QM sub-EBN, activation of "stand-by" power consumers, …
Time interval	This is mere fault detection. The FDTI and MPFDTI is dependent on the respective fault. As the Safety Mechanism can be used to avoid single-point failures, it is recommended to set the MPFDTI lower than the FTTI minus the reaction time. In connection with multiple-point faults, the MPFDTI must be less than the Emergency Operation minus the duration of the planned MRM and the fault reaction.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the EM's functional restriction until the nominal function has been restored or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal and the system safety concept
Mode	Driving Mode
Applicability to variants	N/A
Derived from	EBN-FSR 1.1.1, EBN-FSR 1.1.3
Comment	The objective is to avoid latent faults caused by an insufficient supply of energy or a required energy consumption for the MRM. *Always necessary in case of availability requirements

EM-FSR 4:	The Energy Management must ensure that a reduction of the power and/or energy consumption is requested from the EBN Elements (loads, ATVs or Active Sources, provided they do not function as SR sources). This applies, if one or more faults exist that entail a restriction of the sources' energy and power supply or an unplanned increase of the power or energy consumption of the EBN Elements.
Time interval	This is a mere fault reaction. The FRTI and MFRTI is dependent on the respective fault. As the Safety Mechanism can be used to avoid single-point failures, it is advisable to set the MPFDTI lower than the FTTI minus the detection time.
Safe state of the Element	Maintaining the nominal function*
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Repetition of the request for load reduction from the EBN Elements. Cyclical notification of the Higher-Level Instance about the functional restriction until the nominal function has been restored or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal and the system safety concept
Mode	Driving Mode
Applicability to variants	N/A
Derived from	EBN-FSR 1.1.1, EBN-FSR 1.1.3
Comment	The objective is to avoid latent faults caused by an insufficient supply of energy or a required energy consumption for the MRM. *Always necessary in case of availability requirements

6.6.3.2 Requirement resulting from Freedom from Interference

EM-FSR 5:	The Energy Management must ensure that a fault reaction specified in the safety concept is initiated if the EM receives reports of fault conditions from EBN Elements.
Time interval	MPFHTTI maximum EOTTI for the respective fault minus the duration of the MRM and the duration of the signal transit time.
Safe state of the Element	Shutdown of communication.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Notification of the Higher-Level Instance about the functional restriction until the nominal function has been restored.
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal and the system safety concept
Mode	Driving Mode

Applicability to variants	N/A
Derived from	EBN-FSR 1.1.1, EBN-FSR 1.1.3
Comment	In case of multiple-point faults (connected multiple-point faults or independent multiple-point faults) it is advisable to adjust the fault reaction to the correspondingly increased risk. The objective is to reduce the risk in case of existing multiple-point faults and to reduce design errors at the interfaces of safety concepts. The design of a standardized interface between SR-Vehicle-Functions and the EBN is less prone to errors than the implementation of many interfaces for each EBN Element individually.

EM-FSR 6:	The Energy Management must ensure that the operating time (or, in case of repeated exposition, accumulated operating time across the product life cycle) during Emergency Operation for a specific fault is limited to the respective EOTTI.
Time interval	As the Safety Mechanism refers to a statistical effect resulting from increased error rates caused by faulty systems, exceeding the EOTTI only increases the risk incrementally. It is advisable to limit the MPFHTI to the active driving cycle.
Safe state of the Element	Shutdown of communication.
Substitute reaction of the Element to fulfill the safety requirements at EBN level	Recording of a persistent fault condition. Cyclical report of restricted functionality to the Higher-Level Instance or shutdown of communication.
Integrity	Dependent on the architecture of the electrical power supply, the initial Safety Goal and the system safety concept
Mode	Failure mode
Applicability to variants	N/A
Derived from	EBN-FSR 1.1.1, EBN-FSR 1.1.3
Comment	The objective is avoidance of increased failure rates caused by frequent or long exposition of the Emergency Operation due to an insufficient energy supply for the MRM. Note: The Safety Mechanism addresses primarily Level 3 SR-Vehicle-Functions where the passenger/driver is integrated in the safety concept.

Annex

A. Normative References

A1 Detailed Requirements of the Steering Function Arising from Technical Requirements and Standards

From the current perspective, the following regulatory requirements must be taken into account for the design of the electrical power supply. This collection is by no means exhaustive and reflects the current status of rules and regulations. For a concrete elaboration, a review of the regulations specific to the respective SR-Vehicle-Function must be carried out.

EPS-LR 1	Failures in other systems affecting the energy supply shall not result in a loss of steering as described in the test criteria referenced below.
Source(s)	UN R79, 5.1.10 UN R79, 5.3 (associated test criteria)

The subsequent requirements (EPS-LR 2 and EPS-LR 3) from the current ECE regulations take into account the case of manual driving with steer-by-wire systems. These requirements must be incorporated conditionally for the purpose of the present recommendation; an adaption to automated driving has not been made yet. For automated driving, an energy reserve must be taken into consideration to transition the vehicle to a safe state, cf. also LR-ADS 02 und LR-ADS 03.

EPS-LR 2	In case of steer-by-wire, energy shall be available for 36 minutes in case of a fault of the energy source in order to continue the steering function and other necessary systems such as lighting, windscreen wipers, engine management and braking systems.
Source(s)	UN R79, 5.3.3.3 UN R79, 6.1.4

EPS-LR 3	In case of steer-by-wire, energy shall be available for at least 38 minutes in case of a failure within the energy transmission in order to continue the steering function and other essential systems such as lighting, windscreen wipers, engine management and braking system.
Source(s)	UN R79, 5.3.3.4 UN R79, 6.1.4

EPS-LR 4	In case of the steering system and the braking system sharing the same energy source, the steering system shall have priority.
Source(s)	UN R79, 5.3.1.4

EPS-LR 5	In case of vehicles with auxiliary steering equipment, the Electrical Power Supply System shall be protected against overvoltage.
Source(s)	UN R79, Annex 4, 2.1.3

EPS-LR 6	Faults in the energy supply of the auxiliary steering equipment shall not alter the steering angle of the vehicle. Otherwise, additional requirements for the electrical power supply shall be derived.
Source(s)	UN R79, Annex 4, 2.2.1 UN R79, Annex 4, 2.2.1.1 associated test criteria

EPS-LR 7	Towing vehicles of trailers shall be protected from an overload, undervoltage and short-circuit of the electrical power supply of the trailer.

Source(s)	UN R79, Annex 7, 2.4.1

EPS-LR 8	The cables used to connect the trailer to the towing vehicle shall be designed with a cross-section that matches the occurring current.
Source(s)	UN R79, Annex 7, 2.5.1

EPS-LR 9	If the trailer has electric auxiliary systems, the steering system of the trailer shall be prioritized with the help of a function of the trailer steering system.
Source(s)	UN R79, Annex 7, 3.2/3.3

EPS-LR 10	A break in the electrical supply shall be taken into consideration for driving maneuvers with a trailer.
Source(s)	UN R79, Annex 7 3.6.2.1 UN R79, 6.3

The following **test specifications** must be complied with:

EPS-LR 11	In case of steer-by-wire systems, the minimal energy level of the electrical power supply components shall be at the level at which a failure is indicated to the customer (incl. taking into account the effects of e.g. temperature and ageing on battery performance).
Source(s)	UN R79, 5.3.3.5

EPS-LR 12	The tests shall be conducted on a level surface affording good adhesion.
Source(s)	UN R79, 6.1.1 GB17675-2021, 5.1.1

EPS-LR 13	During the tests, the vehicle shall be loaded to its technically permissible maximum mass and its technically permissible load on the steered axle.
Source(s)	UN R79, 6.1.2 GB17675-2021, 5.1.2

EPS-LR 14	Test shall be performed at the tire pressure prescribed by the manufacturer.
Source(s)	UN R79, 6.1.3 GB17675-2021, 5.1.3

EPS-LR 15	Electrical loads of important systems can be simulated during vehicle tests.
Source(s)	UN R79, 6.1.4

The following regulations or **customer warnings** must be taken into consideration:

EPS-LR 16	The customer shall receive a clear indication of non-mechanical faults which impair the steering function.
Source(s)	UN R79, 5.3.1.3 UN R79, 5.4.1.1

EPS-LR 17	A warning can be issued as an optical, acoustic or mechanical signal (e.g. increase in steering force).
Source(s)	UN R79, 5.4.1.1 UN R79, 5.4.1.2 UN R79, 5.4.1.3

EPS-LR 18	If the same energy source is used to supply several systems and the state of charge is low, resulting in an increased steering force, an optical or acoustic warning shall be issued.
Source(s)	UN R79, 5.4.1.4

EPS-LR 19	In case of steer-by-wire systems, a red warning signal shall be issued for non-mechanical faults.
Source(s)	UN R79, 5.4.2.1.1

EPS-LR 20	In case of auxiliary steering equipment, a failure of the energy supply shall be indicated.
Source(s)	UN R79, Annex 4, 2.3.1.2

The following **documentation requirements** must be taken into consideration:

EPS-LR 21	Documentation of the safety concept shall be provided.
Source(s)	UN R79, Annex 6, 3.

EPS-LR 22	This documentation shall be drawn up in the context of the design and development process.
Source(s)	UN R79, Annex 6, 3.

Additional requirements resulting from **GB17675-2021**:

EPS-LR 23	Not applicable to autonomous steering systems
Source(s)	GB17675-2021, 1 Scope

EPS-LR 24	Additional homologation-relevant normative references to GB/T 34590-2017 Road vehicles -- Functional safety (equivalent to ISO 26262:2018) and reference to application for steering control
Source(s)	GB17675-2021, 2 Normative References

EPS-LR 25	Supplemented by Annex B Functional safety requirements Definition of system boundaries including E/E part, energy supply and transmission
Source(s)	GB17675-2021, 3.1.1.2 Definition of steering transmission equipment, 3.1.1.4 Definition of power supply equipment

EPS-LR 26	Requirements for the documentation and the safety strategy (incl. FMEA and FTA)
Source(s)	GB17675-2021, Annex B.2.6.

EPS-LR 27	Verification and validation of functional safety (normal operation, error mode, predictable misuse)
Source(s)	GB17675-2021, Annex B.3

EPS-LR 28	ASIL-specifications for – unintended lateral motion (self-steering) – unintended loss of lateral motion control (jamming) – sudden electr. failure is to be assessed separately using HARA
Source(s)	GB17675-2021, Annex B.2.5

EPS-LR 29	Implementation date 1/1/2022 for new type approval, 1/1/2023 for initial registration
Source(s)	GB17675-2021, 6 Implementation Date

A2 Detailed Requirements of the Braking Function Arising from Technical Rules, Regulations and Standards

The **design of the electrical power supply for braking systems** must take the following into consideration:

Note: At the moment of publication of the VDA 450 recommondation, the UN R13 EMB is currently being processed as an EMB specific update to the UN R13.

EBS-LR 1	The energy supply system shall have at least two completely independent energy storages, each provided with its own transmission, also independent, and each storage may act on the brakes of only two or more wheels.
Sources	UN R13 5.2.1.2.7.2 UN R13h 5.2.2.8

The following requirements (EBS-LR 2 and EBS-LR 3) from the current UN ECE and FMVSS-regulations take into account manual driving. However, these requirements only need to be taken into account as a basis for the purpose of this recommendation, since adaptation to automated driving has not yet taken place. For automated driving, an energy reserve for transitioning the vehicle to a safe state must be taken into account, cf. also ADS-LR 02 and ADS-LR 03.

EBS-LR 2	For a faultless system, repeated braking maneuvers with maximum brake force (depending on the respective regulation) and a further secondary braking shall be taken into account in order to determine the storage (device) size.
Sources	UN R13 Annex 7 Part A 1.2.1 UN R13 EMB draft regulation 5.2.1.35.6 UN R13 EMB draft regulation Annex 7 Part D 1.2.1 UN R13h Annex 4 1.2.1 FMVSS 121 S5.1.2.1, S5.2.1.1

EBS-LR 3	For a system with a first fault, a reduced number (as stipulated by the respective regulation) of braking maneuvers with maximum brake force and a further secondary braking/residual braking performance shall be taken into account in order to determine the storage (device) size.
Sources	UN R13 5.2.1.5.2 UN R13h 5.2.4.2 UN R13 EMB draft regulation 5.2.1.5.4.1 UN R13 EMB draft regulation 5.2.1.35.2 FMVSS 105 S5.1.3.3 FMVSS 135 S7.10.4 FMVSS 121 S5.7.1 UN R79, 5.3.1.4 UN R79 5.3.1.5

EBS-LR 4	In case of an Electrical Power Supply System divided between the brake and other consumers, a sufficient state of charge and/or sufficient power shall be provided for the brake.
Sources	UN R13 EMB draft regulation 5.2.1.13.2 UN R13 EMB draft regulation 5.2.1.35.10 UN R13 EMB draft regulation 5.2.1.35.15 UN R13 EMB draft regulation 5.2.1.35.15.1 UN R13 EMB draft regulation 5.2.1.35.15.2

EBS-LR 5	The capability of the charging system for the Electrical Power Supply System of the brake shall be sufficiently dimensioned to ensure that the state of charge during normal driving can be upheld at any time (with the exception of initial charging after ignition) above the energy warning threshold of the Electrical Power Supply System) (cf. EBS-LR 10).
Sources	UN R13 EMB draft regulation Annex 7 Part D 2 UN R13 EMB draft regulation 5.2.1.35.7.1 UN R13 EMB draft regulation 5.2.1.35.7.2 UN R13 EMB draft regulation 5.2.1.35.7.3

