

Functional Safety and Electric Vehicle Charging: Requirements Analysis and Design for a Safe Charging Infrastructure System

Tommi Kivelä¹^a, Mohamed Abdelawwad²^b, Marvin Sperling¹^c, Malte Drabesch²,
Michael Schwarz², Josef Börsök²^d and Kai Furmans¹^e

¹*Institute for Material Handling and Logistics (IFL), Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany*

²*Department of Computer Architecture and System Programming, University of Kassel, Kassel, Germany*

Keywords: Electric Vehicle Charging, Functional Safety, Safety-related Systems, System Design.

Abstract: As society moves from fossil fuels towards electric mobility, there's an increasing need for charging infrastructure for electric vehicles. Aside from a network of public charging stations, charging equipment will also be increasingly installed in homes and used on a daily basis to charge electric vehicles (EVs) overnight. With this increasing role of charging infrastructure in day-to-day life, safety and security should be guaranteed for these systems. In this work we present the requirements analysis and a charging infrastructure system design for both private and public charging stations, with the goal of fulfilling the requirements of current functional safety and EV supply equipment (EVSE) standardization. Risk assessment for the charging process and the derived functional safety requirements are presented. The overall system design is discussed, with the main focus on the safety-related parts. The presented work can be used as a basis for the development of functionally safe next generation EVSE.

1 INTRODUCTION


According to the IEA (2020), the amount of electric vehicles (EVs) has jumped from 17 000 cars in 2010 to 7.2 million in 2019. As society moves from fossil fuels towards electric mobility, there's an increasing need for charging infrastructure for EVs. Aside from a network of public charging stations, charging equipment will be increasingly installed in homes and used on a daily basis to charge electric vehicles overnight. In 2019, 7.3 million chargers worldwide have been installed, majority of them private (IEA 2020). With this increasing role of charging infrastructure in day-to-day life, safety and security should be guaranteed for these systems.


In this work we present results from the research project SiLis ("Sicheres Ladeinfrastruktursystem für Elektrofahrzeuge": "a safe charging infrastructure system for EVs"). The goal of the project is to develop a compact and cost-effective electronic


control system for both private and public 3-phase AC (mode 3) charging stations, while fulfilling the requirements of current functional safety and EV supply equipment (EVSE) standardization.


The standard IEC 61851-1 (IEC 2017) defines general and safety requirements for EVSE, but does not currently define any functional safety requirements in case the safety-related functions in the charging station are implemented through programmable electronic systems. Relevant background regarding the requirements for charging stations, safety engineering and functional safety, as well as related work is discussed in section 2.


In order to define functional safety goals, a risk assessment for the charging application was performed, which is presented in section 3. Following the risk assessment, a system architecture was developed, where the safety-related and non-safety-related functionality were separated into their respective subsystems. The safety-related subsystem was developed according to the standard IEC 61508

^a  <https://orcid.org/0000-0003-4795-0030>

^b  <https://orcid.org/0000-0001-9501-8278>

^c  <https://orcid.org/0000-0002-1970-9891>

^d  <https://orcid.org/0000-0003-4394-1305>

^e  <https://orcid.org/0000-0001-6009-5564>

(IEC 2010). The developed safety subsystem includes a safety control board with a 1oo1D architecture (Börcsök 2004), which is responsible for the charging control main circuit, with redundant switching components to achieve a fail-safe design. The system design is presented in section 4. In section 5, we finish with a summary and a discussion of the work still to be finished in the near future.

2 BACKGROUND

2.1 Electric Vehicle Supply Equipment

The general and safety requirements for EVSE are provided by the IEC 61851 standard series (IEC 2017). The complete EV charging system includes the EVSE and the functions within the EV required for charging (IEC 2017). The EV side safety requirements for the charging system are defined in ISO 17409 (ISO 2020).

IEC 61851-1 (IEC 2017) defines different configurations of the EV charging system and different charging modes, including AC and DC charging. The presented system targets mode 3 charging, i.e. AC charging with dedicated EVSE permanently connected to the grid (IEC 2017).

