An Approach of Fail Operational Power Supply for Next Generation Vehicle Powernet Architectures

Armin Köhler

Automotive Electronics, Product Area Energy Management Powernet - Architecture (AE-BE/PAN2), Robert Bosch GmbH, Germany. E-mail: armin.koehler3@de.bosch.com, armin.koehler@ima.uni-stuttgart.de

Prof. Dr.-Ing. Bernd Bertsche

Institute of Machine Components, University of Stuttgart, Germany. E-mail: bernd.bertsche@ima.uni-stuttgart.de

This technical elaboration evaluates state of the art powernets regarding functional safety aspects, considering ISO 26262. Increasing safety requirements due to market trends as well as gaps in current powernets and development processes are derived. It is stated out, why these processes cannot be applied for future powernets anymore. These challenges are illustrated by introducing the impact on Electric Power Steering (EPS) systems. Additionally, new awareness for the use of functional safety in systems engineering for safe power supply will be created. Problem solving approaches and technical measures, achieving new functional safety targets are demonstrated. Looking into a safe future for automated vehicles, necessary steps for next generation powernet topology designs are pointed out. Regarding this, a system solution on component- and powernet level for safe supplied EPS systems is presented. The results of this investigation are very valuable for safety engineers and assessors dealing with technical and safety relevant systems.

Keywords: Availability, Electric Power Steering (EPS), Functional Safety, ISO 26262, Powernet, Reliability, Requirements, Safe Supply, Safety Measures.

1. Introduction

The automotive sector is currently driven by the global megatrends electrification and automation. Accordingly, most of the conventional developed and novel vehicle systems are electrical and/or electronic (E/E) systems, which are responsible for safety of drivers. Thereby, the basis of system functionality is always the sufficient power supply. With Automated Driving (AD) functionality in particular, the safety relevance of vehicle powernets and related components increases enormously. For this reason, the whole powernet has to be developed and assessed according to functional safety standards. Especially in the sector of road vehicles, the functional safety process with extensive safety analysis according to ISO 26262 has to be applied [ISO 26262-4:2018(E)].

The current development process of powernets is limited to the analysis of voltage stability and load balance. Future powernet developments additionally need to consider legislation, technical standards, functional safety and reliability. Additionally to enhanced functionality on component level (e.g. Electric Power Steering), various technical safety measures are getting inevitable on powernet level such as:

- redundancy in powernet system design,
- power distribution units,
- intelligent switching modules,
- system diagnoses / Prognostics and Health Management.

A closer look on the market needs has shown that faults of electric components, like a short circuit, can lead to low voltage or a complete breakdown of the powernet. Therefore, there is the necessity for an adapted power supply architecture even for manual driving. The market also shows a trend for increasing vehicle weights for SUVs and Battery Electric Vehicles (BEVs) (rising axle loads) [Statista (2020)] and more Advanced Driver Assistance Systems (ADAS). Therefore more and more safe power supply solutions that fulfill an “ASIL C” rating become mandatory.

Especially the conventional Electric Power Steering (EPS) has considerably rising Safety Related Availability (SaRA) requirements. This is based on the failure scenario “sudden loss of steering assist” due to e.g. occurring power supply faults. These faults reflect e.g. a malfunction where power supply falls below the specified voltage-time limit and therefore an additional technical measure to avoid this drop is inevitable. It is obvious that the requirements

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

beyond the steering system still cause uncertainty and that technical solutions fulfilling these requirements are discussed extensively.

This technical elaboration evaluates state of the art powernets regarding functional safety aspects, considering ISO 26262. It also covers increasing safety requirements due to market trends like electrification and automation as well as gaps in current powernets and development processes, which cannot be applied for future powernets anymore. These challenges are illustrated by introducing the impact on EPS steering systems. Additionally new awareness for the use of functional safety in systems engineering for safe power supply will be created. Problem solving approaches and technical measures, achieving new functional safety targets and showing necessary steps for next generation powernet and topology designs are displayed. Regarding this, a system solution on component- and powernet level for safe supplied EPS systems is presented. The results of this investigation are very valuable for safety engineers and assessors dealing with technical and safety relevant systems.