When designing the Electrical Power Supply System, the following notes are relevant not just for braking systems for automated driving:

EBS-LR 6	In case of a failure of the energy source of the electric control/transmission device, the full control range of the service braking system shall be ensured after twenty consecutive full stroke actuations of the service braking control. During the test, the braking control shall be fully applied for 20 seconds and released for 5 seconds on each actuation.
Sources	UN R13 5.2.1.27.5 UN R13 EMB draft regulation 5.2.1.35.5 UN R13h 5.2.20.4

EBS-LR 7	The power supply (generator and battery) of the power-driven vehicle shall have sufficient capacity/power to provide the current for an electrical braking system of the tractor unit and the trailer.
Sources	UN R13 5.2.1.19.1 UN R13h 5.2.17.1

EBS-LR 8	The energy supply for trailer ABS shall have a redundant supply.
Sources	FMVSS 121 S5.5.2

EBS-LR 9	The requirements for charging times in the UN R13/h standards can be taken into account since they currently only apply to other than electrical energy media.
Sources	UN R13 Annex 7 Part A 2 UN R13h Annex 4 2

The following regulations in respect of **warnings to drivers/driving function** shall be taken into consideration:

EBS-LR 10	Each energy storage shall be equipped with a warning device – requirement of indication in case of falling below the energy warning threshold of the energy storage device – requirement of an **optical** warning signal – requirement of an **acoustic** warning
Sources	UN R13 5.2.1.2.7.2 UN R13 5.2.1.27.6 UN R13h 5.2.2.8 UN R13h 5.2.14.1 UN R13 EMB draft regulation 5.2.1.35.3 UN R13 EMB draft regulation 5.2.1.35.7 UN R13 EMB draft regulation 5.2.1.35.9 UN R13 EMB draft regulation 5.2.1.35.13 FMVSS 121 S5.1.5

EBS-LR 11	Failures in the energy transmission of the braking system shall be signaled to the driver / the driving function by a device comprising a red warning signal. – **non-mechanical faults** shall be indicated – requirement of an **optical** warning signal – requirement of an **acoustic** warning
Sources	UN R13 5.2.1.4.2 UN R13 5.2.1.27.3 UN R13h 5.2.3 UN R13 EMB draft regulation 5.2.1.35.11 UN R13 EMB draft regulation 5.2.1.35.13 FMVSS 105 S5.3.1

EBS-LR 12	Insufficient capability of the energy supply (Active Sources) of the braking system shall be indicated to the driver / the driving function with a warning message corresponding to a yellow warning signal. – requirement of an indication in case of the charging capacity falling below the warning threshold of the energy source
Sources	UN R13 EMB draft regulation 5.2.1.35.3 UN R13 EMB draft regulation 5.2.1.35.8

From the current perspective, the following **regular technical reviews** must be taken into account for the design of the electrical power supply. This collection is by no means exhaustive and reflects the current status of rules and regulations. For a concrete elaboration, a review of the regulations specific for the respective SR-Vehicle-Function must be carried out.

EBS-LR 13	It shall be possible to diagnose the energy transmission device for braking systems.
Sources	UN R13 5.1.4.2.4 UN R13h 5.1.4.1

EBS-LR 14	It shall be possible to assess the condition of the components of the service brake that are subject to wear and tear / degradation, e.g. SOH monitoring of the energy storage.
Sources	UN R13 5.1.4.1 UN R13h 5.1.4.1

From the current perspective, the following safety mechanisms must be taken into account for the design of the electrical power supply. This collection is by no means exhaustive and reflects the current status of rules and regulations. For a concrete elaboration, a review of the regulations specific for the respective SR-Vehicle-Function must be carried out.

EBS-LR 15	The means by which the device constituting the energy source is driven shall be as safe as possible.
Sources	UN R13 5.2.1.5 UN R13h 5.2.4

A3 Detailed Requirements for the Lighting and Visibility Function Arising from Technical Rules, Regulations and Standards

In respect of the lighting and visibility equipment of the vehicle, there are no known specific requirements for automated driving. Cross-connections of lighting functions are included in many common concepts. At present, regulatory or normative sets of requirements also contain no requirements in terms of the hazard warning lights duration.

Note.: Requirements of SR-Vehicle-Functions for the lighting and visibility equipment must be taken into account for specific use cases. An example in case is the environment detection via camera as part of the SR-Vehicle-Function ADS, which relies on lighting provided by the function "light".

A4 Detailed Requirement of the SR Vehicle Function ADS Arising from Technical Rules, Regulations and Standards

The following points show requirements placed on the self-check of the electrical power supply and the reactions of the SR-Vehicle-Function ADS based on that:

Note: At the moment of publication of the VDA 450 recommendation, the FRAV-09-05 is currently being processed.

ADS-LR 1	The EBN shall ascertain its status and communicate this to a Higher-Level Instance. A release of the ADS functions by the electrical power supply is only permissible if no fault was found in the electrical power supply.
Source(s)	UN R157, 6.2.3

ADS-LR 2	The electrical power supply may only release ADS functions if there is a sufficient energy reserve to transition the vehicle to a safe state (e.g. standstill of the vehicle in the current driving lane).
Source(s)	SAE J3016, 3.17 Note 3 – Level 4

ADS-LR 3	If the Electrical Power Supply System withdraws the release for automated driving, the energy reserve shall be sufficient for the driver to take over driving (Level 1 to 3) or for the vehicle to be transitioned to a safe state by the SR-Vehicle-Function ADS (Level 4 and 5).
Source(s)	SAE J3016, 3.17 Note 3 – Level 4 SAE J3016, 3.14 Note 4 - Level 4 and 5 UN R157, 5.4.3 SAE J3016, 5.5 Level 4: Note 1 SAE J3016, 3.14 Note 3 – Level 3 UN R157, 5.3.2 SAE J3016, 3.14 Note 5: Level 4 or 5 SAE J3016, 8.6 FRAV-09-05, 4.13.4

ADS-LR 4	If the electrical power supply detects a fault in the supply of SR functions, a reaction shall follow depending on the level of automation: – L4/5 automated driving: – Warning/information to the Higher-Level Instance – Optional: Information to the driver/passenger – L3 automated driving: – Warning/information to the Higher-Level Instance – Transition demand to the driver
Source(s)	UN R157, 6.2.3 UN R157, 5.4.2.3 UN R157, 6.4.1 FRAV-09-05, 4.13.2.3, 5.2.4, 5.4.4

ADS-LR 5	If the vehicle was transitioned to a safe state following a failure, the electrical power supply shall ensure the supply to the hazard warning lights.
Source(s)	UN R157, 5.3.3.2 UN R157, 5.4.3.1 UN R157, 5.5.1

B. Freedom from Interference

Freedom from interference must be assessed separately for each Element within an SR-EBN Channel (QM/SR Functions, cables & plug connectors, switches etc.) and be proven in respect of all safety-relevant functions. The following procedure must be followed for proof of freedom from interference:

- step 1: There is proof that the Element/vehicle component/function and the connections of several dependent Elements do not have the potential to violate a safety requirement of the safety-relevant functions.
- step 2: If proof as described in step 1 does not exist, the target values of ISO 26262:2018 (PMHF_bud, SPFM_bud, LFM_bud) for the avoidance of random hardware fault (PMHF_bud, SPFM_bud, LFM_bud) and the procedural requirements of ISO 26262:2018 for the avoidance of systematic failures must be fulfilled for the Element/vehicle component.
- step 3: If proof cannot be provided as described in step 2, an additional Safety Mechanism must be implemented to ensure freedom from interference. This Safety Mechanism is not restricted to the individual Element but can also be implemented centrally for several Elements.

Example: A short-circuit to ground in a control unit leads to undervoltage in the electrical power supply. Freedom from interference is deemed to exist for the control unit as soon as one of the following steps has been achieved:

- step 1: This undervoltage as well as all other relevant faults of this control unit cannot result in a violation of safety requirements in the safety-relevant functions (e.g. environment perception, logic, actuators) within the same channel and the other channels of the electrical power supply. This is fully proven in line with the below-mentioned "Scenarios for the assessment of freedom from interference" and any necessary energy and power reserves are safeguarded by corresponding ASIL integrity.
- step 2: The control unit was designed and developed systematically and in respect of random hardware faults in such a way that the requirements of ISO 26262:2018 regarding Coexistence of Elements and the target values PMHF_bud, SPFM_bud, LFM_bud are complied with. In the process, it is particularly important to assess dependent failures affecting other control units, which may arise, for example, from using the same plug connector, microcontroller, hardware or software.
- step 3: There are suitable safety mechanisms for avoiding or controlling relevant faults of the control unit. These safety mechanisms must be designed and developed both systematically and in terms of avoiding random hardware failures in such a way that the requirements of ISO 26262:2018 regarding Coexistence of Elements and the target values PMHF_bud, SPFM_bud, LFM_bud can be complied with.

As proof of freedom from interference in line with step 1, the vehicle component must be implemented in such a way as to ensure that at least the faults of the vehicle components, specified in the "Scenario for the assessment of freedom from interference", cannot result in violations of the safety requirements in the safety-relevant functions under the specified boundary conditions. In doing so, compliance with the safety requirements must be achieved without the use of safety mechanisms. In the process, all relevant faults of the vehicle component must be taken into account, e.g. in case of a QM consumer:

- hard (low resistance) and soft (high resistance) short-circuits
- energy-related faults
- overvoltage fault due to power feedback or a sudden shutdown by the consumer

Further faults and/or assessment criteria can be added, based on expert judgement. For the implementation of suitable safety measures to ensure compliance with the safety requirements, step 3 will be referred to.

Scenarios for the assessment of freedom from interference:
When assessing freedom from interference, the key parameters of the design range for the electrical power supply must be taken as a basis. That means that compliance with the safety requirements must not only be examined at specific, suitable points in the design range. Instead, it must be possible to rule out a violation of safety requirements across the entire design range of the electrical power supply with corresponding ASIL integrity in order to prove freedom from interference in terms of ISO 26262:2018. This also applies to the combination of different influencing parameters in accordance with the following table:

Parameter	Idea for derivation	Note
EBN static load	Installed power – minus the power superposition which is avoided by means of a safety measure with a sufficient ASIL – minus the power superposition which can generally be ruled out by physical correlations	Each separate load collective must ensure freedom from interference. Assumption for "power superposition which can generally be ruled out by physical correlations": there are no SW/HW faults or customer interactions that can lead to a power superposition.
EBN dynamic load	Superposition of all loads of the SR driving maneuver – minus the power superposition which is avoided by means of a safety measure with a sufficient ASIL – minus the power superposition which can generally be ruled out by physical correlations	The superposed maneuver load of the relevant SR-Vehicle-Function does not have to be switched on permanently during the entire driving cycle; instead, it can be limited to the time windows of the SR-Maneuvers. Note 1: All SR-Maneuvers must be proven separately, e.g. MRM, double lane change or "Spielstraßenmanöver”. Note 2: The "Spielstraßenmanöver” corresponds to an evasive maneuver at low speed.
Ambient air temperature	Specified range of the SR-Vehicle-Function – restriction possible if a temperature range can be ruled out by safety measures with sufficient integrity (e.g. restriction of ODD).	A suitable safety measure might be a change of the operating condition with lower requirements placed on the availability of the EBN or an active warning (red) to the driver.

Condition of the interconnected sources (AQ and PQ)	Freedom from interference must be proven separately for each combination of the supply paths, cf. 4.2.2.3 freedom from interference for sufficiently independent sources.	Depending on the architecture, several combinations of sources and energy storage devices are possible.
Condition of the Passive Source	Aged battery with increased internal resistance and reduced capacity in accordance with the end-of-life specification: The state of charge must be set to the level of the warning threshold and the battery temperature be selected according to the minimum ambient air temperature of the vehicle specification.	Batteries outside the end-of-life specifications must be detected by suitable safety measures and a corresponding vehicle reaction be initiated. Note 1: The battery diagnosis can also take into account the interaction between ageing, state of charge and battery temperature for assessing the capability. In this case, the different characteristic key parameters at the warning threshold must be taken into account for an assessment of interference. Note 2: For an assessment of power feedback, high battery states of charge must also be taken into account as these present the worst case in this example.
Separation characteristics of the fuse/ the separating Element	Fuse: Slowest tripping characteristic according to ISO 8820 and avoidance of unauthorized replacement with fuses not qualified according to ISO 8820 Separating Element: ASIL safeguarded specification of the active separating and connecting Element	
Fault pattern 1: Short Circuit	Variation of the short-circuit resistance from 0 milliohm (short-circuit resistance in the component plug) to a short-circuit resistance leading to a current in accordance with ISO 8820-2 B.2.3.2 (slow tripping due to a soft short-circuit)	If a fault distribution was detected, the value range for the short-circuit resistances must be adjusted. The impedance of the overall circuit (plus and minus path) must be taken into account for the analysis. ISO 8820-2, B.2.3.2 specifies test currents of 2x I_R or 6x I_R depending on the fuse type.
Fault pattern 2: Fault currents	Consumer with a permanent maximum nominal power, no degradation possible	If a fault distribution was detected, the value range for the fault currents must be adjusted.
Fault pattern 3: **Power feedback**	Due consideration of the regenerative loads with their maximum power feedback capacity as per specification	Superposition of all current power feedback capacities minus the minimum base load in the electrical power supply analogous to the EBN peak load. Note 1: Safety Mechanism that take appropriate countermeasures in case of overvoltage, with sufficient integrity, may be taken into consideration.