The standard series IEC 62196 (IEC 2014) defines standardized plugs, socket-outlets, vehicle connectors and vehicle inlets for EV charging. Specifically, IEC 62196-2 (IEC 2016) defines standardized connectors for use in AC charging, including the Type 2 connector, commonly used in Europe. The standards IEC 62196-1 (IEC 2014) and IEC 61851-1 (IEC 2017) define the basic vehicle interface for AC charging and the Control Pilot (CP)-function for basic communication between the EVSE and the EV during charging, allowing for continuous monitoring of the proximity of the EV, basic signalling between the EVSE and EV, and encoding the charging cable current capability. The power supply to the EV shall be energized and de-energized based on the state of the CP signal (IEC 2017).

For this work, we assumed the use of IEC 62196-2 (IEC 2016) conforming connectors and the basic interface with CP function. The developed system can optionally support high-level communication e.g. according to ISO 15118 (ISO 2019), but the safety-related functions are based on the basic interface.

For the purposes of the risk assessment, the electrical basic protection requirements (IEC 2005a), such as the IP-rating of the enclosures and connectors, are assumed fulfilled. These basic protection and other requirements from IEC 61851-1 (IEC 2017)

were taken into account during the development project, but for the purposes of this paper we focus on the main functions relevant for the development of the safety-related control system.

In addition to the mandatory functions related to mode 3, IEC 61851-1 (IEC 2017) sets requirements for electrical fault protection. Fault protection (protection against indirect contact) shall be provided with one or more measures according to IEC 60364-4-41 (IEC 2005a), for example, automatic disconnection of supply. Protective earthing conductor shall be provided and for mode 3 it shall not be switched. A DC sensitive residual current protective device (RCD), when using a socket-outlet or connector according to IEC 62196 series (IEC 2014) shall be used.

To summarise, the developed charging infrastructure system shall provide the basic vehicle interface and the associated functions (Control pilot, proximity detection, cable current capability detection), as well as provide electrical fault protection in the form of disconnection of supply in case of overload and AC or DC fault current.

2.2 Safety Engineering & Functional Safety

Since the system to be developed is an infrastructure system and not part of the EV itself, the standard IEC 61508 (IEC 2010) was chosen as development guidance and certification target. The standard provides generic guidance for the development of safety-related electric, electronic or programmable electronic (E/E/PE) systems.

The goal of safety engineering is to assure the safety of a system over its lifecycle. In the concept phase, the system to be developed is analysed: the hazards related to the system are first identified and the associated risk is estimated and evaluated. Based on the risk assessment, risk reduction measures are designed to reduce the risks in the system to an acceptable level. Risk reduction measures can be passive measures, such as basic electrical isolation or active measures, such as fault current protection. A safety integrity level (SIL) is used to specify the integrity requirements for a safety function, which will be allocated to a E/E/PE-system. The standard defines SILs 1-4, with a higher level corresponding to higher risk reduction (IEC 2010).

Although SILs are defined in IEC 61508 in relation to safety functions, they are used in risk assessments as a generic measure of risk. Typical tools for risk estimation are risk graphs and matrices. A risk matrix should always be calibrated for the

considered application (IEC 2010). One example of a calibrated risk matrix, from IEC 62061 (IEC 2005b), is shown in Table 1. As a generic standard, IEC 61508 considers industrial catastrophes possible e.g. in the process industry (up to SIL 4), whereas the IEC 62061 targets the machinery industry, where possible risks are limited in comparison (up to SIL 3). The risk matrix from IEC 62061 provides a fine granularity for estimating risks related to single casualties or injuries to individual persons, and is thus well suited also for this application area.