1.1 *Safety Trends*

The past few years showed some major changes and trends in the vehicle market. That affects combustion engine vehicles, especially SUVs, as well as BEVs. It is described, that these trends do have a huge impact on safety related functions on component- and powernet level.

1.1.1 *Increasing vehicle weight*

One of the major trends is the increasing vehicle weight. Statistics of the German "Kraftfahrt-Bundesamt" published by Statista (2020) confirm continuous rising values at new registered vehicles in Germany. Because of increasing vehicle weight, the rack force needed to steer the vehicle rises. In case of sudden loss of assist in the EPS system the driver has to perform manual steering with suddenly significantly increased steering wheel torque. The controllability is getting worse. That leads to new challenges for steering hazardous events.

1.1.2 *Advanced Driver Assistance Systems*

The second major trend is the increasing global market development for ADAS systems. These systems and functionalities are essential for AD vehicles. Each step to higher SAE automated driving Level, according to SAE J3016 (2018), accompanies specific standards for vehicle behaviour. Giving an example for SAE Level 1 and Level 2 AD vehicles. At Level 1 the driver is continuously exercising longitudinal or lateral control. Thereby, the lateral or longitudinal control is accomplished by the system. At Level 2 the system has longitudinal and lateral control in specific use cases, but the driver has to monitor the system at all times. With increasing AD functionality, the role of driver in vehicle guidance is decreasing. He is getting more and more out of the control loop of the vehicle. This leads to a critical point. In case of risky situations, the driver still needs to take over control of the vehicle. At that moment, the driver needs longer reaction times to get back into the control loop of the vehicle. This leads to new challenges for vehicle controllability e.g. in case of loss of steering assist. [SAE J3016 (2018)]

1.1.3 *Automated Driving*

At least the overall trend for automated driving vehicles leads to several requirements on system, powernet and component level (see Table 1).

Table 1. Effects of automated driving on powernet

	Automated Driving
System Requirements	Fail-operational instead of fail-safe (no driver in the control loop).
Powernet Properties	Two independent powernets.
	Base loads and safety relevant loads share the main powernet.
Component Functions	Powernet monitoring, independent channel isolation and trigger of safe state transmission.
	Powernet firewall: separation of base loads from safety relevant AD system in case of failure.
	Diagnostic function for monitoring of the backup powernet to prevent latent faults.
	Active stimulation to ensure the diagnosability of the backup powernet.

Source: [ECE-R13h (2018)], [ISO 26262 (2018)]

1.2 *State of the Art Powernets*

Current powernet designs do have significant influence on the reliability of the vehicle. Recent vehicle breakdown statistics demonstrate that electronic components are the major proportion of all vehicle faults leading to a breakdown (see Fig. 1). Looking back at previous statistics shows a continuously increasing proportion of electronic faults leading to a breakdown. It increased 12 % in the past 7 years (see Fig. 2). Having regard to implemented E/E systems, which are safety relevant for vehicle controllability, all of these faults potentially lead to a dangerous driving situation or hazardous event.

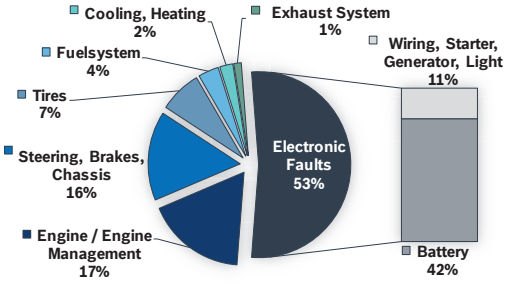

Fig. 1. ADAC breakdown statistics 2019 [ADAC (2020)]

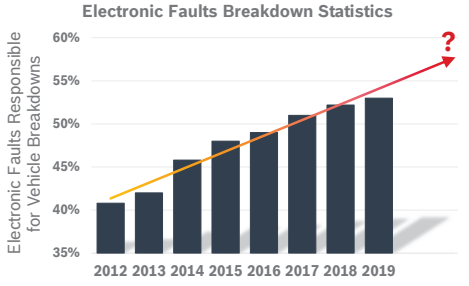

Fig. 2. Electronic faults breakdown statistics [ADAC (2020)]