		Note 2: Examples of the above-mentioned safety mechanisms could be the connection of resistive loads or the separation of faulty paths.
Wiring harness	Due consideration of the specification range of contact resistance and specific resistance from begin-of-life to end-of-life under the specified operational conditions (e.g. temperature, humidity,…)	Both key parameters of the specification range must be tested as the worst case cannot always be clearly assigned.

Tab. 6: Scenarios for the assessment of freedom from interference

C. Topologies

The implementation of this recommendation can be achieved by means of various electrical power supply architectures. By way of example, various conceptional architecture topologies in star topology, tree topology or ring topology are illustrated, which also take into account different voltage classes (HV / 48 V / 24 V / 12 V).

In case of the conceptual architecture topologies, the focus is in particular on the important characteristics of the central Elements regarding freedom from interference, availability and independence (cf. Figure 8 and 9)

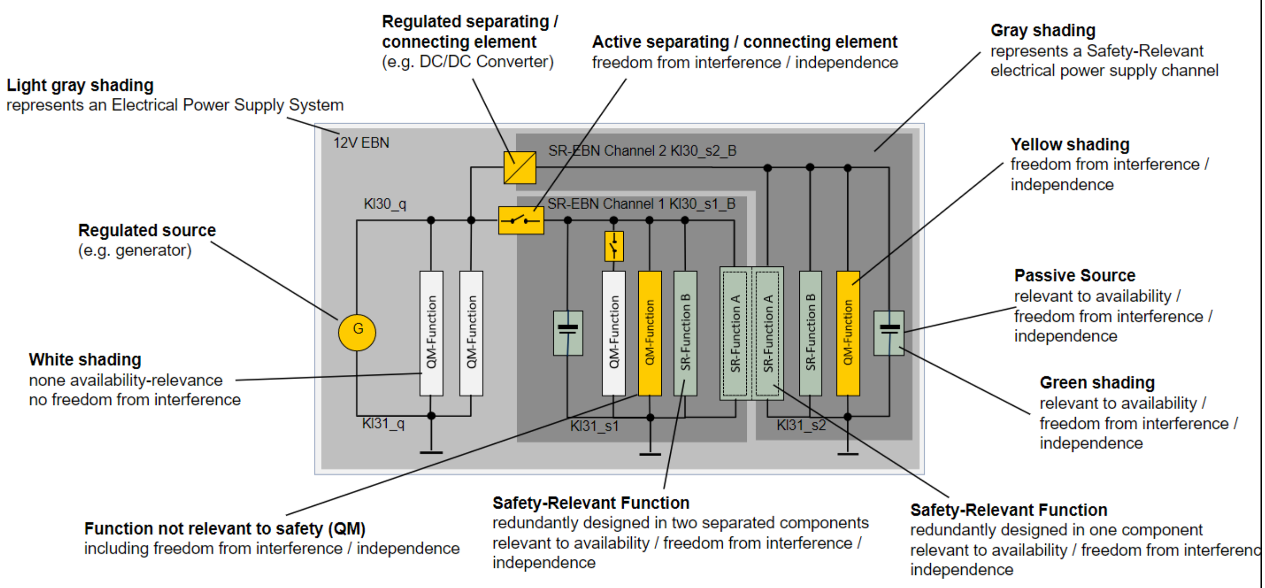
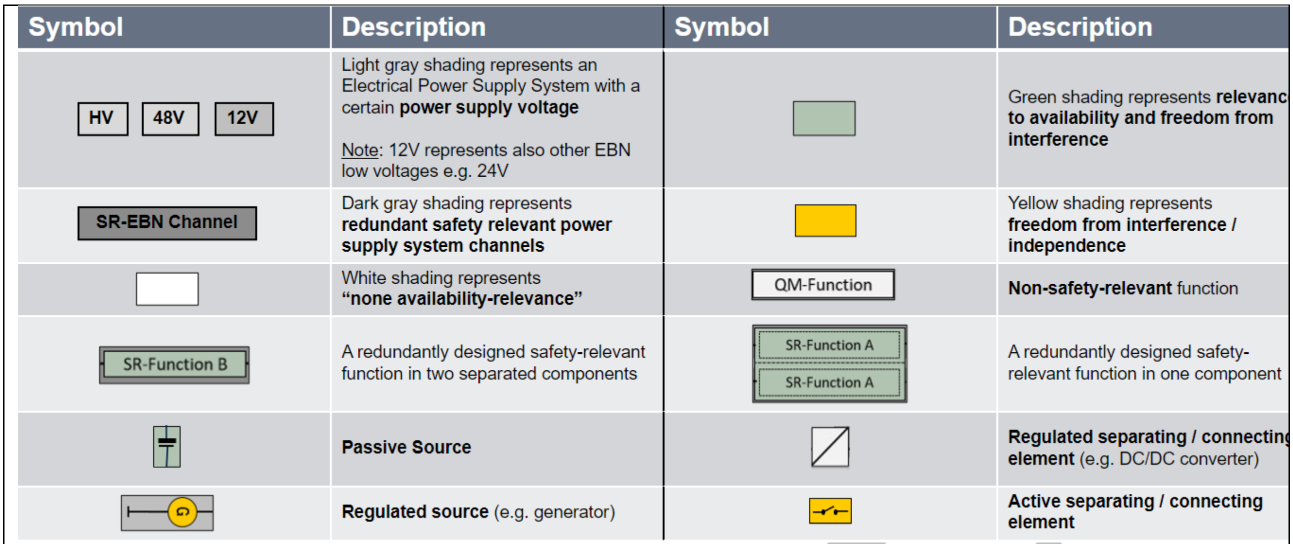

Regulated separating / connecting element
(e.g. DC/DC Converter)
Active separating / connecting element
freedom from interference / independence
Gray shading
represents a Safety-Relevant electrical power supply channel
Light gray shading
represents an Electrical Power Supply System
12V EBN
SR-EBN Channel 2 Kl30_s2_B
Kl30_q
SR-EBN Channel 1 Kl30_s1_B
Yellow shading
freedom from interference / independence
Regulated source
(e.g. generator)
G
QM-Function
QM-Function
QM-Function
QM-Function
SR-Function B
SR-Function A
SR-Function A
SR-Function B
QM-Function
Passive Source
relevant to availability / freedom from interference / independence
White shading
none availability-relevance
no freedom from interference
Kl31_q
Kl31_s1
Kl31_s2
Green shading
relevant to availability / freedom from interference / independence
Safety-Relevant Function
redundantly designed in two separated components
relevant to availability / freedom from interference / independence
Safety-Relevant Function
redundantly designed in one component
relevant to availability / freedom from interferenc
independence
Function not relevant to safety (QM)
including freedom from interference / independence

Fig. 8: Important characteristics of the central Elements in topologies



Symbol	Description	Symbol	Description
HV 48V 12V	Light gray shading represents an Electrical Power Supply System with a certain **power supply voltage** Note: 12V represents also other EBN low voltages e.g. 24V	🟩	Green shading represents **relevanc to availability and freedom from interference**
SR-EBN Channel	Dark gray shading represents **redundant safety relevant power supply system channels**	🟨	Yellow shading represents **freedom from interference / independence**
□	White shading represents **"none availability-relevance"**	QM-Function	**Non-safety-relevant** function
SR-Function B	A redundantly designed safety-relevant function in two separated components	SR-Function A SR-Function A	A redundantly designed safety-relevant function in one component
⊥	**Passive Source**	⧄	**Regulated separating / connecting element** (e.g. DC/DC converter)
G	**Regulated source** (e.g. generator)	🟨	**Active separating / connecting element**

Fig. 9: Explanation of symbols used and their characteristics

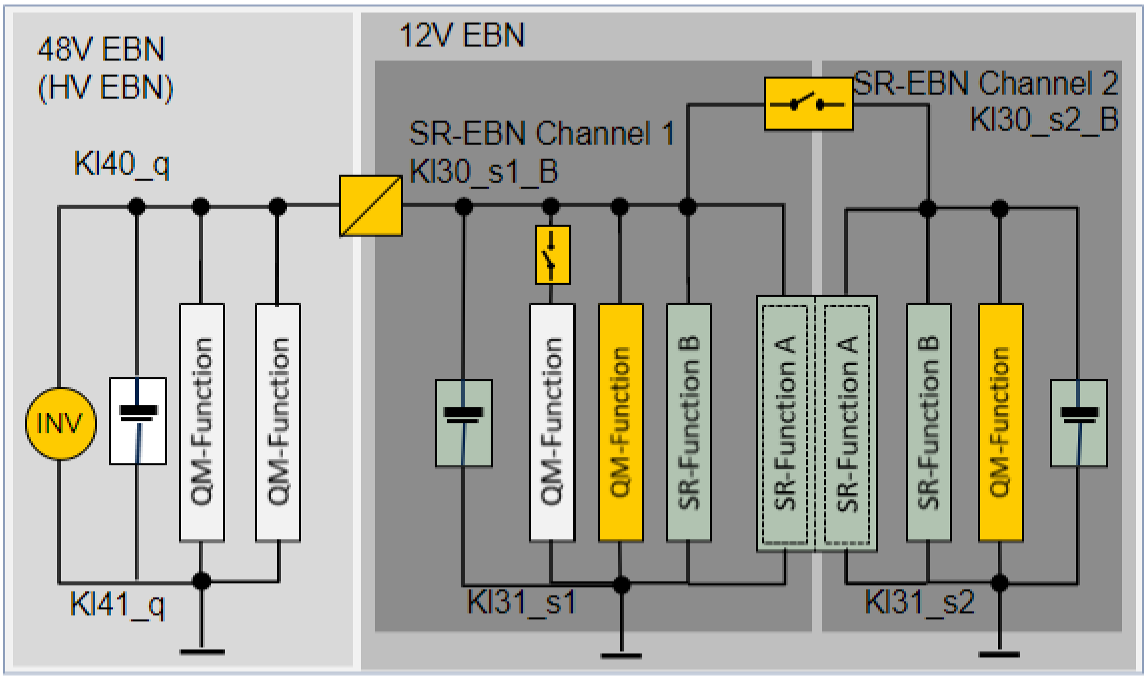


Fig. 10: Topology 1

Two independent SR-EBN channels, each with its own 12 V supply system, separated by an ATV and a 48 V/12 V DC/DC converter free from interference

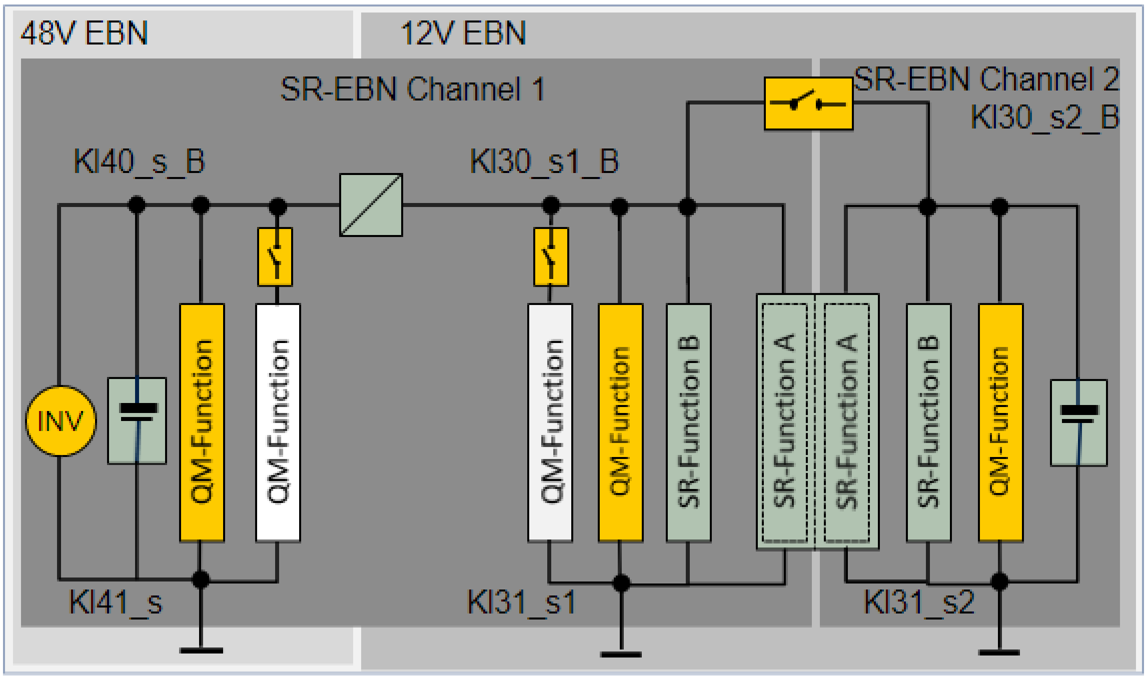


Fig. 11: Topology 2

An SR-EBN Channel is supplied by the safety-relevant 48 V Electrical Power Supply System and one SR-EBN Channel on the basis of 12 V, separated by an ATV