The parameters F, P and W (Table 3) are summed to calculate the risk class C, which together with the parameter S (Table 2) is used to define the risk estimate by look-up from Table 1. A resulting SIL-level indicates that measures must be taken towards risk reduction. If the risk reduction measure is implemented with a safety-related control system, then this estimate is allocated as the required SIL-level for the SF. OM means that there is a remaining unacceptable risk, but no SIL allocation is needed. NR means that the risk is acceptable, further measures are not necessary. For a more detailed description of the risk parameters the reader is referred to IEC 62061 Annex A (IEC 2005b).

2.3 Related Work

Few publications seem to discuss functional safety aspects of charging systems. Instead, scientific literature regarding charging infrastructure tends to focus on other aspects, for example power electronic solutions for high power charging (Tu et al. 2019) or smart charging strategies and grid integration (Wang et al. 2016; Veneri 2017).

Schmittner et al. previously studied functional and electrical safety for charging stations (2013). The authors considered a typical implementation of a charging station with the safety-related functions implemented mainly through discrete electromechanical and electronic components, whereas we consider an integrated software controlled system. The work used the example risk graph from IEC 61508-5 (IEC 2010), which provides only very rough granularity for single person injuries or casualties.

A thorough safety assessment for EV charging was presented by Vogt et al. (2016). They considered several hazard types (e.g. electrical, mechanical, ergonomic) based on ISO 12100 (ISO 2010) and defined safety goals to be fulfilled by the EVSE or through other means and assigned SIL-targets (with IEC 62061 risk matrix) for each. Their work provided a basis for the risk analysis presented here. However,

some safety goals are reached through a combination of risk reduction measures. Thus, a more detailed analysis is required in order to determine the required contribution of each risk reduction measure towards the safety goal.

Several charging systems and in-cable-charging devices are available on the market today. To the author's knowledge, none of them are currently certified with respect to functional safety.

Table 1: Risk matrix according to IEC 62061 (IEC 2005b). S=Severity, C=Risk class, F=Frequency and duration of exposure, P=Possibility of avoiding or limiting harm, W=Probability of occurrence of the hazardous event, OM=Other measures, NR=No SIL requirements.

S	C=F+P+W				
	4	5-7	8-10	11-13	14-15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3	NR	OM	SIL1	SIL2	SIL3
2	NR	NR	OM	SIL1	SIL2
1	NR	NR	NR	OM	SIL1

Table 2: Values for S (IEC 2005b).

	S
1	Reversible, requiring first aid
2	Reversible, requiring attention from a medical practitioner
3	Irreversible, broken limb(s), losing finger(s)
4	Irreversible, death, losing an eye or arm

Table 3: Values for F, P and W (IEC 2005b).

	F	P	W
1	-	Probable	Negligible
2	> 1 year	-	Rarely
3	> 2 weeks to ≤ 1 year	Rarely	Possible
4	> 1 day to ≤ 2 weeks	-	Likely
5	≤ 1 day	Impossible	Very high

3 SAFETY REQUIREMENTS

The project target was to develop a compact and cost-effective electronic charging infrastructure system, which integrates several functions, currently typically implemented with multiple discrete components, required in a charging station. In this section we present the risk assessment for the charging application and the defined safety requirements for the charging infrastructure system. The charging infrastructure system should provide a common basis for both public and private charging. Mode 3 was the main target, but the risk analysis was held as generic

as possible to cover the different charging configurations defined by IEC 61851-1. The focus of the work was on AC-charging, but the developed safety system should also be adaptable to DC-charging in the future.

3.1 Risk Assessment

The goal of the risk assessment was to specify the functional safety requirements for the system. The approach and results of Vogt et al. (2016) was taken as a basis for the assessment. The focus of the assessment was on electrical hazards. Basic electrical protection against electrical hazards were considered covered through following the product standardisation. This includes for example fulfilling the isolation, breaking capacity and IP-classification requirements set for housing and cabling in IEC 61851-1 (IEC 2017) and using the charging plugs and sockets as defined in e.g. IEC 62196-2 (IEC 2016). Other, e.g. mechanical or ergonomic hazards were similarly considered covered through the existing standardisation. The hazards considered are shown in Table 4.