Figure 3 displays a general powernet architecture as a schematic. The power supply is achieved due to an alternator or electrical machine, a DC/DC-converter and a 12 V battery. Base loads can be either supplied by high voltage (HV) terminal or 12 V side. E.g., base loads could be consumers like seat-heating, infotainment or engine cooling fan. Due to the fact, these consumers do not follow any safety requirements but Quality Management (QM), they are also called QM-consumers. These share the same powernet path with safety relevant consumers like steering EPS, braking, lights, wiper or AD computing functionality. Power distribution- and fuse boxes ensure the power supply to other safety or non-safety relevant consumers, which can also be post-crash consumers like SOS-call. An Electronic Battery Sensor (EBS) usually monitors the voltage stability of the 12 V battery.

With no additional safety measures, a variety of faults can lead to failures in safety related consumers. Giving a few examples, these faults could be for one thing faults of high HV power supply: overvoltage, non-performant DC/DC-converter or unintended activation of QM-Consumers at high voltage terminal. Secondly, faults of power distribution can occur like a high wiring resistance, an unintended fuse burn or a wiring open circuit. Thirdly, faults of the 12 V battery power supply could emerge like a non-performant battery, an open circuit or an aged battery. Finally, all the consumers can have faults like a high quiescent current, unintended activation, an undervoltage or a short circuit. The freedom from interference between safety relevant and non-safety relevant consumers is not given in general. As a result, all of these faults need to be prevented or controlled depending on the target use case.

Evaluating the powernet as a technical system, it is under wide influence of:

- component dimensioning,
- topology design,
- fault reactions (vehicle- and powernet level),
- malfunction behaviour,
- voltage-time limits of consumers,
- operating strategy,
- potential of degradation,
- error handling,
- safety measures,
- diagnoses.

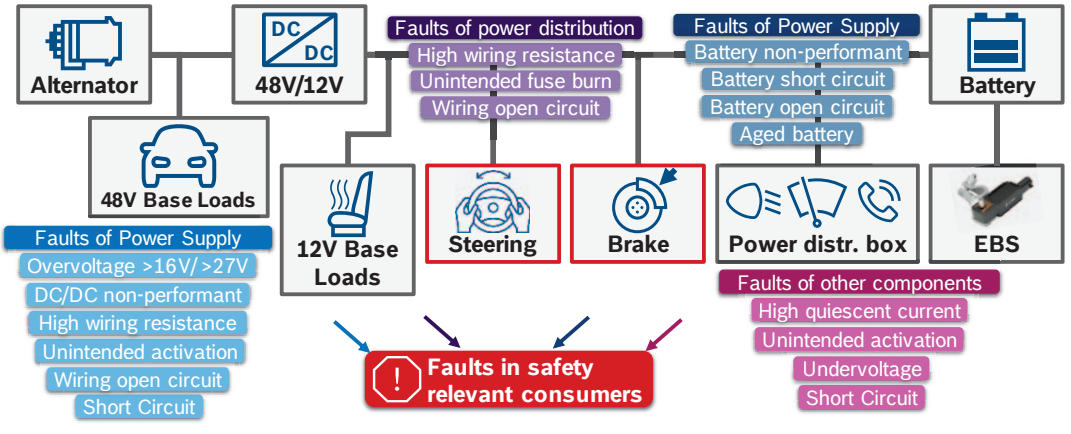

Fig. 3. Schematically powernet topology design

The powernet itself, with all the related components and inherent properties must be treated as one item or system.

2. Functional Safety Aspects

Considering the functional safety requirements in the area of powernet, the following aspects have to be taken into account.