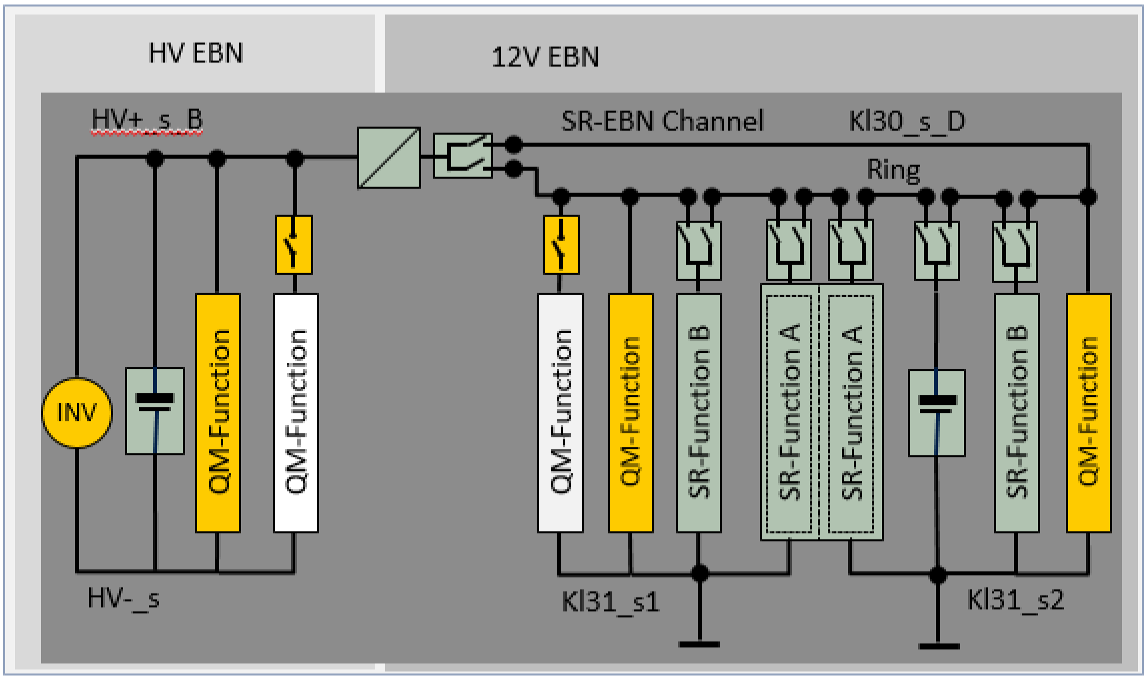


Fig. 12: Topology 3

The SR-EBN Channel in ring topology is supplied by a 12 V supply system and a safety-relevant HV Electrical Power Supply System incl. HV/12 V DC/DC converter

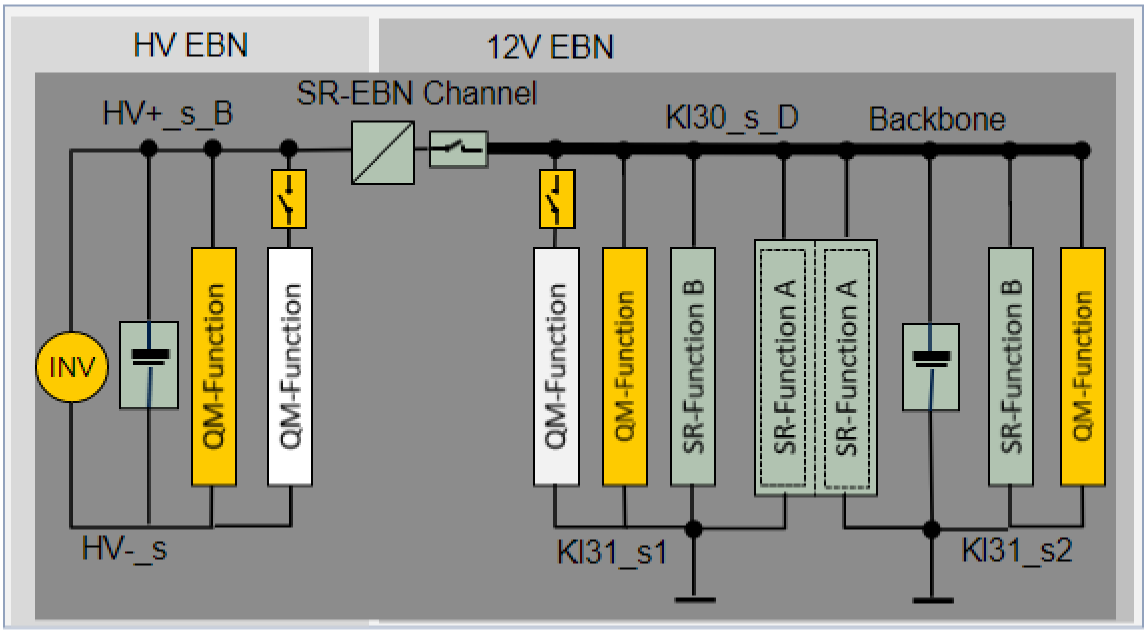


Fig. 13: Topology 4

The SR-EBN Channel in its capacity as a backbone is supplied by a 12 V supply system and an available safety-relevant HV Electrical Power Supply System incl. HV/12 V DC/DC converter

Note: This architecture violates the requirement of the EBN-FR 2 in chapter 4.1.2 "at least two completely independent energy storage devices, each with its own, also independent transmission devices".

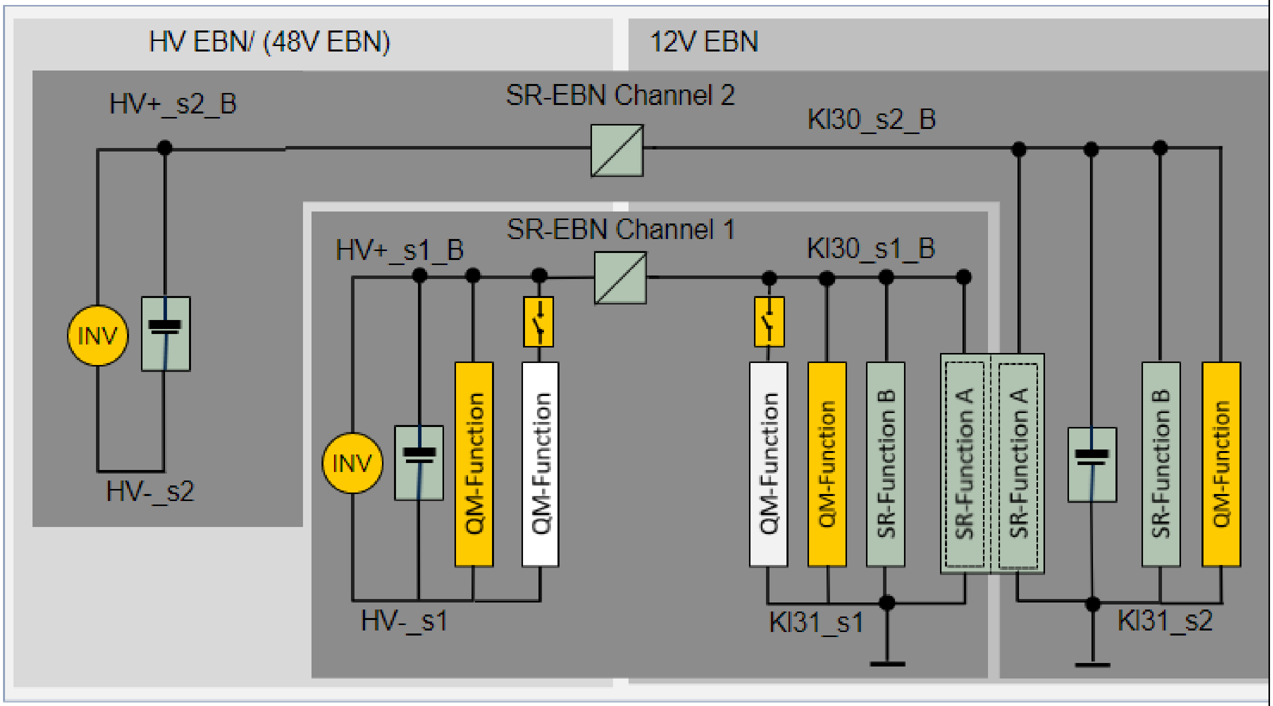


Fig. 14: Topology 5

Available EBN consisting of two independent SR-EBN channels comprising an SR-HV EBN including HV/12 V DC/DC converter and an SR-12 V EBN

D. Case Studies

The objective of this Annex is to illustrate the practical application of this document based on concrete case studies.

Case study A: According to chapter 4.1.1, the SR-Vehicle-Function ADS requires the generic, simplified Safety Goal ADS-SG1: " Avoid faulty ADS vehicle function” with ASIL D. From this requirement, an availability requirement for the EBN is derived, which according to chapter 5.2 and irrespective of the concept classification in chapter 5.1, is translated into a decomposed EBN with independent SR-EBN channels and their functional safety requirements.

- EBN-FSR 1.1.1 / 1.2.1: Ensure sufficient power feed by the energy sources of EBN channel 1 (Kl30_s1) to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
- EBN-FSR 1.1.2 / 1.2.2: Ensure sufficient power distribution from the Kl30_s1 energy sources to the Kl30_s1 SR-Loads to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
- EBN-FSR 1.1.3 / 1.2.3: Avoid interference from EBN loads with the Kl30_s1 power supply, which endangers the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals.

Below, all ASIL allocations in terms of availability of the EBN are stated, unless another Safety Goal is explicitly stated.

The redundant design of the SR functions environment perception, planning and actuation allows the use of an ASIL decomposition. The latter is used to reduce the requirements placed on the systematic design and development process of the respective SR subfunction according to ASIL B(D). The SR-EBN channels follow this decomposition scheme and are therefore also implemented in ASIL B(D).

Figure 15 illustrates schematically the decomposed 12 V electrical power supply, examined here by way of example, with two sufficiently independent SR-EBN channels 1 and 2, the different QM-Functions and redundant SR-Functions, the active and Passive Sources and the ATVs according to chapter 6.

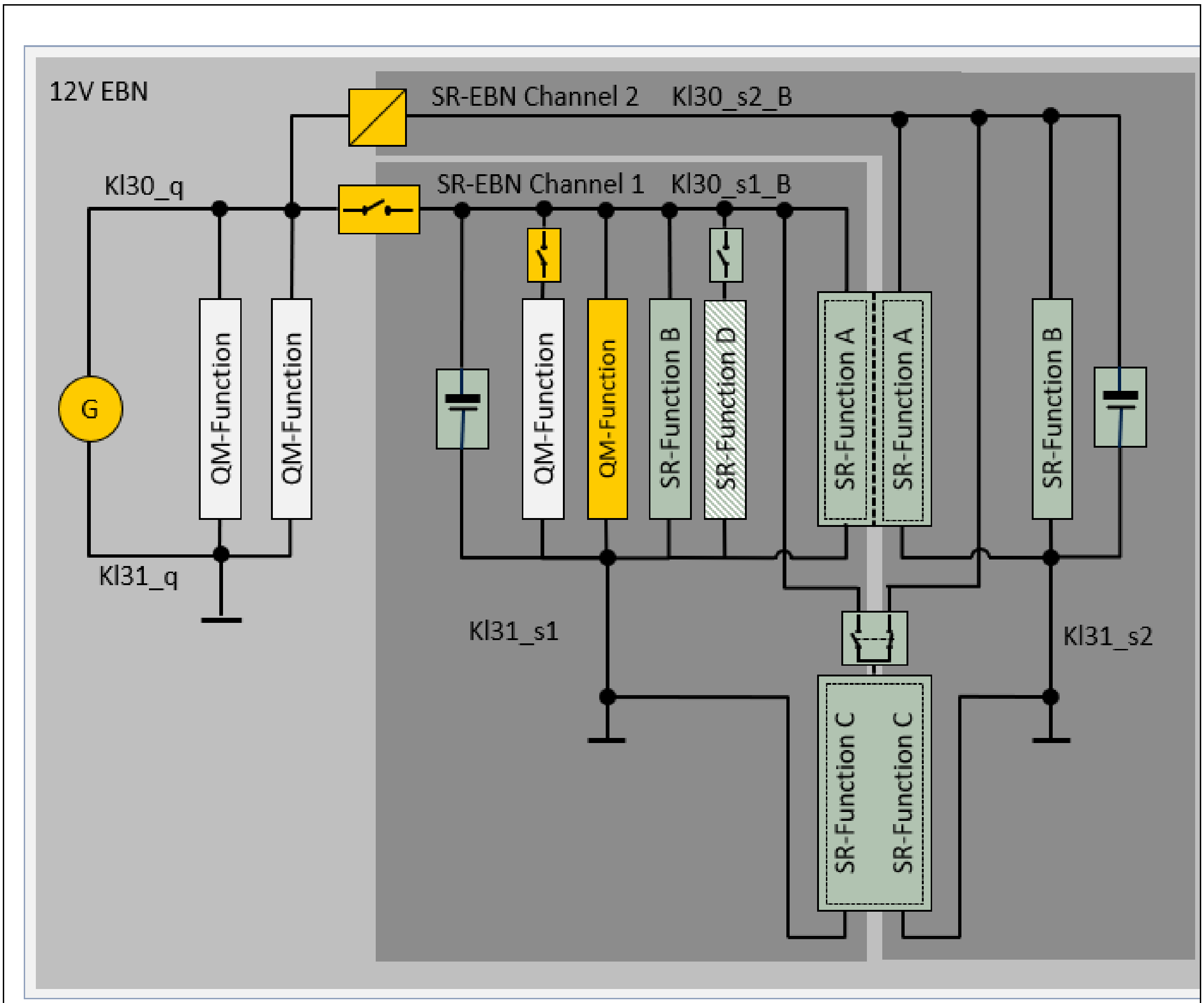


Fig. 15: Conceptional architecture topology of a safety-relevant EBN according to the nomenclature in Annex C

Within the decomposed SR-EBN Channel, the supply of energy and power by active and/or Passive Sources is implemented in accordance with the Functional Safety Requirement EBN-FSR 1.1.1 from chapter 5.3. In the case study presented here, the channel-specific ASIL B(D) requirement for the supply of energy and power is allocated to the Passive Source – the battery. In this example, no safety-relevant availability requirement is allocated to the supply of energy and power by the generator as Active Source. However, freedom from interference regarding the insufficient supply of energy and power by the generator must be dealt with in order to avoid a Cascading Failure, which in turn leads to the loss of energy and power supplied by the Passive Source.

