Abschlussbericht

Sicheres Ladeinfrastruktursystem

Teilprojekt: Design eines robusten und sicheren Hardwaremoduls für das Laden von Elektrofahrzeugen

Date: 28.02.2021

Teilprojekt: Design eines robusten und sicheren Hardwaremoduls für das Laden von Elektrofahrzeugen

ABSCHLUSSBERICHT

Zuwendungsempfänger

Universität Kassel
Rechnerarchitektur und Systemprogrammierung
(ICAS – Institute of Computer-architecture and System-programming)
Wilhelmshöhe Allee 71
34121 Kassel

Förderkennzeichen

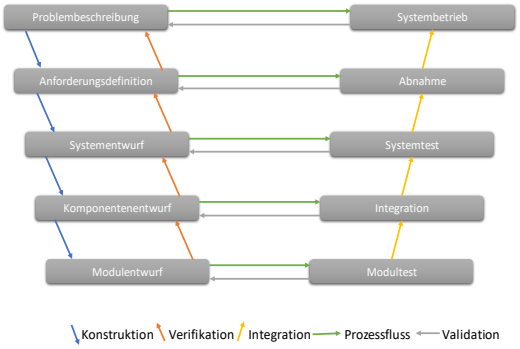
16EMO0330

Vorhabensbezeichnung:

SiLis

Sicheres Ladeinfrastruktursystem

(***Fördermaßnahme***: KMU-innovativ
im ***Förderbereich***:
Forschungsbereich Elektronik- und Mikrosysteme, Elektromobilität und Entwurfsautomatisierung)



Teilvorhaben:

Design eines robusten und sicheren Hardwaremoduls für das Laden von Elektrofahrzeugen

Laufzeit des Projektes:

01.09.2018 - 31.08.2020

Berichtszeitraum:

01.09.2018 - 31.08.2020

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16EMO0330 gefördert.

Gefördert vom:

Bundesministerium für Bildung und Forschung

Inhalt

Symbole, Abkürzungen und Bezeichnungen

ASIL	Automotive Safety Integrity Level
CAN	Controller Area Network
GPIO	General Purpose Input / Output
LIN	Local Interconnect Network
MAB	Main-Board
OPB	Operational Board
PL	Performance Level
SCI	Scalable Coherent Interface
SAB	Safety Board
SIL	Safety Integrity Level
USB	Universal Serial Bus

1. Zusammenfassung der wesentlichen fachlichen Inhalte des Abschlussberichtes zum Teilvorhaben des ICAS

Intelligente und sichere Ladestationen sind ein wichtiger Bestandteil, um E-Mobilität weiter ausbreiten zu lassen. Nur wenn genügend Ladestationen vorhanden sind, werden mehr Menschen auf Elektrofahrzeuge umsteigen. Dies stellten einen wichtigen Baustein der Reduzierung der CO_2 Emissionen dar um die Klimaziele der Bundesregierung zu erreichen.

Die immer steigende elektrische Energieversorgung der künftigen E-Fahrzeuge und das immer schnellere aber dennoch sichere Laden ermöglicht notwendige, zukunftsträchtige und interessante Bereiche der Forschung und Entwicklung.

Insgesamt zeigt aber auch der Bereich der sicheren und zuverlässigen Mikrosysteme ein hohes Potential für einen breiten Markt aber auch für Forschung und Entwicklung. Anfänglich in der Luftfahrt und besonders in der Prozessindustrie geforderten Sicherheitssysteme nach Norm, werden in mehr Branchen und Bereichen neue Sicherheitsnormen eingeführt, die an die IEC 61508 angelehnt sind. Das sichere und zuverlässige verarbeiten von Werten wird in immer mehr Bereichen gefordert, sei es in der Automobilindustrie, Medizintechnik, Logistik aber auch in neuen Bereichen wie beim intelligenten, mobilen Gesundheitsmonitoring, Smart Home, Sportdiagnostik, Telemedizin, Vitalfunktions-überwachung und intelligenten Textilien.

Weiterhin dehnt sich die funktionale Sicherheit von der verarbeitenden Einheit (Steuerung, Rechner) in die Sensorik und Aktorik aus, um intelligente sichere und zuverlässige Gesamtsysteme zu erzielen.