2.1 *Next Generation Powernet Design Process*

The scope of the ISO 26262 is defined as safety related systems that include one or more electrical and/or electronic (E/E) systems [ISO 26262-1:2018(E)]. The wiring harness including splice and connectors is mentioned explicitly as an electrical element with E/E-relevant failure modes [ISO 26262-5:2018(E)]. Thereby, wires, fuses and connectors are mentioned in relation to metric calculation like Single Point Fault Metric (SPFM) and Latent Fault Metric (LFM) [ISO 26262-5:2018(E)]. Thus, the whole powernet development process must be ISO 26262 conform. Figure 4 illustrates an approach of such a development process aiming next generation powernet design process.

2.2 *Functional Safety Concept*

Following the ISO 26262 design process, these steps have to be applied [Gebauer (2018)]:

(i) Hazard Analysis and Risk Assessment (HARA) identifies the functionality the loss of which can lead to a hazardous event with its corresponding Automotive Safety Integrity Level (ASIL) [ISO 26262-3:2018(E)]. The valuation depends on the severity, the exposure and the controllability of the operating scenario.

(ii) The safety goal on the vehicle and its ASIL rating are derived from hazardous events.

(iii) SaRA requirements are derived:
  (a) Specify the functionality needed to prevent the hazardous event.
  (b) Specify the error reaction (emergency operation).
  (c) Specify the safe state.

The derived SaRA requirements are addressed by the following safety measures [Gebauer (2018)]:

- fault prevention,
- fault tolerance (providing the specified functionality),
- fault forecasting and fault detection.

As a result of this process there will be SaRA requirements with different ASIL leading to different safety measures.

2.3 *Current Safety Trends affecting Electronic Power Steering*

A HARA analysis according to the current safety trends mentioned in chapter 1.1 regarding the sudden loss of steering assist performes as shown in Figure 5. Thereby, the classification depends on the target use case. This could be for example:

(i) Driving in a roundabout with a speed more than 40 km/h.

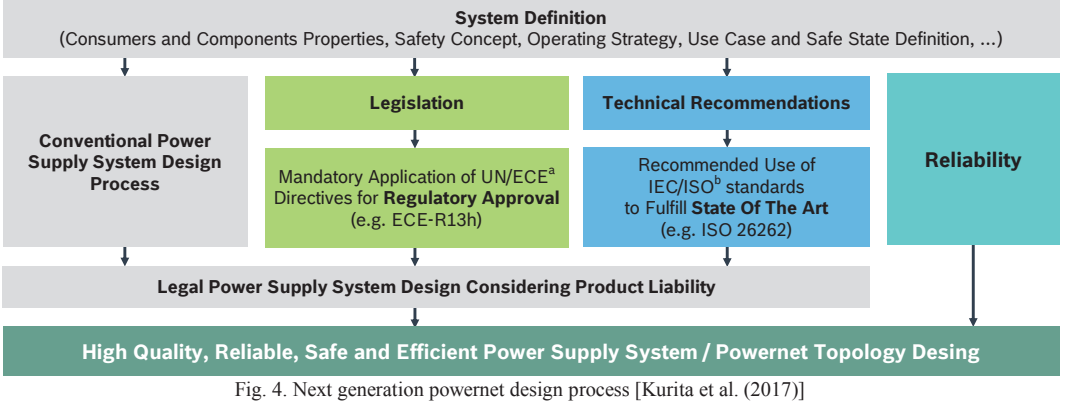

Fig. 4. Next generation powernet design process [Kurita et al. (2017)]

[a] United Nations (UN) / Economic Commission for Europe (ECE)

[b] International Electrotechnical Commission (IEC) / International Organization for Standardization (ISO)

(i) Highway driving situation with a speed more than 120 km/h and high curvature.

The investigation of ASIL rating establish a change for ASIL rating for sudden loss of steering assist from ASIL-B towards ASIL-C. The ASIL for an unintended blocking torque and unintended actuator function is still rated as ASIL-D.