Vogt et al. (2016) considered several environmental and operational conditions. For this work, some of the conditions were summarised to focus on the worst case scenarios to derive the functional safety requirements. The considered environmental conditions and process states are shown in Table 5. To cover all cases, the worst case location, a public charging station on the side of a public road and no cover or roofing, was taken as the basis for the assessment. Assumed was, that the vehicle fulfils ISO 17409 (ISO 2020) requirements, which do not allow vehicle movement powered by its own drives while it is connected to external power supply, excluding this as a possible state. Other possible situations where the vehicle is moving are covered by VS2.

The considered situations were all possible combinations of the listed weather conditions, operating and vehicle states, except for combinations of VS2 and A, which were not considered realistic. For each situation, all the 4 hazards were considered. The user of the charging station was assumed to be a layperson with limited knowledge regarding electric equipment. Thus in most cases a worst case assumption has to be made about the capability of the user to detect and avoid hazards. For each case the initial risk was evaluated and risk reduction measures were added until the remaining risk was considered acceptable (result "NR" in the risk matrix in Table 1).

The considered risk reduction measures are shown in Table 6, originating from IEC 61851-1 (IEC 2017).

Table 4: Hazards considered in the risk assessment.

	Hazard
Hz1	Electric shock through contact with live electric parts
Hz2	Electric shock through contact with live electric parts when considering external misuse (e.g. vandalism)
Hz3	Fire, burnout, projection of molten parts due to arcing or sparking
Hz4	Fire, burnout, projection of molten parts due to short-circuit or overload of the charging system

Table 5: Environmental conditions and process states.

Weather conditions	
W1	Fog or otherwise high humidity
W2	Ice, snow or snowfall
W3	Rain, driving or heavy rain, water splashes from passing vehicles, or flooding
Operating states	
A	User insert charging connector, charging process is started
B	Charging connector is plugged in, charging process ongoing
C	User removes charging connector, charging process is stopped
Vehicle states	
VS1	Vehicle is standing (velocity = 0)
VS2	Vehicle is moving (velocity > 0) due to external influences.

Table 6: Considered risk reduction measures.

	Risk reduction measure
RM1	Overload and short circuit protection
RM2	Fault current protection (AC & DC)
RM3	EV Proximity monitoring, energy supply only when present and automatic disconnection by loss of continuity (CP/Basic vehicle interface)
RM4	Charging cable capacity detection and overload protection (CP/Basic vehicle interface)
RM5	Locking mechanism for the charging connector (Optional requirement for modes 2-4 (IEC 2014, 2017))

A total of 53 cases were analysed. In the following, representative examples are discussed. As the functions related to the basic vehicle interface are part of the risk reduction measures, the analysis assumed that they are not yet present in the system, in order to evaluate their required contribution to risk reduction.

As first example, the situation of W1-A-VS1 is considered: The user plugs the charging connector to

a standing vehicle to start the charging process. In case of the failure of the basic protection (for example a crack in the charging connector or isolation of the charging cable due to e.g. equipment aging) the user could touch live active parts and get an electric shock (Hz1), since without prior measures the connector is already active. The shock could in a worst case lead to death (S=4). Assumedly the user charges their car daily (F=5). It can be argued, that such an incident happens only rarely considering that the charging cable and connectors are built to last for the lifetime of the application, but the probability is not negligible (W=2). It might be rarely possible for a layperson to detect and avoid the hazard (P=3). The resulting risk estimate is SIL2 (cf. Table 1). The risk estimate for this case is the same in all weather conditions and if vandalism is considered (Hz2). The first risk reduction measure used is fault current protection (RM2). However, to ensure the effectiveness of this measure, the charging cable should additionally include a protective shielding (Vogt et al. 2016). After implementing RM2, the severity is reduced to S=2 due to the timely disconnection of power supply. For the remaining risk, other measures (OM) are sufficient. The addition of RM3 further reduces the risk.