Durch den Einsatz von funktional sicheren Schaltungen, Komponenten und Systemen aber auch deren Miniaturisierungen (Safety Chips) in unterschiedlichen Bereichen und auch der Wiederverwendung und Erweiterung sorgen letztendlich dafür, dass es zwar keine Massenprodukte aber dennoch preiswerte und gut verfügbare Komponenten werden, die in zahllosen Bereichen eingesetzt werden können.

In Kooperation mit den Verbundpartnern wurden im Fachgebiet Rechnerarchitektur und Systemprogrammierung folgende Ergebnisse erzielt:

- Es wurde eine kompakte sichere Steuerungseinheit entworfen, die folgende Eigenschaften besitzt:
    - Programmier- und Diagnoseschnittstelle
    - Spannungsversorgung
    - Externe und interne Spannungsüberwachung
    - Statusanzeige
    - Zweistufigen Watchdog
    - Kontrolllogik zum sicheren Laden
    - Sichere galvanische Trennung der Ein- und Ausgänge

  - Sichere CPU
- Ein Betriebssystem wurde portiert und Anpassungen durchgeführt
- Testreihen wurden erstellt und durchgeführt
- Sicherheitsanalysen wurden durchgeführt und erfolgreich bestanden
- Es wurden alle Meilensteine erfüllt.

Das entworfene Sicherheitssystem ist ein weiterer Baustein in der Reihe von zahlreichen und erfolgreichen Entwürfen und Entwicklungen von sicheren programmierbaren Steuerungssystemen, die Anforderungen nach unterschiedlichen Standards und Normen erfüllen.

2. Kurzdarstellung

In diesem Kapitel werden zunächst das Projekt und das Konsortium allgemein dargestellt. In der Aufgabenstellung wird als erstes auf Ladestationen für E-Fahrzeuge generell eingegangen, bevor die Aufgabenstellung des Teilvorhabens beschrieben wird. Die Expertise des Fachgebietes Rechnerarchitektur und Systemprogrammierung wird beschrieben, sowie die notwendigen Voraussetzungen, um die Aufgabe erfolgreich starten und auch abschließen zu können. Die einzelnen Aufgaben innerhalb des Konsortiums werden in Form von Arbeitspaketen beschrieben und das Konsortium selbst wird kurz skizziert, ebenso wird ein kurzer Stand der Technik präsentiert.

2.1 Aufgabenstellung

Die Auswirkung der Zunahme der Anzahl der Fahrzeuge auf die Klimaveränderungen ist eindeutig und kann nicht geleugnet werden. In einer Konferenz, die 2013 vom deutschen Verkehrsministerium organisiert wurde, wurde bekannt gegeben, dass von 43 Millionen zugelassenen Fahrzeugen nur 7.000 Elektroautos und 65.000 sogenannte Hybride sind. Um den Klimawandel abzumildern und damit seine globalen katastrophalen Folgen wie steigende Temperaturen und steigende Meeresspiegel zu begrenzen, hat die Bundesregierung mehrere Maßnahmen formuliert, die es zu erreichen gilt. Eine der geplanten Maßnahmen ist es, die Zahl der zugelassenen Elektrofahrzeuge in Deutschland bis 2020 auf eine Million zu erhöhen[1].

Laut IEA (2020) ist die Anzahl der Elektrofahrzeuge (EVs) von 17.000 Autos im Jahr 2010 auf 7,2 Millionen im Jahr 2019 angestiegen[2]. Da sich die Gesellschaft von fossilen Brennstoffen hin zur Elektromobilität bewegt, besteht ein zunehmender Bedarf an Ladeinfrastruktur für Elektrofahrzeuge. Neben einem Netz von öffentlichen Ladestationen werden zunehmend Ladegeräte in Haushalten installiert und täglich genutzt, um Elektrofahrzeuge über Nacht aufzuladen. Im Jahr 2019 sind weltweit 7,3 Millionen Ladegeräte installiert, die meisten davon privat[2]. Mit dieser zunehmenden Rolle der Ladeinfrastruktur im täglichen Leben sollte die Sicherheit dieser Systeme gewährleistet sein.