Based on the ASIL definition, different categories according to ISO 26262 are mandatory to be fulfilled. One of the most relevant is the calculation of the Probabilistic Metric for random Hardware Failures (PMHF). It is defined as the average probability per hour over the operational lifetime, see Eq. (1) [ISO 26262-5:2018(E)], [ISO 26262-10:2018(E)].

$$PMHF = \frac{\int_0^{T_L} f(\tau) \cdot d\tau}{T_L} = \frac{F(t)\,|_{t=T_L}}{T_L} . \quad (1)$$

Thereby, operational lifetime only includes operation hours. The unit of PMHF is Failure in Time (FIT), same as it is of the Failure rate λ. Nevertheless, PMHF and λ are different values even if they share the same unit. FIT is defined as the number of failures in 10^9 operating device hours.

Severity Class	Exposure Class	Controllability Class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Fig. 5. Hazard Analysis and Risk Assessment example use case: sudden loss of steering assist [ISO 26262-3:2018(E)]

The second and third metrics are the Single Point Fault Metric (SPFM) and the Latent Fault Metric (LFM). A SPFM/LFM greater than 90 % means, that only 10 % of severe single-point/ latent faults are allowed [ISO 26262-5:2018(E)]. The last two categories describe the necessity of a deductive quantitative failure analysis like a Fault Tree Analysis (FTA) [Bertsche (2008)] and a method finding potential dependent failures: Dependent Failure Analysis (DFA). The different categories and their corresponding target values are listed in Table 2.

Table 2. ASIL requirements

ASIL	QM/A	B	C	D
General Handling	Avoid potential failures by robust and tested design		Control the potential failures	
PMHF	NO	< 100 FIT	< 100 FIT	< 10 FIT
SPFM	NO	≥ 90 %	≥ 97 %	≥ 99 %
LFM	NO	≥ 60 %	≥ 80 %	≥ 90 %
FTA	NO	NO	YES	YES
DFA	NO	NO	YES	YES

Source: [ISO 26262-5:2018(E)]

For the example use case of EPS, the safety goal could be: avoid sudden loss of steering assist. In this case, the corresponding E/E systems like steering components or powernet inherit the associated target values. The vehicle requirements are directly allocated to the power supply system [ISO 26262-5:2018(E)]. Besides these regular requirements, there are additional requirements affecting Residual Faults (RFs) and SPFs of ASIL-C/D systems concerning random hardware faults. Especially, these requirements are:

(i) ASIL-C/D systems with a Diagnostic Coverage lower than 90 % need to achieve every RF < 0.1 FIT for ASIL-C systems and RF < 0.01 FIT for ASIL-D systems.

(ii) ASIL-C/D systems need to achieve every SPF < 0.1 FIT for ASIL-C systems and SPF < 0.01 FIT for ASIL-D systems.

If these target values cannot be met, additional dedicated measures have to be applied [ISO 26262-5:2018(E)]. Therefore, fault exclusion measures in powernet are also required for manual driving.

3. ASIL-C Powernet Approach

In consideration of the system- and powernet requirements given in chapter 1 and 2, an approach of an ASIL-C safe supply powernet architecture is described and evaluated. The focus on that is the ASIL-C of the safety goal "avoid sudden loss of steering assist", the component function, the power supply and the connection of the steering actuator.

3.1 *Requirement Derivation*

A requirement engineering process derives all the SaRA requirements. This process has to be applied to each safety goal. An example excerpt

for the safety goal "avoid sudden loss of steering assist" is shown in Figure 6. Different safety requirements are derived due to requirement allocation or decomposition schemes [ISO 26262-9:2018(E)], [Münzing et al. (2018)]. The whole process leads to several safety requirements regarding component- and powernet level, which need to be fulfilled in the further safety concept. Giving some examples, this could be:

- detect a non-performant battery,
- prevent dual point faults from being latent at battery wiring harness,
- detect increased resistance faults of EPS wiring harness,
- ensure power distribution to EPS connection,
- avoid vehicle QM-components (e.g. engine cooling fan) interfere with power supply,
- ensure power distribution from DC/DC-converter to EPS.

Depending on the specific requirements, various technical safety measures have to be applied.