Note: To achieve the target metrics, it may be expedient to take the supply of energy and power by the generator in QM(D) into consideration for the safety concept, cf. chapter 4.2.2. This leads to further safety considerations/requirements for the QM consumers of Kl30_q and an availability requirement for the ATV between Kl30_q and Kl30_sX_B. Due to the resulting complexity, this approach will not be pursued any further here.

After a first fault, the system is transitioned to the safe state within the EOTTI. This safe state corresponds to a new SR-Vehicle-Function as described in chapter 4.2.4.3 strategy B without a time limit and with a lower integrity level. In this case study, the associated hazard is rated as ASIL B by way of example, cf. ISO 26262-10:2018, 12.2.4.2.b and Figure 28. This new SR-Vehicle-Function places new independent safety requirements on the remaining SR-EBN Channel in ASIL B. This SR-EBN Channel must therefore be able to perform the new SR-Vehicle-Function with the required ASIL B integrity, thus ensuring that the remaining ASIL capability of the residual system matches at least the ASIL of the hazard. For this SR-Vehicle-Function, an independent safety case must be conducted. This includes both the implementation of the systematic design and development process and proof of compliance with the target metrics regarding random HW faults for ASIL B.

According to interpretation option 2, which is adopted in this recommendation (cf. chapter 4.2.4.2), the supply of energy and power within the EOTTI does not have to be implemented with the initial ASIL D goal; instead, an ASIL B(D) implementation according to the decomposition is sufficient. The initiation of the MRM function, the time limit for the transition (EOTI) to the new SR-Vehicle-Function and compliance with the restrictions of the new SR-Vehicle-Function must be implemented with ASIL D. Due to the above-mentioned decomposition, safety-relevant availability requirements that exceed ASIL B(D) are not permissible. Therefore, the functions triggering the MRM, ensuring the time limits for the transition and ensuring the compliance with the restrictions of the SR-Vehicle-Function must be implemented Fail-Passive, cf. ISO 26262-10:2018 12.2.4.1 and VDA recommendation, chapter 4.2.3.2. For the time being, this case study will only look at transitioning the SR-Vehicle-Function ADS to the safe state within the EOTTI and ensuring the decomposition requirements for sufficient independence and freedom from interference. For detailed notes regarding compliance with freedom from interference refer to Annex B.

As described above, the SR-EBN channels must meet the functional safety requirements EBN-FSR 1.1.2 and 1.1.3. In this example, the SR-EBN channels are implemented asymmetrically, thus enabling only SR-EBN Channel 1 for onward travel with ASIL B. If a first fault occurs in channel 1, the vehicle must be transitioned to a safe standstill of the vehicle within EOTTI (example 3 in chapter 4.2.3.3), using channel 2. Annex E contains a quantitative illustration of how this type of division effects the budgeting of the target metrics regarding random hardware faults – PMHF_bud, SPFM_bud and LFM_bud.

If terminals with different systematic ASIL capability coexist in one EBN, safety Elements have to be introduced to ensure freedom from interference. Therefore, figure 15 provides, by way of example, for an ATV and/or an Active Source, which ensures the freedom from interference, between Kl30_q and the safety-relevant Kl30_s1_B and Kl30_s2_B. The safety Elements must each comply with an ASIL B(D) integrity regarding safe separation. In addition, sufficient independence between the two safety Elements must be proven, cf. chapter 4.2 and ISO 26262-9:2018, 5.1. For a simplified illustration, the two different safety Elements "Active Source – free from interference AQ-R" (chapter 6.1.2) and "active separating Element EBN[SR]-EBN[QM]" (chapter 6.3.2) are used.
The safety Elements introduced may possibly be unable to maintain the separating function if the breakdown voltage of the components used is exceeded. To avoid dependent failures on both EBN channels, the regulated source is allocated the Safety Goal "Avoidance of overvoltage across the operating voltage range of the safety Elements with ASIL D" according to ISO 26262-9:2018, 5.4.3.

Accordingly, this freedom from interference requirement of the Active Source can be reduced to ASIL B(D) if at least one safety Element has ASIL B(D) capability for freedom from interference regarding all generator faults. If both safety Elements have ASILB(D) capability for freedom from interference regarding all generator faults, a QM(D) requirement for an unintentional overvoltage of the Active Source is sufficient.

Within the safety-relevant EBN channels, freedom from interference of each Element and each function spanning several Elements must be assessed separately with ASIL B(D) (QM/SR-Function, cables & plug connectors, switches etc.) and proven in respect of all safety-relevant functions. In this example, QM-Functions cannot prove the requirements regarding freedom from interference by themselves, cf. step 1 and step 2 in Annex B. Therefore, according to step 3 in Annex B, the active separating Element EBN[SR]-L[QM] with ASIL B(D) integrity regarding safe separation is introduced as a safety Element.

According to the recommendation in chapter 4.2.3.3, SR-Functions should comply at least with the same ASIL integrity for freedom from interference which they require from the SR-EBN Channel for a safe supply of energy and power. In this case study, the required supply of energy and power by the SR-Functions A and B corresponds to the availability requirement of the SR-EBN Channel. Therefore, no further measures have to be taken regarding freedom from interference.

As the SR-Function D only requires ASIL A for the supply of energy and power, the required freedom from interference in ASIL B(D) is not inherently given. To ensure freedom from interference with the SR-EBN Channel, the active separating and connecting Element EBN[SR]-L[SR] is introduced with ASIL B(D) integrity in respect of safe separation. To ensure the safe supply of the SR-Function D, the active separating and connecting Element must ensure availability of the energy and power transmission in ASIL A.

For the purpose of further illustration, this case study presents an SR-Function C which is supplied by both SR-EBN channels and does not satisfy the required proof of freedom from interference. Accordingly, an active separating and connecting Element EBN[SR]-L[SR]-EBN[SR] (Y switch) must be introduced as a safety Element with the following characteristics:

- The safety Element must ensure freedom from interference of the SR function with the respective SR-EBN Channel with an ASIL B(D) rating.
- The safety Element must prevent simultaneous interference on both terminals Kl30_s1_B and Kl30_s2_B with an ASIL D rating.
- The safety Element must prevent an undetected low-resistance connection of the two terminals Kl30_s1_B and Kl30_s2_B with an ASIL D rating.
- The safety Element must ensure the safe supply of the two SR functions C, each with an ASIL B(D) rating.

If a passive separating and connecting Element, e.g. cable or connector, does not fulfill the freedom from interference requirement as described in Annex B step 2, an active safety Element must be introduced once again with the necessary integrity. The requirements regarding the transmission of energy and power must also be collated for all passive separating and connecting Elements and verified separately.

In addition to the availability requirement of the Passive Source to supply sufficient energy and power, it must also ensure freedom from interference with the SR-EBN Channel with the same integrity as the EBN channel. To ensure this, the FSR from chapter 6.2 for Type 3 "Safety-relevant Passive Source permanently switched on" PQ[SR]-On must be fulfilled.

Case study B: In contrast to case study A, in this case study both safety-relevant EBN channels 1 and 2 are to be capable of enabling continued travel after a first fault. After the first fault, a transition to a new SR-Vehicle-Function will take place - within the EOTTI – with a hazard assessment of ASIL B integrity. +

According to case study A, both SR-EBN channels must be able to independently perform the new SR function with the required new ASIL B integrity. For this SR-Vehicle-Function, an independent safety case must be conducted. This includes both the implementation of the systematic design and development process and the proof of compliance with the target metrics regarding random HW failures for ASIL B.

For the implementation, this study will use the example of the passive high-voltage supply system of an electric vehicle to safeguard the supply of energy and power as illustrated in Figure 16. In addition, an Active Source is needed to convert the energy from HV to 12 V.

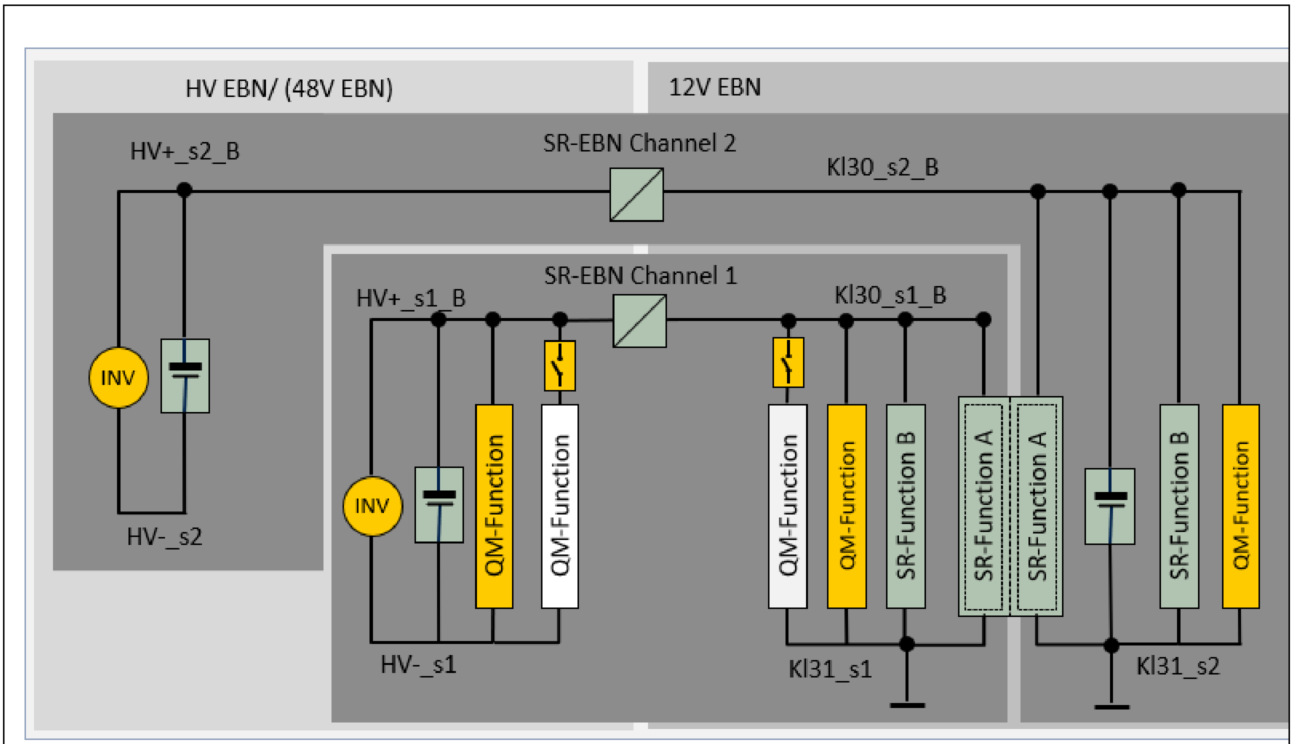


Fig. 16: Conceptual architecture topology of a safety-relevant EBN according to the nomenclature in Annex C

The safety-relevant EBN channels 1 and 2, consisting of the HV and 12 V voltage level, are symmetric but not structured homogenously redundant. Both EBN channels must comply with a systematic integrity of ASIL B(D), in accordance with the decomposition of the initial requirement, and an integrity of ASIL B for continued travel after a first fault. This integrity requirement then applies to the HV source (type 3 according to chapter 6.2) and to the DC/DC converter (type 3 according to chapter 6.2). In both EBN channels, the HV source and the DC/DC converter are designed in such a way that they can independently provide the energy and power both for the MRM – which must be completed within the EOTI – and for the subsequent continued travel in the new SR-Vehicle-Function.
In addition, the DC/DC converter must be designed highly dynamic in channel 1 and comply to the metrics regarding availability, without an additional Passive Source, as no second Passive Source is available in this EBN channel – cf. Kl30_s1_B in Figure 16. In channel 2, the Passive Source is used as an additional availability-relevant energy source. A decomposition of the two sources for the purpose of being able to provide higher PHMF budgets for both sources can be performed as described in chapter 4.2.2.

For the HV inverter, a freedom from interference requirement with the Safety Goal "Avoidance of overvoltage across the operating voltage range of the safety Elements with ASIL D" applies, analogous to the generator in case study A.
Furthermore, sufficient independence between the two safety-relevant EBN channels must be ensured, in accordance with ISO 26262-9:2018, 5.1 and chapter 4.2, to avoid independent failures between the EBN channels. This applies in particular to the HV sources and the DC/DC converter.
Within the SR-EBN channels, freedom from interference of each Element, both in the HV electrical power supply and in the 12 V electrical power supply, must be assessed - analogous to case study A - separately with ASIL B(D) (QM and SR functions, cable & plug connectors, switches etc.) – and proven in respect of all safety-relevant functions. If the proof according to Annex B step 1 and 2 cannot be provided, a safety Element with ASIL B(D) for safe separation must be introduced as described in Annex B step 3.