In the same situation, an internal fault in the charging cable, connector or within the EV could result in a short circuit of the EVSE power supply upon inserting the cable, leading to e.g. fire (Hz4). The other risk parameters are same as in the first case (S=4, F=5, W=2), but for this case it is not possible for the user to detect and avoid the hazard (P=5). The risk estimate for this case is SIL3. First, RM1 is used, reducing the possible severity (S=2). The remaining risk is estimated with SIL1. As further risk reduction, RM3 can be employed to ensure that the charging connector is not active when plugging the vehicle in. Even further risk reduction can be achieved with RM4 and other measures such as user information.

As final example, consider the situation B-VS2 in any weather condition: The vehicle is being charged, but moves due to external influences (e.g. due to another vehicle colliding with the EV). As a result, the charging cable or connector breaks and sparking or, in a worst case, arcing happens as a result. If people are in the vicinity when this happens, death is the worst case result (S=4). The probability of this event can be argued to be rare or even negligible (W=2 or 1). A layperson could in a rare case have the possibility to both detect and avoid the hazard (P=3). The resulting risk class is C=9 or 10 (F=5), for both the risk estimate is SIL2. The only suitable risk reduction measure is RM3. Further risk reduction

measures are external to the EVSE, e.g. user information, reduced speed limits or fencing around charging stations.

Assessing risk is always subjective (Redmill 2002). In order to keep the assessment as objective as possible and avoid introducing significant biases, the focus was kept on worst case estimates. The risk in this approach is that the results might be overly conservative. Considering that charging station usage is still relatively limited and that as a society we have relatively little experience over longer periods of time in laypersons using such equipment on a daily basis, a conservative approach seems reasonable. Once more information and real-life experiences over the lifecycle is gathered with the currently installed equipment, the risk assessment could be revisited.

3.2 Functional Safety Requirements for the Charging Station

Based on the risk assessment, the safety functions required to reduce the risk of the hazards related to the charging application were defined as shown in Table 7. The defined safety functions cover the risk reduction measures RM1-RM3 (SF1-SF3). SF4 is additionally needed to safely activate the power supply to allow charging in the first place. The measures RM4 & RM5 provide further risk reduction, but were assigned no SIL requirements.

Table 7: Safety Functions.

SF	Description	SIL	Related Hazards
SF1	EVSE Overload and short circuit protection.	SIL3	Hz4
SF2	AC & DC Fault current protection.	SIL2	Hz1, Hz2
SF3	Proximity monitoring, disconnection of energy supply upon loss of continuity.	SIL2	Hz1-Hz4
SF4	Safe start and stop of charging process. Start only when EV connected and self-tests successful. Internal system supervision and stop upon detection of unsafe state or internal faults.	SIL2	Hz1-Hz4

4 DESIGN

4.1 System Design

The designed overall system architecture is shown in Figure 1. The main subsystems are the main board, safety board (SAB), and the operational board (OPB). The main board includes fuses and the main charging circuit. The main charging circuit includes redundant charging relays, to supply power to the EV, and associated feedback signals, a fault current sensor, current sensors, the basic vehicle interface circuitry, DC power supply and interfaces for SAB and OPB. The SAB is responsible for the safety-related functions (core charging control) and the OPB for non-safety-related functions such as energy monitoring, EV communication, communication with the user over a web- or application-based GUI and with the backend servers required in public charging for e.g. payment processing. The safety and operational board communicate over a serial bus with a Modbus RTU-protocol modified with additional reliability measures. The system architecture allows for separation and freedom from interference between safety- and non-safety-related functions.

The SF1 (Overload protection) is implemented through fuses on the main board. The SAB does not take part in this SIL3-rated SF, but does participate in the implementation of the remaining SFs, which are all rated SIL2. Thus, the SAB development targets systematic capability SC2 (required for SIL2).

The control loop implementing SF2 (AC & DC Fault current protection) consists of the fault current sensor within the main charging circuit, the SAB and the charging relays. Detected fault current leads to immediate disconnection of the power supply. The chosen 30mA AC & 6mA DC fault current sensor (Bender RCMB121) includes a self-test function. Additionally, an independent fault current emulation circuit is implemented as part of the main charging circuit. Before a charging process is started, the self-test and the independent test of the fault current sensor are performed for fault detection.