3.2 *Powernet Architecture*

Facing all the derivable requirements from component and powernet level, a sufficient powernet architectural assumption is presented in Figure 7. The powernet consists out of three terminals: the high voltage side, the terminal 30.0 and terminal 30.1. High voltage QM-consumers are located at the high voltage side together with an Electrical Machine (EM) and/or a high voltage battery. 12 V QM-consumers and parts of the redundant braking system are connected to terminal 30.0 via a fuse box. The remaining safety relevant consumers, like the EPS or braking system, are connected to terminal 30.1 via safety switches. This can be applied in

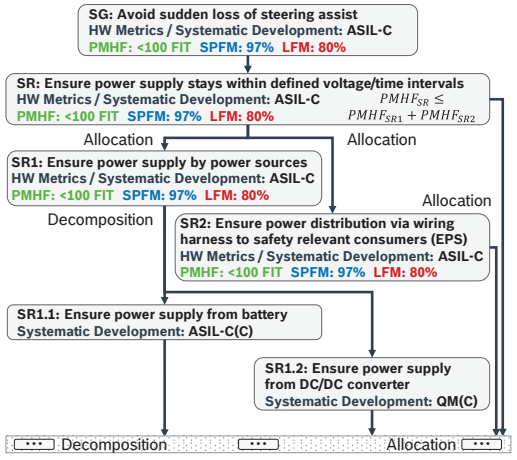

Fig. 6. Example excerpt for requirement derivation

direct connection or via a power distribution box. It can be possible to locate post-crash consumers with QM rating at the power distribution branch. The safe power supply is implemented by redundancy due to the DC/DC-converter and the 12 V battery system.

An intelligent safety switch must be able to disconnect terminal 30.0 and 30.1 immediately, in case a severe failure accurse in one of the terminals, e.g. a short circuit of QM-consumers. By that, independent redundancy of power supply and component functionality can be realized. The safety switches for connection of consumers must ensure the freedom from interference between safety- and non-safety relevant consumers as well as between safety relevant consumers itself. By that, a single channel connection of the EPS system is possible, as long as the component itself is able to fulfil all target values concerning the corresponding ASIL rating (in this case ASIL-C) (see Chapter 3.3 and 3.4). An electronic battery

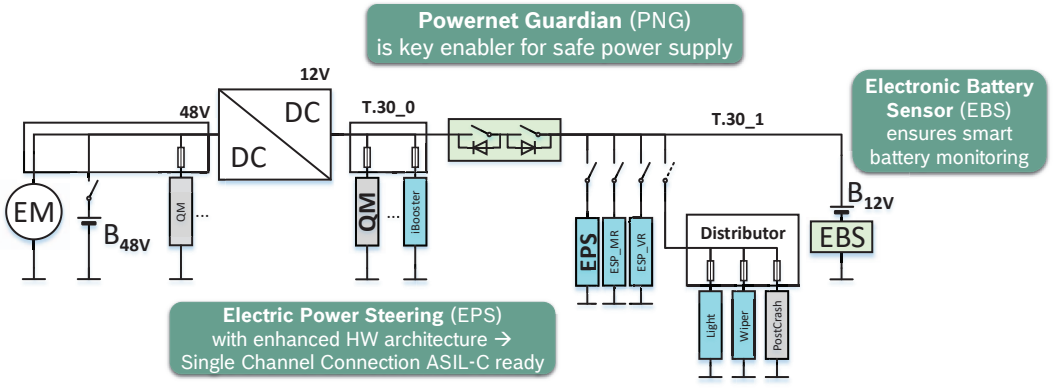

Fig. 7. Manual driving ASIL-C powernet approach

sensor must be able to monitor the battery status regarding state of health and performance. A higher-level system takes control about the safety functionalities and execution of technical safety measures like intelligent switches. Such a system could be called a Powernet Guardian (PNG), which is the key enabler for a safe power supply. All SaRA requirements can be met due to multiple diagnostic functions. This could be for example the control of:

- battery faults leading to non-performant battery,
- faults in wiring harness leading to insufficient power supply
- faults leading to non-performant DC/DC-converter,
- negative effects of QM-consumers,
- separated short circuits,
- faults in EPS wiring harness leading to loss of EPS supply.