E. Derivation of Quantitative Target Metrics according to ISO 26262:2018

In Annex E, proposals are introduced for the allocation of the ISO 26262:2018 target metrics to the Safety Goals and requirements specified in chapter 5.2. In this example, only the derivation of the requirement placed on the Item EBN within the scope of the Entity concept in chapters 3.2.3 and 5.2.1 is described. In doing so, the following distinction is made in accordance with chapter 4.2.4:

Scenario A: The focus is exclusively on the capability of the EBN to supply the SR-Vehicle-Function ADS (in accordance with EBN-SG 1) in compliance with ASIL D. In this scenario, the EBN is designed exclusively for the SR-Vehicle-Function ADS according to the decomposition ASIL B(D) for each terminal, Kl30_s1 and Kl30_s2.

Scenario B: The focus is both on the capability of the EBN to supply the SR-Vehicle-Function ADS in compliance with ASIL D and on the capability of an EBN channel to ensure the manual or ADAS vehicle function. Accordingly, at least one Kl30_s or Kl30_s1 has additional ASIL B or ASIL C capability and allows, for example, for a manual continuation of the journey after failure of the redundant EBN channel Kl30_s2.

For both scenarios, the safety requirement

- EBN-FSR 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals

introduced in chapter 5.2 is used as a starting point at EBN level. If the concept "EBN as Item" is adopted as per chapter 5.2.1, the target metrics of ISO 26262:2018 can be used directly for EBN-FSR 1. Based on this assumption, the following target values arise for the EBN, taking into account ASIL D SG from chapter 4.1.1:

- PMHF (EBN-FSR 1): 10 FIT
- SPFM (EBN-FSR 1): 99 %
- LFM (EBN-FSR 1): 90 %

With the help of a fault-tolerant implementation of the safety requirements for the electrical power supply by means of redundant EBN channels, target metrics for the individual electrical power supply terminals Kl30_s1 und Kl30_s2 are then defined – by application of the concepts of allocation and decomposition, introduced in chapter 5.4 -, cf. EBN-FSR 1.1 and EBN-FSR 1.2. In the process, dependent failures of both channels must be avoided as per EBN-FSR 1.3. The target metrics of the individual terminals depend on the above-mentioned scenarios and will therefore be described specifically for each scenario.

Note 1: The target metrics described below present a first rough top-down approach. Effects such as sequence effects and the use of statistical safety mechanisms – taking effect within FTTI – and cyclical safety mechanisms – taking effect within MPFHTTI – have a project-specific influence on the quantitative metrics and are not taken into account in the first step. For this reason, the budgeting of PHMF is based on a T_life = 8000 h, which corresponds to the operating time of the vehicle.

Note 2: Both for the ASIL allocation and the ASIL decomposition, the procedure presented below can be digressed from if compliance with the target metrics of the original requirement at Item level can be proven.

Scenario A: Singular Analysis of the ASIL D use case:

In this scenario, the focus is on the SR-Vehicle-Function ADS. Therefore, the requirements for the redundant EBN channels Kl30_s1 and Kl30_s2 a are considered for this use case only. The result of the requirement derivation with respect to the quantitative target metrics is illustrated in Figure 17.

For a derivation of the requirements for the EBN channels according to EBN-FSR 1.1 and EBN-FSR 1.2, an ASIL decomposition is performed. Due to the boundary conditions of a decomposition as described in chapter 4.2, dependent failures of both EBN channels must be avoided and/or controlled in the process, cf. safety requirement EBN-FSR 1.3.

In case of a symmetric distribution of the PMHF target value of 10 FIT (cf. introduction) allocated to EBN-FSR 1 to the

- simultaneous occurrence of independent failures on both electrical power supply terminals, i.e. simultaneous violation of EBN-FSR 1.1 and EBN-FSR 1.2, with a PMHF budget of 5 FIT
- occurrence of dependent failures, i.e. violation of EBN-FSR 1.3, with a PMHF budget of 5 FIT

as well as the symmetric distribution of the PMHF budgets of both EBN channels Kl30_s1 and Kl30_s2, the following exemplary target values ensue. The symmetric distribution of the PMHF budgets between the redundant terminals Kl30_s1 and Kl30_s2 can therefore be applied as this scenario entails no additional requirements (e.g. by numerous other manual SR-Vehicle-Functions or further QM convenience functions) for Kl30_s1.

- PMHF_bud (EBN-FSR 1.1): 790 FIT
- SPFM_bud (EBN-FSR 1.1): 90 %
- LFM_bud (EBN-FSR 1.1): n.a.

- PMHF_bud (EBN-FSR 1.2): 790 FIT
- SPFM_bud (EBN-FSR 1.2): 90 %
- LFM_bud (EBN-FSR 1.2): n.a.

- PMHF_bud (EBN-FSR 1.3): 5 FIT
- SPFM (EBN-FSR 1.3): 99 %
- LFM (EBN-FSR 1.3): 90 %

In the next step, the requirements resulting from EBN-FSR 1.1 and EBN-FSR 1.2 will be allocated to the subordinate subrequirements of the individual EBN channels according to EBN-FSR 1.1.1, 1.1.2 and 1.1.3 and EBN-FSR 1.2.1, 1.2.2 und 1.2.3. Using this allocation, the following target metrics can be defined as an example:

Power feed

- PMHF_bud (EBN-FSR 1.1.1): 680 FIT
- SPFM_bud (EBN-FSR 1.1.1): 90 %
- LFM_bud (EBN-FSR 1.1.1): n.a.

Power distribution

- PMHF_bud (EBN-FSR 1.1.2): 30 FIT
- SPFM_bud (EBN-FSR 1.1.2): 90 %
- LFM_bud (EBN-FSR 1.1.2): n.a.

Freedom from interference

- PMHF_bud (EBN-FSR 1.1.3): 80 FIT
- SPFM_bud (EBN-FSR 1.1.3): 90 %
- LFM_bud (EBN-FSR 1.1.3): n.a.

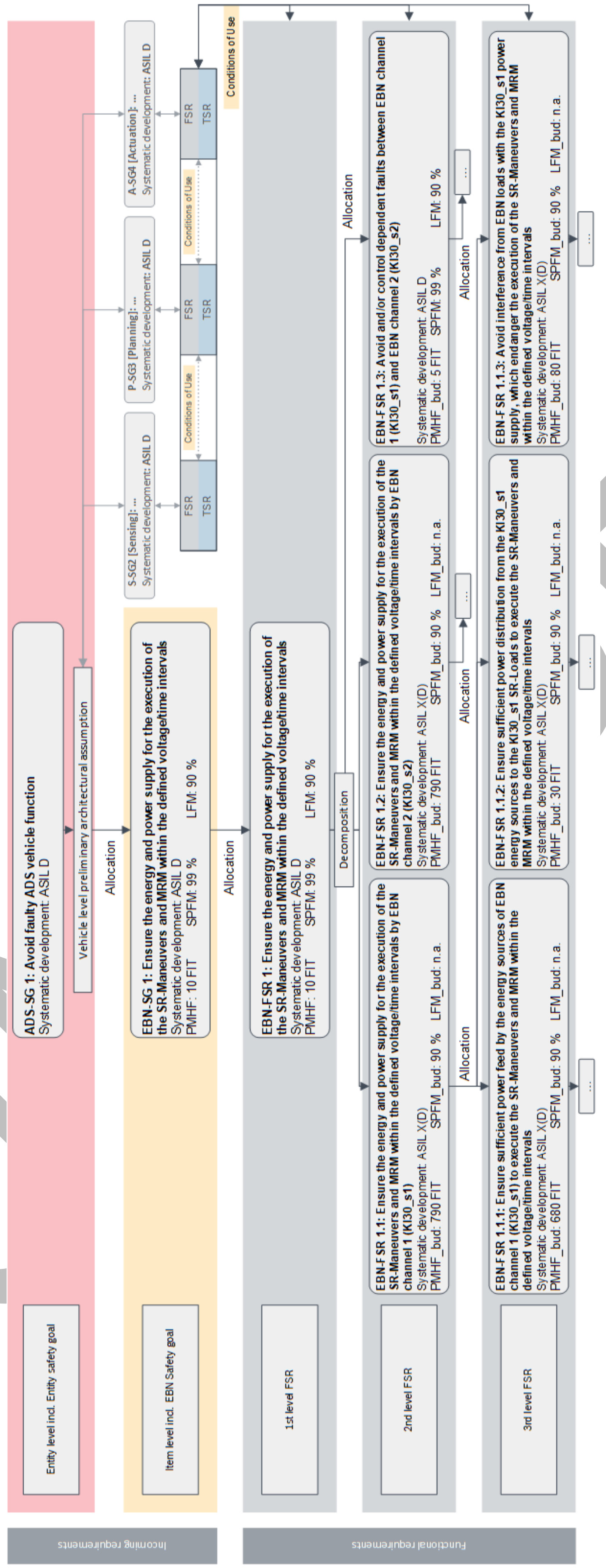

Incoming requirements
Functional requirements
Entity level incl. Entity safety goal
Item level incl. EBN Safety goal
1st level FSR
2nd level FSR
3rd level FSR
ADS-SG 1: Avoid faulty ADS vehicle function
Systematic development: ASIL D
Vehicle level preliminary architectural assumption
S-SG2 [Sensing]: ...
Systematic development: ASIL D
P-SG3 [Planning]: ...
Systematic development: ASIL D
A-SG4 [Actuation]: ...
Systematic development: ASIL D
FSR
TSR
Conditions of Use
Allocation
EBN-SG 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
PMHF: 10 FIT SPFM: 99 % LFM: 90 %
EBN-FSR 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
PMHF: 10 FIT SPFM: 99 % LFM: 90 %
Decomposition
EBN-F SR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 1 (Kl30_s1)
Systematic development: ASIL X(D)
PMHF_bud: 790 FIT SPFM_bud: 90 % LFM_bud: n.a.
EBN-F SR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 2 (Kl30_s2)
Systematic development: ASIL X(D)
PMHF_bud: 790 FIT SPFM_bud: 90 % LFM_bud: n.a.
EBN-F SR 1.3: Avoid and/or control dependent faults between EBN channel 1 (Kl30_s1) and EBN channel 2 (Kl30_s2)
Systematic development: ASIL D
PMHF_bud: 5 FIT SPFM: 99 % LFM: 90 %
EBN-F SR 1.1.1: Ensure sufficient power feed by the energy sources of EBN channel 1 (Kl30_s1) to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
PMHF_bud: 680 FIT SPFM_bud: 90 % LFM_bud: n.a.
EBN-F SR 1.1.2: Ensure sufficient power distribution from the Kl30_s1 energy sources to the Kl30_s1 SR-Loads to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
PMHF_bud: 30 FIT SPFM_bud: 90 % LFM_bud: n.a.
EBN-F SR 1.1.3: Avoid interference from EBN loads with the Kl30_s1 power supply, which endanger the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
PMHF_bud: 80 FIT SPFM_bud: 90 % LFM_bud: n.a.
...

Fig. 17: Metrics derivation for scenario A

The exemplary PMHF target metrics in EBN-FSR 1.1.1 and EBN-FSR 1.2.1 were specifically selected to provide the option of dispensing with a second source in the respective EBN channels Kl30_s1 or Kl30_s2. Possible forms of implementation are

- to supply terminal Kl30_s2, without a storage device, with an Active Source from a higher voltage level
- when using a 12 V separating Element according to the case study in Annex C, to supply terminal Kl30_s2, after separation of the terminal, only from a Passive Source – without taking into account the Active Source in the safety concept.

Note: In comparison with terminal Kl30_s2 in scenario B, additional safety mechanisms must be introduced as only a significantly lower PMHF budget is available in case of a failure of terminal Kl30_s2. For EBN-FSR 1.1.2, a lower PMHF budget is specified compared to the requirements for the energy sources as per EBN-FSR 1.1.1, as passive separating and connecting Elements usually have relatively low PMHF values. When budgeting for the avoidance of interferences according to EBN-FSR 1.1.3, it is assumed that safety mechanisms such as ATVs are implemented. As high PMHF values for the occurrence of interferences are to be expected in practice, the derived target values can usually not be achieved in any other way.

Due to the symmetric allocation of requirements to the two EBN channels Kl30_s1 and Kl30_s2, the objective, in practice, is to implement both terminals identically, if possible. This is initially a contradiction to the boundary conditions of a decomposition, as the latter requires sufficient independence of both EBN channels Kl30_s1 und Kl30_s2 as described in chapter 4.2. If both EBN channels are implemented in a comparable manner, a homogenous redundancy might be possible. For this reason, measures according to chapter 4.2, in particular 4.2.2.3, must be taken.

Scenario B: Additional capability of the basic electrical power supply in accordance with ASIL B/C:

To derive the requirements for EBN channels Kl30_s1 and Kl30_s2 according to EBN-FSR 1.1 and EBN-FSR 1.2, an ASIL decomposition is performed analogous to scenario A. The result of the requirement derivation in terms of quantitative target metrics is illustrated in Figure 18.