Derzeit fehlt es noch an der elektronischen Grundausstattung für Ladestationen. Obwohl mehr als 80 % der Fahrzeuge in privaten Haushalten geladen werden[3], gibt es erhebliche Sicherheitsdefizite. So ist bei vielen Produkten eine Schutzeinrichtung (FI-Schutzschalter) im Hausanschluss erforderlich[4], was aber oft nicht der Fall ist. In Zukunft wird es weitere Herausforderungen geben, wie z. B. das Thema Smart Grids, für das es noch keine breit anwendbaren Lösungen gibt, die auch wirtschaftlich sein sollen.

[1] D. Welle, Germany aims for 1 million e-cars by 2020 | DW | 27.05.2013. [Online]. Available: https://www.dw.com/en/germany-aims-for-1-million-e-cars-by-2020/a-16841141 (accessed: Feb. 11 2021).
[2] IEA, Global EV Outlook 2020 – Analysis - IEA. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2020 (accessed: Oct. 4 2020).
[3] Neue Welten, "80 Prozent der Ladevorgänge von Elektroautos finden zuhause statt“. [Online]. Available: https://www.journalistenakademie.de/dossiers/neue-welten/elektroautos-zuhause-laden/ (accessed: Feb. 14 2021).
[4] Normgerechte Errichtung von Ladeinfrastruktur | Elektroauto Wiki | GoingElectric.de. [Online]. Available: https://www.goingelectric.de/wiki/Normgerechte-Errichtung-von-Ladeinfrastruktur/ (accessed: Feb. 14 2021)

Teilprojekt: Design eines robusten und sicheren Hardwaremoduls für das Laden von Elektrofahrzeugen

Um Elektroautos gegenwärtig laden zu können, müssen diese für lange Zeit an den Ladestationen verbleiben. Heutzutage werden Elektroautos meist über Nacht geladen, um morgens geladen zur Verfügung zu stehen. Um die Steigerung der angemeldeten Elektrofahrzeuge in Deutschland umsetzen zu können, muss zwingend die Ladezeit reduziert werden.

Erhebliche Problemstellungen ergeben sich in der funktionalen Sicherheit (Safety), was insbesondere beim Schnellladen mit hohen Ladeleistungen eine große Herausforderung darstellt. Der private Sektor ist davon besonders betroffen. Bei günstigen Lösungen werden derzeit nicht die gebotenen Maßnahmen der Sicherheitstechnik berücksichtigt (z. B. allstrom-sensitiver FI). Gleichzeitig steigen die Ladeleistungen, was zu einer Verschärfung der Sicherheitssituation beiträgt. Zudem laufen bereits Versuche mit Ladeleistungen von bis zu 350 kWh (Ultra- Schnellladesäulen)[5], die früher oder später in öffentlichen Anwendungen auftreten werden. Dies kann jedoch nur funktionieren, wenn auch die Ladespannungen deutlich, über das heute in Netzen mögliche, angehoben werden. Die existierenden Ladesäulensteuerungen können die Bandbreite nicht abdecken, es müssen stets individuelle Steuerungslösungen entwickelt werden.

Zielstellung: Das Ziel des Teilvorhabens ist, eine neuartige sicherheitsgerichtete Steuerungsarchitektur für eine Ladesäule zu entwerfen, die nach der im Jahr 2012 neu eingetretenen ISO- Norm 26262 (ASIL-A/ASIL-B) für sicherheitsrelevante elektrische/elektronische Systeme im Automotivbereich zertifiziert werden kann. Die Sicherheitsarchitektur deckt die Einschränkungen hinsichtlich der existierenden Insellösungen vollständig ab. Aspekte sowohl der sicheren und zuverlässigen Datenverarbeitung und Eigenüberwachung werden vereint.