An architectural approach like this is able to meet all ISO 26262 target values and requirements.

3.3 *Electric Power Steering EPS Component*

The EPS component itself needs to fulfill the ASIL-C requirements as well. As mentioned, these are especially the target metric values like PMHF, SPFM and LFM as well as the additional requirements for ASIL-C systems like specific FIT rates for SPFs and RFs (SPF/RF < 0.1 FIT) or dedicated measures that have to be applied. Current single logic EPS systems are not able to comply with these requirements. ASIL-C requires architectural changes on component level to meet ISO 26262 target values. An appropriate solution is to add a redundant logic path to the EPS hardware concept. This decreases the PMHF from approximately 700

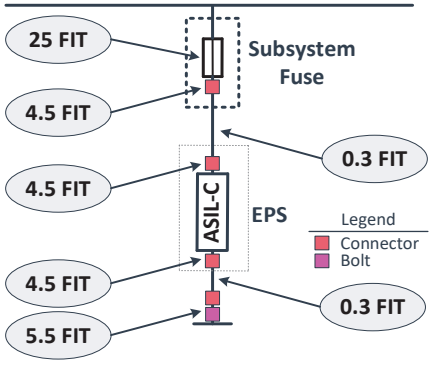

Fig. 9. Example failure rates of single channel connection

FIT of the single logic to approximately 100 FIT of the dual logic system (see Fig. 8). A dual logic EPS system configuration can be enhanced with redundant steering actuators like a six-phase electrical machine. That leads to a high efficient and full redundancy system on component level.

The conclusion is that single logic EPS systems are sufficient up to ASIL-B use cases with a single channel supply. ASIL-C systems require a dual logic EPS configuration with at least a single channel supply, which is also ASIL-C capable (see Chapter 3.4). ASIL-D systems in general tend to require a dual logic system and dual channel supply.

3.4 *Electric Power Steering EPS Connection*

To fulfill all the ASIL-C requirements regarding EPS, even the connection of component needs to meet the ISO 26262 target values as mentioned before. Especially the required SPF/RF < 0.1 FIT are in general not feasible for any kind of connection. Every connector, bolt, fuse or wire has itself more than 0.1 FIT (see Fig. 9). The investigation is done according to SN 29500 and ISO 26262 as a worst-case approach [SN 29500-5:2004-06], [ISO 26262-5:2018(E)].

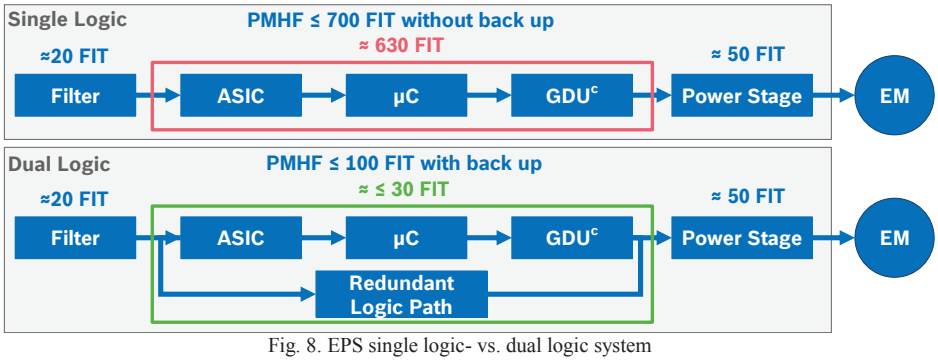

Fig. 8. EPS single logic- vs. dual logic system

[c] Gate Driver Unit (GDU)

The position of functional safety experts is that a single channel connection of ASIL-C EPS cannot be realized with current powernet solutions. In order to change this, technical safety measures like a Powernet Guardian safety system, as described in chapter 3.2, have to be applied. Especially intelligent HW/SW-functions enabling fault forecasting on EPS single channel connection are required for ASIL-C capability. In this case, the SaRA requirements could be addressed as mentioned in Table 3.