The CP driver signal is generated by the OPB. The SAB has a separate measurement of the CP signal to independently detect the EV proximity and that the charging cable is properly plugged in. The IEC 62196-2 (IEC 2016) charging connectors guarantee that the CP-lines are connected last and disconnected first. The SF3 is implemented with the control loop consisting of the CP voltage measurement circuit, the SAB and the charging relays.

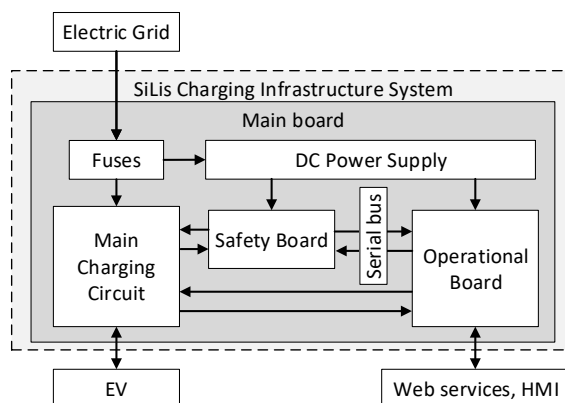


Figure 1: System architecture.

The SF4 is implemented by the control loop including the SAB and the redundant charging relays and their contact feedbacks. For the targeted current rating (32A), force guided relays, a typical solution for safety-critical applications, were not available. Thus, a redundant set of relays (the contacts in two rows in series connection) without force guided contacts were used (cf. 2 in Figure 3). In order to detect faults in the relay contacts (contact welded shut, contact remains open), a feedback signal was included for each grid phase (L1-L3) contact. The SAB controls each relay row separately, and thus is capable of diagnosing each relay row separately during energization and de-energization. If any single relay contact is welded shut, the power supply can still be disconnected. Additionally, the SAB and the used safety MCU (Microcontroller unit) include numerous self-diagnostics. Upon detection of internal faults, the system is brought to a safe state (energy supply de-energized).

The risk reduction measures RM4 (and the optional RM5) were not allocated any SIL-requirements, and thus these functions were allocated onto the OPB instead of the SAB. For RM4 (Cable capacity detection and overload protection), the OPB detects the capacity through the basic vehicle interface. The OPB utilises the current sensors in the main circuit for charging cable protection as well as for energy monitoring of the charging process. Upon overload the OPB requests the SAB to stop the power supply to the EV.

To initiate or stop the charging process, the OPB can send requests to and get diagnostics from the SAB through the communication interface. The SAB is in control of and continuously monitors the charging process and deactivates the power supply to the EV if any faults are detected. The system design and communication solution provides moderate protection against cybersecurity threats. Since all

external communication is implemented on the OPB, the SAB itself is not in direct connection to the internet and uses direct physical digital and analogue IO for the safety-related functions.

4.2 Safety Hardware Design

The SAB (shown in Figure 2) is responsible for carrying out the majority of safety functions. To achieve the safety integrity requirements, the board was designed around a safety-certified MCU (TI Hercules RM48). The MCU has redundant Arithmetic Logic Units (ALUs) in lockstep, error correction code (ECC) memory and built-in self-tests. The SAB includes galvanic isolations for inputs, outputs and the power supply, as well as voltage monitoring and a two-stage hardware watchdog.