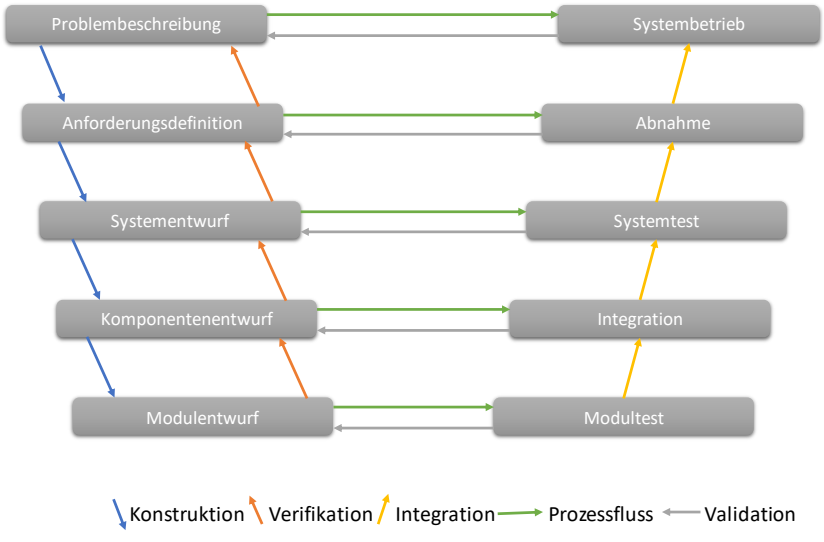


Abbildung 1: V-Modell

[5] www.tuvsud.com, E-Mobility | Alles zu Ladesäulen. [Online]. Available: https://www.tuvsud.com/de-de/industre/gebaeudeausruestung-info/ladesaeulen (accessed: Feb. 14 2021).

Das Ziel der Forschung seitens ICAS ist eine hochkompakte und hochintegrierte „System on a Chip"-Hardware (SoC), das mit einem Kommunikations- und einem Anwendungsmodul zusammenarbeitet. Hierdurch wird das System deutlich kompakter und kostengünstiger. Im Anschluss an das Forschungsprojekt wird eine Zertifizierung im Sicherheitslevel ASIL-A/ASIL-B (Automotive Safety Integrity Level) angestrebt. Die Anforderungen für sicherheitsrelevante elektrische/ elektronische Systeme im Automotivbereich sind in der ISO 26262 fest definiert. Dementsprechend ist eine systematische Vorgehensweise, wie im V-Modell, Abbildung 1, beschrieben, zwingend notwendig.

Ein angestrebter Effekt ist zudem, dass der Zertifizierungsaufwand durch die integrierte Sicherheitseinrichtung deutlich reduziert wird, um zum einen eine einfache Übertragbarkeit von Sicherheitssystemen auf neue Herausforderungen (bspw. Interoperabilität mit Netzen und zwischen Ladepunkten ohne Backend) zu gewährleisten und zum anderen, um den Preis eines Sicherheitssystems noch stärker zu reduzieren. Dies führt zu Faktor 3 - 4 kürzeren Entwicklungs- und Zertifizierungszeiten und senkt somit deutlich die Kosten der Sicherheitssteuerung. Diese werden dadurch für viele Anwendungen erschwinglich und tragen zur Attraktivität der Elektromobilität bei.

2.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Voraussetzung für die Bearbeitung des Vorhabens waren die unterschiedlichen Kompetenzen im Bereich des sicheren und zuverlässigen Schaltungsentwurfs nach Norm, der funktionalen Sicherheit, der sicheren Bezahlungsverfahren und die Erfahrung in Leistungselektronik und Starkstrom.

Das Fachgebiet Rechnerarchitektur und Systemprogrammierung wurde im Jahre 2005 gegründet und hat sich zum Ziel gesetzt, intelligente, zuverlässige und sichere Rechnerarchitekturen zu entwerfen, diese mathematisch zu beschreiben und durch reale Aufbauten sowohl zu verifizieren als auch zu validieren. Dabei ist ein Schwerpunkt die Konzeption und Erforschung neuer und sicherer Strukturen. Der Umfang der Forschung reicht von den eigentlichen Hardwarestrukturen und Architekturen, über den Entwurf sicherer Softwaresysteme, bis hin zu sicheren Netzwerken.

Um sichere Hardware oder Komponenten zu entwerfen und beurteilen zu können, benötigt es langjährige Erfahrung in diesem Bereich. Dieses zeigt sich durch fortwährende Entwicklungen von sicheren Architekturen, wie einer Hardware für industrielle Steuerungen[6,7] neuen, sehr sicheren Architekturen[8] oder „*Systems on Chips*" für den IOT Bereich[9].