Due to the boundary conditions of a decomposition in accordance with chapter 4.2, dependent failures of both electrical power supply channels must be avoided, cf. EBN-FSR 1.3. To allow for a scalable EBN design, scenario B takes into account additional ASIL B/C requirements from SR functions in the context of manual driving when deriving the quantitative target metrics for EBN-FSR 1.1. The accompanying strict requirements for terminal Kl30_s1 result in a comparatively large PMHF budget for the redundant terminal Kl30_s2. From the perspective of functional safety, this PMHF budget can be used to dispense with redundant sources in EBN channel Kl30_s2. Possible forms of implementation are

- to supply terminal Kl30_s2, without a storage device, with an Active Source from a higher voltage level
- when using a 12 V separating Element according to the case study in Annex C, to supply terminal Kl30_s2, after separation of the terminal, only from a Passive Source – without taking into account the Active Source in the safety concept

In case of a symmetric distribution of the PMHF target value of 10 FIT (cf. introduction) allocated to EBN-FSR 1 to the

- simultaneous occurrence of independent failures on both electrical power supply terminals, i.e. simultaneous violation of EBN-FSR 1.1 and EBN-FSR 1.2, with a PMHF budget of 5 FIT
- occurrence of dependent failures, i.e. violation of EBN-FSR 1.3, with a PMHF budget of 5 FIT

the following exemplary target values ensue:

- PMHF (EBN-FSR 1.1): 100 FIT
- SPFM (EBN-FSR 1.1): 90% (at ASIL B) / 97% (at ASIL C)
- LFM (EBN-FSR 1.1): 60% (at ASIL B) / 80% (at ASIL C)

- PMHF_bud (EBN-FSR 1.2): 6250 FIT
- SPFM_bud (EBN-FSR 1.2): 90 %
- LFM_bud (EBN-FSR 1.2): n.a.

- PMHF_bud (EBN-FSR 1.3): 5 FIT
- SPFM (EBN-FSR 1.3): 99%
- LFM (EBN-FSR 1.3): 90%

For EBN-FSR 1.3, additional requirements regarding SPF and RF are to be taken into account as described in ISO 26262-5:2018, 9.4.1.2 and 9.4.1.3, as these are potential single faults that might violate the Safety Goal. If ASIL C requirements from the use case "manual driving" are to be taken into account, this also applies to terminal Kl30_s and thus to the safety requirement EBN-FSR 1.1.

In the next step, the requirement arising from EBN-FSR 1.1 is allocated to the subordinate subrequirements EBN-FSR 1.1.1, 1.1.2 und 1.1.3. Using this allocation, the following exemplary target metrics can be defined:

Power feed

- PMHF_bud (EBN-FSR 1.1.1): 50 FIT
- SPFM (EBN-FSR 1.1.1): 90% (for ASIL B) / 97% (for ASIL C)
- LFM (EBN-FSR 1.1.1): 60% (for ASIL B) / 80% (for ASIL C)

Power distribution

- PMHF_bud (EBN-FSR 1.1.2): 10 FIT
- SPFM (EBN-FSR 1.1.2): 90% (for ASIL B) / 97% (for ASIL C)
- LFM (EBN-FSR 1.1.2): 60% (for ASIL B) / 80% (for ASIL C)

Freedom from interference

- PMHF_bud (EBN-FSR 1.1.3): 40 FIT
- SPFM (EBN-FSR 1.1.3): 90% (for ASIL B) / 97% (for ASIL C)
- LFM (EBN-FSR 1.1.3): 60% (for ASIL B) / 80% (for ASIL C)

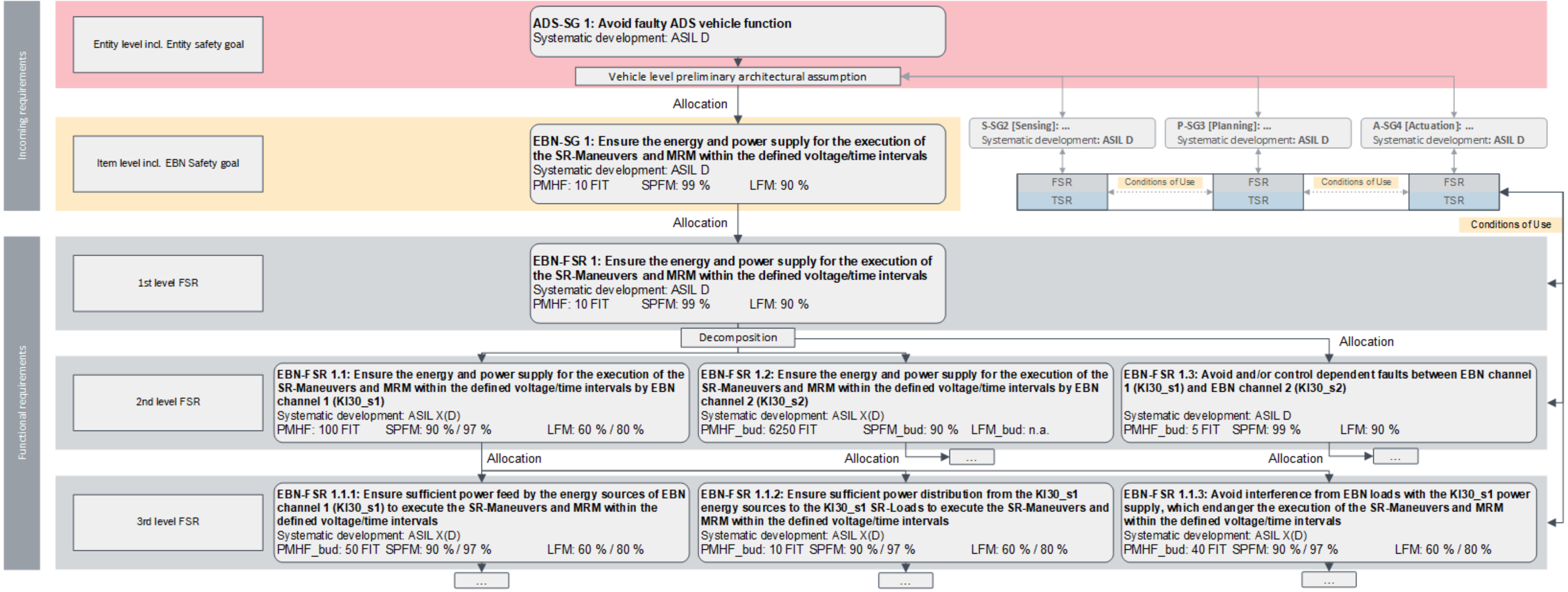

Incoming requirements
Functional requirements
Entity level incl. Entity safety goal
Item level incl. EBN Safety goal
1st level FSR
2nd level FSR
3rd level FSR
ADS-SG 1: Avoid faulty ADS vehicle function
Systematic development: ASIL D
Vehicle level preliminary architectural assumption
Allocation
S-SG2 [Sensing]: ...
Systematic development: ASIL D
P-SG3 [Planning]: ...
Systematic development: ASIL D
A-SG4 [Actuation]: ...
Systematic development: ASIL D
FSR
TSR
Conditions of Use
EBN-SG 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
PMHF: 10 FIT SPFM: 99 % LFM: 90 %
Allocation
EBN-FSR 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
PMHF: 10 FIT SPFM: 99 % LFM: 90 %
Decomposition
Allocation
EBN-FSR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 1 (Kl30_s1)
Systematic development: ASIL X(D)
PMHF: 100 FIT SPFM: 90 % / 97 % LFM: 60 % / 80 %
EBN-FSR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 2 (Kl30_s2)
Systematic development: ASIL X(D)
PMHF_bud: 6250 FIT SPFM_bud: 90 % LFM_bud: n.a.
EBN-FSR 1.3: Avoid and/or control dependent faults between EBN channel 1 (Kl30_s1) and EBN channel 2 (Kl30_s2)
Systematic development: ASIL D
PMHF_bud: 5 FIT SPFM: 99 % LFM: 90 %
Allocation
...
EBN-FSR 1.1.1: Ensure sufficient power feed by the energy sources of EBN channel 1 (Kl30_s1) to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
PMHF_bud: 50 FIT SPFM: 90 % / 97 % LFM: 60 % / 80 %
EBN-FSR 1.1.2: Ensure sufficient power distribution from the Kl30_s1 energy sources to the Kl30_s1 SR-Loads to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
PMHF_bud: 10 FIT SPFM: 90 % / 97 % LFM: 60 % / 80 %
EBN-FSR 1.1.3: Avoid interference from EBN loads with the Kl30_s1 power supply, which endanger the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
PMHF_bud: 40 FIT SPFM: 90 % / 97 % LFM: 60 % / 80 %

Fig. 18: Metrics derivation for scenario B

The PMHF target metrics were selected in way to ensure that, by using the redundancy, high PMHF values of passive 12 V energy sources in EBN-FSR 1.1.1 can be compensated to the active 12 V energy source. Budgeting for the safety requirements EBN-FSR 1.1.2 und EBN-FSR 1.1.3 is performed analogous to scenario A. When budgeting for the avoidance of interferences (cf. safety requirement EBN-FSR 1.1.3), the assumption was made, as in scenario A, that safety mechanisms such as ATVs are implemented.

The requirements of the target metrics of Scenario A and Scenario B are compared in Table 6.

PMHF(_bud)
SPFM(_bud)
LFM(_bud)
	EBN-FSR 1	EBN-FSR 1.1	EBN-FSR 1.2	EBN-FSR 1.3	EBN-FSR 1.1.1	EBN-FSR 1.1.2	EBN-FSR 1.1.3

Scenario A: Singular analysis of the ASIL D use case (ADS-SG1)	10 FIT 99% 90%	790 FIT 90% n.a.	790 FIT 90% n.a.	5 FIT 99% 90%	680 FIT 90% n.a.	30 FIT 90% n.a.	80 FIT 90% n.a.
Scenario B: Additional capability of the basic EBN according to ASIL B/C	10 FIT 99% 90%	100 FIT 90% / 97% 60% / 80%	6250 FIT 90% n.a.	5 FIT 99% 90%	50 FIT 90% / 97% 60% / 80%	10 FIT 90% / 97% 60% / 80%	40 FIT 90% / 97% 60% / 80%

Tab. 7: Summary of the exemplary allocation of ISO 26262:2018 target metrics to the Safety Goals and requirements of chapter 5.2

In the next step, the requirements for the quantitative target metrics are iteratively matched at component level with the required PMHFs, cf. example 1. If the budget defined in an interface agreement is not sufficient,

− the budgets must be adjusted iteratively (i.e. redistributed) or

− the EBN or component design must be optimized in terms of the required PMHF budget.

When adjusting the budget, compliance with the target metrics of the original requirement at Item level must also be proven. That means that in case of an allocation of a higher budget to a first requirement, the budget allocated to a second requirement must be reduced in such a manner that the allocation of the higher budget to the first requirement can be compensated for.

Example 1: Using the example of the EBN topology from the case study in Annex C, a QM consumer is allocated to the safety-relevant terminal Kl30_s1_B to implement post-crash requirements; this allocation is subject to the following assumptions:

a) The QM consumer generates interferences at an FIT rate of λ_V = 200 FIT.

b) To ensure freedom from interference, an active separating Element EBN[SR]-L[QM] matching type 4 in chapter 6.4 is held in reserve.

c) The inability to separate interferences is assessed with a basic failure rate of λ_T = 30 FIT.

d) The Safety Mechanism to detect and separate the interference reaches the following Diagnostic Coverage values for the sample calculations below: DC_Rück1 = 99%, DC_Rück2 = 99.9%, DC_Rück3 = 100%.

e) The SM of the active separating element to detect an inability to separate reaches an exemplary Diagnostic Coverage of DC_Trenn = 90%.

f) Continued travel with the detected non-separable active separating Element is permissible for a period of t_EOTTI = 1 h.

g) The operating time is set to t = 8,000 h.

Note: As a matter of principle, the analyzed failure rates are dependent on the design and the operating conditions of the components and must therefore be determined individually for each specific application. The λ_V values are dependent, for example, on the interference looked at (e.g. short-circuit to ground, increased power consumption, …) and must be determined individually for each consumer. Dependent on the interference looked at and its effect on the EBN, different SMs can be applied. Due to the complexity of the matter to be monitored and the technical implementation of the SM, different DCs may result for different SMs. In this example, the same λ_V value is assumed for the calculation, for simplicity's sake, while the DC_Rück is varied from DC_Rück1 to DC_Rück3 to demonstrate its influence.

For an approximate calculation of the PMHF, ISO 26262-10:2018, 8.3.2.3 can be consulted. In doing so, pattern 3 can be neglected for this example, as all separated short-circuits are detected in the system and transitioning to a safe state is initiated. Pattern 4 is also neglected, as a random hardware failure in the separating mechanism during transition to a safe state after successful separation can be assumed to be sufficiently unlikely due to the little influence on the PMHF. It is therefore neglected.

Using these simplified assumptions, the following approximation ensues for the PMHF_bud of the EBN channel Kl30_s1_B regarding freedom from interference (cf. requirement PMHF_bud (EBN-FSR 1.1.3)), which comprises:

- Residual Fault regarding the requirement EBN-FSR 1.1.3 for the EBN channel Kl30_s1_B due to a non-perfect diagnosis (DC_1 to DC_3) – this corresponds to an MPF at EBN level
- MPF of the EBN channel Kl30_s1_B due to the latent failure of the separating Element – non-separable – in combination with a short circuit according to pattern 1 from ISO 26262-10:2018, 8.3.2.4.
- MPF of the EBN channel Kl30_s1_B due to a fault of the QM consumer during the EOTTI after detection of non-separable ATV according to pattern 2 from ISO 26262-10:2018, 8.3.2.4.

PMHF_bud(EBN-FSR 1.1.3)

$\approx[(1\text{-DC\_Rück})\cdot\lambda\text{\_V}+0{,}5\cdot(1\text{-DC\_Trenn})\cdot\lambda\text{\_T}\cdot\text{DC\_Rück}\cdot\lambda\text{\_V}\cdot t$

$+\ 0.5\cdot\text{DC\_Trenn}\cdot\lambda\text{\_T}\cdot\text{DC\_Rück}\cdot\lambda\text{\_V}\cdot\text{t\_EOTTI}]$

The results for PMHF_bud(EBN-FSR 1.1.3), taking into account the introduced sample values, can be found in Table 7.