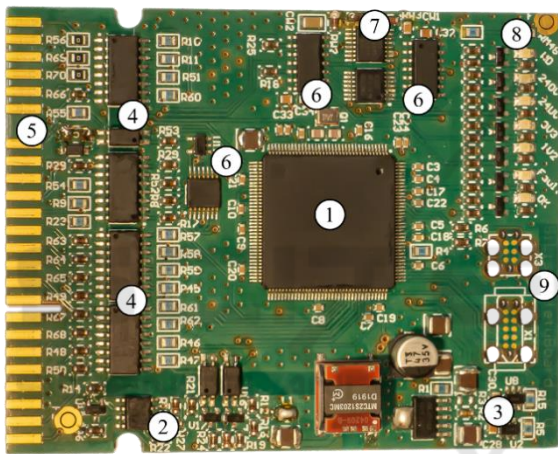


Figure 2: The safety board (SAB). 1: Safety MCU. 2: Input voltage monitoring. 3: Internal voltage monitoring. 4: Galvanic isolation. 5: Mainboard connector. 6: Control logic circuitry. 7: Hardware Watchdog. 8: Status LEDs. 9: Programming and diagnostics interface.

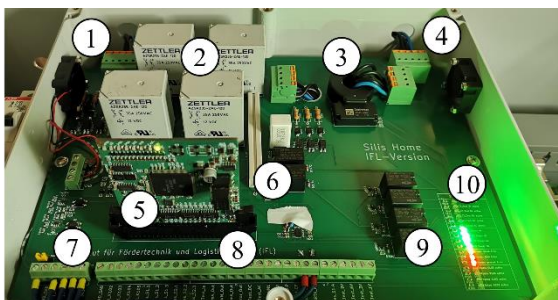


Figure 3: Charging circuit functional prototype. 1: Grid connection. 2: Main relays. 3: Fault current sensor. 4: EV power connection. 5: SAB. 6: FI sensor self-test circuit. 7: DC power terminals. 8: Measurement/Serial bus terminals. 9: CP-signal generator. 10: Status LEDs.

A prototype of the main charging circuit is shown in Figure 3, built to allow for easy verification of the circuit concept and safety software with additional measurement terminals. This prototype was used to assist the safety software development. The industrial project partners have developed a compact production version of the same hardware concept and the OPB. At the time of writing the production version is ongoing verification activities. System validation testing in a charging station with an EV is planned in the near future.

System- and design-FMEAs were performed for the SAB and the safety-related parts of the main circuit. Diagnostics and redundancy were included in the system design to ensure that singular component failures cannot bring the system to a hazardous state or that faults are detected and the energy supply is de-energized before an accident can occur. The SAB implements a 1oo1D architecture (Börcsök 2004), whereas the main application circuitry is redundant.

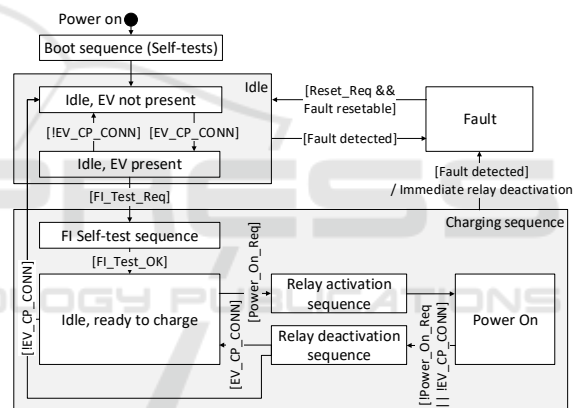


Figure 4: Main state machine for the SAB software.

4.3 Safety Software Design

The design of the Safety-SW running on the SAB was kept modular and as simple as possible for ease of analysis. A time-triggered architecture (single main-loop running at 1ms with a hardware timer) with a minimum of interrupt routines was implemented. The safety-SW executes the charging supervision functions and handles possible incoming messages each loop. MCU Self-tests are executed at boot time.

A high-level view of the main state machine is shown in Figure 4. When EV presence is detected, a test sequence for the fault current sensor is first required. If the test is successfully executed, the system is ready to charge. Upon request from OPB the charging relays are activated row-by-row. Once both rows are on, the power supply to the EV is

active. The OPB can request to turn the power off, triggering the row-by-row de-activation sequence. The de-activation sequence is also triggered if the user unplugs the EV during charging. If any faults are detected during the charging sequence, the system transitions to the fault state accompanied by immediate de-energization of both relay rows to bring the charging process to a safe state. For a subset of faults, the OPB can request a fault reset, which moves the system back to the idle state, other faults require cycling power to the SAB to reset.