Table 3. EPS connection safety measures

SaRA Safety Measures	Single Channel EPS Connection
Fault prevention	Connector, wiring
Fault tolerance (providing the specified functionality)	Partial redundancy
Fault forecasting, Fault detection	Wiring harness diagnoses

Nevertheless, it is a critical task to apply to all the requirements for the connection. There is the possibility that other effort is necessary besides enhanced diagnostic functions to enable single channel EPS supply. Because of implemented monitoring functions and system diagnoses, hardware redundancies may be reduced leading to an optimized cost-benefit ratio. The sufficient application on component- and connection level completes the given safe supply powernet approach.

4. Summary and Conclusion

This paper presents the current vehicle trends like an increasing vehicle weight, more ADAS systems and automated driving functionalities. With regard to this, the effect on functional safety aspects of the vehicle powernet is described. The current vehicle trends tend to change the ASIL of driving functionalities like EPS towards ASIL-C. This leads to new requirements established by ISO 26262 that need to be fulfilled. It is pointed out, that these requirements cannot be met with current powernet topology designs. The main constraints thereby are the mandatory metric calculation for PMHF, LFM and SPFM as well as additional requirements for ASIL-C systems like every SPF/RF must be lower than 0.1 FIT. Facing the new requirements, an overall design process for next generation vehicle powernet is presented. This process complies with legislation, technical standards, safety and reliability. The specific target values for the example use case of EPS are derived whilst performing a HARA. These steps are necessary to adapt the new requirements to a safe supply powernet approach. After giving a short excerpt of a requirement engineering process a proposal for an ASIL-C Powernet architecture is described. The necessity of technical safety measures is emphasized and specific solutions are mentioned. The approach is completed by the demonstration in which way the steering component has to perform on component level and at the powernet connection point. Finally the approach is confirmed to be capable of meeting ISO 26262 requirements.

References

ADAC e.V.. Pannenstatistik 2020. Accessed June 29, 2020. https://www.adac.de/rund-ums-fahrzeug/unfall-schaden-panne/adac-pannenstatistik/.

Bertsche, B. (2008). Reliability in Automotive and Mechanical Engineering.

ECE-R13h:2018-06. (2018). Uniform provisions concerning the approval of passenger cars with regard to braking.

Gebauer, C. (2018). Fail operational and ISO 26262 2nd edition. Safetronic.2018. Carl Hanser Verlag GmbH & Co. KG.

ISO 26262. (2018). Road vehicles - Functional safety - .

ISO 26262-1:2018-12. (2018). Road vehicles – Functional safety – Part 1: Vocabulary.

ISO 26262-3:2018-12. (2018). Road vehicles – Functional safety – Part 3: Concept phase.

ISO 26262-4:2018-12. (2018). Road vehicles – Functional safety – Part 4: Product development at the system level.

ISO 26262-5:2018-12. (2018). Road vehicles – Functional safety – Part 5: Product development at the hardware level.

ISO 26262-9:2018-12. (2018). Road vehicles – Functional safety – Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses.

ISO 26262-10:2018-12. (2018). Road vehicles – Functional safety – Part 10: Guidelines on ISO 26262. 44-46.

Kurita, Y., Münzing, P. and Koller, O. (2017). Future Powernet Topology for Automated Driving.

Münzing, P., Ostertag, A., Bertsche, B., and Koller, O. (2018). Automated ASIL Allocation and Decomposition according to ISO 26262, Using the Example of Vehicle Electrical Systems for Automated Driving. SAE International. doi:10.4271/07-11-02-0011. ISSN: 1946-4614.

SAE J3016:2018-06. (2018). Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.

SN 29500-5:2004-06. (2004). Failure rates of components Part 5: Expected values for electrical connections, electrical connectors and sockets.

Statista GmbH. Entwicklung des Leergewichts von Neuwagen. Accessed June 29, 2020. https://de.statista.com/statistik/daten/studie/12944/umfrage/entwicklung-des-leergewichts-von-neuwagen/.