Case	RF [FIT]	Pattern1 [FIT]	Pattern2 [FIT]	Sum [FIT]
DC_Rück1 = 99%	2	0.0023	~ 0	~ 2
DC_Rück2 = 99.9%	0.2	0.0024	~ 0	~ 0.2
DC_Rück3 = 100%	0	0.0024	~ 0	~ 0.002

Tab. 8: Calculation of the PMHF_bud (EBN-FSR 1.1.3) dependent on DC_Rück

F. Application of ISO 26262:2018 Time Intervals to the Electrical Power Supply

Below, the timing requirements for the 4.5 V voltage threshold in example 1 and the timing requirements for the 18 V threshold in example 2 are derived by way of example. In the requirement derivation in Fig. 19, only the FHTTI values of the 4.5 V threshold are illustrated for reasons of simplicity. In doing so, the development of all voltage/time intervals derived must be taken into account.

Note: In addition to the voltage threshold specified in example 1 and example 2, all other safety-relevant safety/time intervals must be safeguarded with safety measures at an appropriate integrity level. An overview of the voltage/time intervals is presented in chapter 4.1.3.

Example 1 "Derivation of the FHTTI for the 4.5 V voltage threshold":

Via the "Conditions of Use" of the steering control unit, one of the requirements placed on the EBN is that a voltage of <= 4.5 V must be avoided for t >= 100 µs (cf. EBN-FSR 2 from chapter 4.1.3).

This requirement is derived from the fact that in the event of a critical undervoltage of U <= 4.5 V, a steering control unit executing the SR function Lateral Control is already unavailable after t >= 100 µs due to a reset. The steering control unit requires a start-up time of 2 s until the lateral control is available again after a reset. Thus, the duration of the lateral control's non-availability due to reset is much longer than the specified FTTI_ADS_FSR_1 of 80 ms in chapter 4.1.1. The FTTI_EBN_SG1 to avoid a critical undervoltage of 4.5 V is therefore not 80 ms but must be reduced to 100 µs. This correlation is illustrated in Fig. 19.

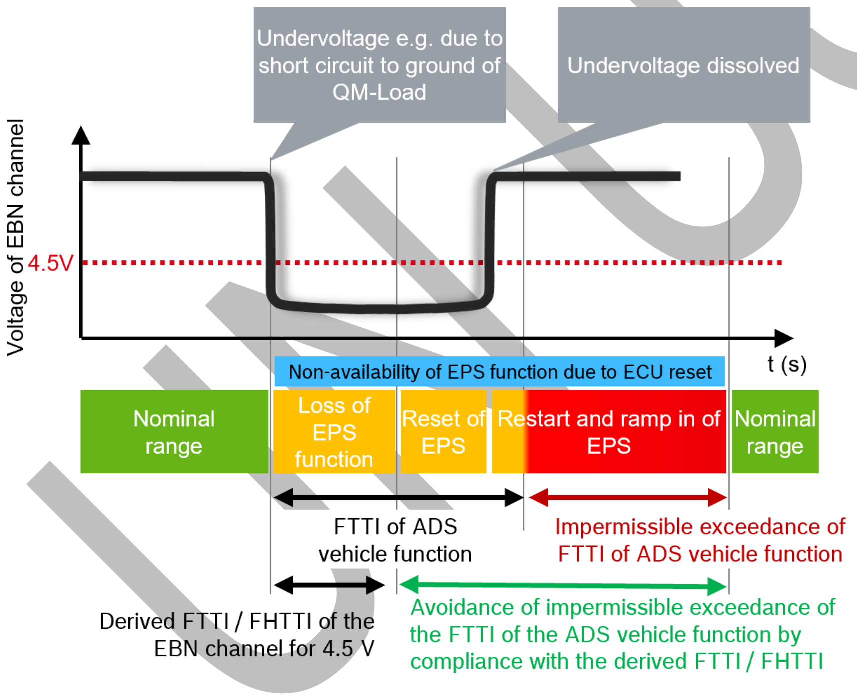
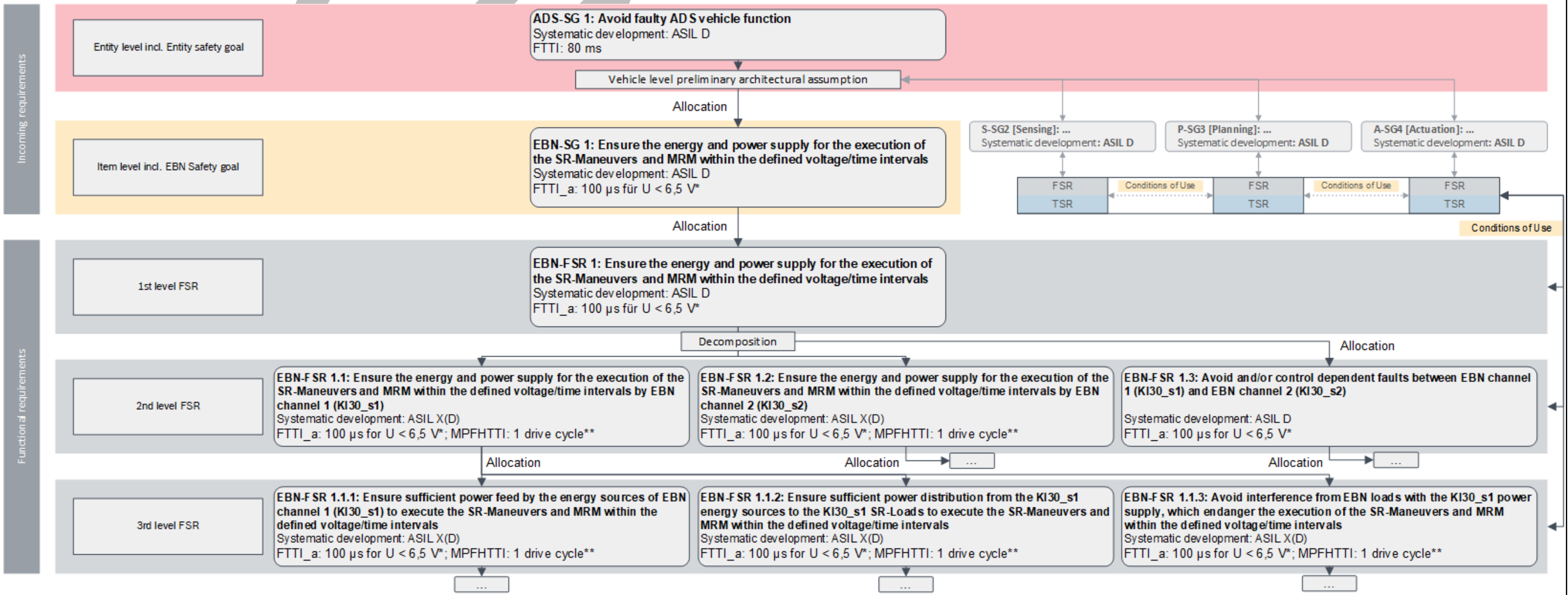

Undervoltage e.g. due to short circuit to ground of QM-Load
Undervoltage dissolved
Voltage of EBN channel
4.5V
t (s)
Non-availability of EPS function due to ECU reset
Nominal range
Loss of EPS function
Reset of EPS
Restart and ramp in of EPS
Nominal range
FTTI of ADS vehicle function
Impermissible exceedance of FTTI of ADS vehicle function
Derived FTTI / FHTTI of the EBN channel for 4.5 V
Avoidance of impermissible exceedance of the FTTI of the ADS vehicle function by compliance with the derived FTTI / FHTTI

Fig. 19: Derivation of the FTTI / FHTTI for the EBN using the example of steering

Note: The FHTTI can be selected for longer than 100 µs if appropriate measures to avoid a reset for a time greater than 100 µs are implemented in all SR-Loads. In the process, the SR-Loads that place a safety-relevant availability requirement on the EBN and might violate the FTTI from ADS-SG 1 must be taken into account.

A use of the exemplary voltage/time interval "< 6.5 V für 100 µs" in chapter 4.1.3 results in the EBN requirement derivation illustrated in Fig. 20.


Incoming requirements
Functional requirements
Entity level incl. Entity safety goal
Item level incl. EBN Safety goal
1st level FSR
2nd level FSR
3rd level FSR
ADS-SG 1: Avoid faulty ADS vehicle function
Systematic development: ASIL D
FTTI: 80 ms
Vehicle level preliminary architectural assumption
Allocation
S-SG2 [Sensing]: ...
Systematic development: ASIL D
P-SG3 [Planning]: ...
Systematic development: ASIL D
A-SG4 [Actuation]: ...
Systematic development: ASIL D
FSR
TSR
Conditions of Use
FSR
TSR
Conditions of Use
FSR
TSR
Conditions of Use
EBN-SG 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
FTTI_a: 100 µs für U < 6,5 V*
Allocation
EBN-FSR 1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL D
FTTI_a: 100 µs für U < 6,5 V*
Decomposition
Allocation
EBN-FSR 1.1: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 1 (KI30_s1)
Systematic development: ASIL X(D)
FTTI_a: 100 µs for U < 6,5 V*; MPFHTTI: 1 drive cycle**
EBN-FSR 1.2: Ensure the energy and power supply for the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals by EBN channel 2 (KI30_s2)
Systematic development: ASIL X(D)
FTTI_a: 100 µs for U < 6,5 V*; MPFHTTI: 1 drive cycle**
EBN-FSR 1.3: Avoid and/or control dependent faults between EBN channel 1 (KI30_s1) and EBN channel 2 (KI30_s2)
Systematic development: ASIL D
FTTI_a: 100 µs for U < 6,5 V*
Allocation
Allocation
Allocation
...
...
EBN-FSR 1.1.1: Ensure sufficient power feed by the energy sources of EBN channel 1 (KI30_s1) to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
FTTI_a: 100 µs for U < 6,5 V*; MPFHTTI: 1 drive cycle**
EBN-FSR 1.1.2: Ensure sufficient power distribution from the KI30_s1 energy sources to the KI30_s1 SR-Loads to execute the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
FTTI_a: 100 µs for U < 6,5 V*; MPFHTTI: 1 drive cycle**
EBN-FSR 1.1.3: Avoid interference from EBN loads with the KI30_s1 power supply, which endanger the execution of the SR-Maneuvers and MRM within the defined voltage/time intervals
Systematic development: ASIL X(D)
FTTI_a: 100 µs for U < 6,5 V*; MPFHTTI: 1 drive cycle**
...
...
...

*exemplary values; derivation of the full set of FTTI / FHTImax acc. To defined voltage/time intervals, cf. chapter 4.1.3

** Default value acc. to ISO 26262-5:2018, 6.4.8 Note 1; Deviations possible, see chapter 4.2.3.4

Fig. 20: Exemplary derivation of the FHTTI / MPFHTTI for the EBN

Example 2 "Derivation of the FHTTI for the 18 V voltage threshold":

An overvoltage of > 18 V and <= 27 V for t = 10 ms (cf. EBN_CU-FSR 1 in chapter 4.1.3) leads to a loss of the steering function. After an overvoltage shutdown, the steering needs 20 ms, for example, to return to the EBN nominal voltage range until the SR function "lateral control" is available again.

In this example, this results in a voltage-dependent FTTI or FHTTI of the EBN for U > 18 V of 70 ms - consisting of the following time intervals:

- + 10 ms until shutdown of the SR function Lateral Control
- + 80 ms permissible non-availability of the SR function Lateral Control (FHTTI from ADS-SG 1)
- – 20 ms until the SR function Lateral Control is available again as soon as the EBN voltage returns to the nominal range.

G. Further Documents and Working Groups on the Topic "Electrical Power Supply for Automated Driving"

Document	Title	Author	Relevance
FIDES guide 2009 Edition A	Reliability Methodology for Electronic Systems	FIDES Group, under the supervision of the French ministry of defense FIDES Group: AIRBUS France, Eurocopter, Nexter Electronics, MBDA France, Thales Systèmes Aéroportés SA, Thales Avionics, Thales Corporate Services SAS and Thales Underwater Systems.	Catalogue for the calculation of failures rates of E/E components.
ISO 16750 volume 1 to 5	Road vehicles – Environmental conditions and electrical testing for electrical and electronic equipment	International Organization for Standardization	Definition of environmental damage for E/E systems dependent on their installation location; recommendation of requirements and tests
SN 29500 part 1 to part 16	Failure rates components	Siemens	Catalogue for the calculation of failure rates of E/E components.
MIL HDBK 217f	Military Handbook Reliability Prediction of Electronic Equipment	US Defense Department	Catalogue for the calculation of failure rates of E/E components.
N/A	Ausfallraten für Bordnetz-Komponenten im Automobil	ZVEI	Catalogue for the calculation of failure rates of E/E components of the physical power supply system.

ISO 21780	Road vehicles – Supply voltage of 48 V – Electric requirements and tests	International Organization for Standardization	Definition of tests and voltage ranges of 48 V components.
ISO 8820			

Consortium	**Working Group**	**Relevance**
CBI (Consortium for Battery Innovation)	Safety State of Function	Standardization for energy and performance forecasts of automotive batteries.
VDA	GRVA	Revision of R79 / R79H in the context of X-by-Wire