5 CONCLUSIONS

In this work we presented a requirements analysis and a system design for a safe electronic charging infrastructure system. The system was designed according to current functional safety and EVSE standards. System validation tests with a production-version of the SiLis-hardware and an EV is planned for the near future. The system discussed here is a research prototype, a safety certification of the production version of the system is planned by the industrial project partners in the future.

The presented work can be used as a basis for the development of safe next generation EVSE. Even with the urgent need for this new critical infrastructure, the proper care should be taken in building it. The safety of these electronically controlled systems should be guaranteed as we move into increasingly electrified forms of transportation.

ACKNOWLEDGEMENTS

We gratefully acknowledge that this research is funded by the German Federal Ministry of Education and Research (BMBF: Bundesministerium für Bildung und Forschung) under grant number 16EMO0329. We would additionally like to thank the partner companies, ProSystems GmbH and kortec Industrieelektronik GmbH & Co. KG, for the collaboration on the project.

REFERENCES

- Börcsök, J. 2004. *Electronic safety systems: Hardware concepts, models, and calculations*. Heidelberg: Hüthig, 565 pp. (eng).
- IEA. 2020. Global EV Outlook 2020 – Analysis - IEA. Retrieved 4 October, 2020, from <https://www.iea.org/reports/global-ev-outlook-2020>.
- IEC. 2005a. Low voltage electrical installations - Part 4-41: Protection for safety - Protection against electric shock, IEC 60364-4-41. International Electrotechnical Commission.
- IEC. 2005b. Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems, IEC 62061. International Electrotechnical Commission.
- IEC. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508. International Electrotechnical Commission.
- IEC. 2014. Plugs, socket-outlets, vehicle connectors and vehicle inlets – Conductive charging of electric vehicles – Part 1: General requirements, IEC 62196-1. International Electrotechnical Commission.
- IEC. 2016. Plugs, socket-outlets, vehicle connectors and vehicle inlets – Conductive charging of electric vehicles – Part 2: Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories, IEC 62196-2. International Electrotechnical Commission.
- IEC. 2017. Electric vehicle conductive charging system - Part 1: General requirements, IEC 61851-1. International Electrotechnical Commission.
- ISO. 2010. Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010), ISO 12100. International Organization for Standardization.
- ISO. 2019. Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition, ISO 15118-1. International Organization for Standardization.
- ISO. 2020. Electrically propelled road vehicles — Conductive power transfer — Safety requirements, ISO 17409. International Organization for Standardization.
- Redmill, F. 2002. Risk analysis-a subjective process. *Engineering Management Journal* 12: 91–96. doi: 10.1049/em:20020206.
- Schmittner, C., G. Scharfenberg, J. Mottok, S. Strassmeier, T. Limmer, and others. 2013. Analysis of the Functional and Electrical Safety of Charging Stations.
- Tu, H., H. Feng, S. Srdic, and S. Lukic. 2019. Extreme Fast Charging of Electric Vehicles: A Technology Overview. *IEEE Transactions on Transportation Electrification* 5: 861–878. doi: 10.1109/TTE.2019.2958709.
- Veneri, O. 2017. *Technologies and Applications for Smart Charging of Electric and Plug-in Hybrid Vehicles*. Cham: Springer International Publishing.
- Vogt, M., S. Link, K. Ritzinger, E. Ablingyte, and P. Reindl. 2016. *Sicherheitsaspekte beim Laden von Elektrofahrzeugen*. Bergisch Gladbach: Bundesanstalt für Straßenwesen.
- Wang, Q., X. Liu, Du J, and F. Kong. 2016. Smart Charging for Electric Vehicles: A Survey From the Algorithmic Perspective. *IEEE Communications Surveys Tutorials* 18: 1500–1517. doi: 10.1109/COMST.2016.2518628.