[6] Hayek A. and Börcsök J., 2016: Miniaturized Safety PLC on a Chip for Industrial Control Applications. 13th International Conference of Distributed Computing and Artificial Intelligence (DCAI16), June 01-04. Sevilla, Spain.
[7] Josef Börcsök, Miniaturized Safety Systems: A Way for Future Tasks in Safety Engineering, 2015 XXV International Conference on Information, Communication and Automation Technologies (ICAT) October 29 – October 31, 2015, Sarajevo, Bosnia and Herzegovina
[8] M. Abdelawwad, A. Hayek, A. Alsuleiman and J. Börcsök, FPGA Implementation of a Safety System-on-Chip Based on 1oo4 Architecture Using LEON3 Processor, 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 2018, pp. 231-235. doi: 10.1109/COMAPP.2018.8460288
[9] Josef Börcsök, Waldemar Müller, Eike Hahn, Michael Schwarz, and Mohamed Abdelawwad, Approach for a Safe-SoC for Cyber-physical Application according to IEC 61508. International Journal of Computers, vol. 14, 2020, doi: 10.46300/9108.2020.14.12.

Inhärente Diagnosemaßnahmen[10] sind ein weiterer Bestandteil, um sichere Systeme zu gestalten, damit die Systeme ein hohes Maß an Selbstüberwachung haben. Dies ist notwendig, um sicherzustellen, dass alle Komponenten intakt und zuverlässig arbeiten und interne Fehler die zu gefahrbringenden Situationen führen können, rechtzeitig erkannt und entweder eliminiert oder das System sicher abgeschaltet werden kann.

Nicht nur der eigentliche Entwurf ist wichtig, sondern auch der mathematische und/oder analytische[11] Nachweis, dass das System die geforderten Sicherheitsmaßnahmen erfüllt und das diese ausreichen, um das entworfene System in der geforderten Sicherheitskategorie einsetzen zu können. Weiterhin müssen auch Erfahrungen im Bereich der sicheren und zuverlässigen Softwareentwicklung[12] vorhanden sein.

Diese Kenntnisse sind notwendig, um dann sichere und zuverlässige Gesamtsysteme[13,14,15] entwickeln zu können, die den normativen Sicherheitsanforderungen genügen. Auch ein frühes Einbinden von Zertifizierungsinstituten ist hilfereich und wurde auch in diesem Projekt durchgeführt, um den generellen Aufbau und Vorgehensweise zu demonstrieren und frühzeitig Schwierigkeiten und Probleme zu vermeiden.

Erfahrungen im Umgang mit Systemen die in rauen, industriellen Umgebungen und unterschiedlichen Wetterbedingungen ausgesetzt sind, dabei aber durchaus höhere Spannungen bzw. Ströme geschaltet oder abgeschaltet werden müssen, kam dem Projekt durchaus zu Gute.

So wurden im ZIM-Projekt KF22030213 „Beschleunigung und Vibrationsmessung“ Messdaten in rauen Umgebungen im Bereich von Lokomotiven, sicherheitstechnisch schnell und korrekt ermittelt und bewertet, um im einstelligen Millisekunden-Bereich ein Durchrutschen der Räder zu erkennen und diesem sicherheitstechnisch entgegenzuwirken.

Im ZIM-Projekt KF2230214CL2 „Sicherheitsgerichtetes, diagnostisches Notschaltsystem zur sicheren Abschaltung und Verhütung von Spannungsunfällen bei Photovoltaikanlagen“ musste gewährleistet werden, dass im Fehlerfall Photovoltaikanlagen abgeschaltet werden. In einem Brandfall stehen die

[10] Larissa Gaus, Michael Schwarz and Josef Börcsök, Estimation of Optimal Safety Parameters for a Communication Channel with Required SIL 3 at runtime. 29th European Safety and Reliability Conference, (ESREL), 22 – 26 September 2019, Hannover, Germany

[11] Krini J. and Börcsök J., 2015: Contribution to reducing the critical faults in critical Software Systems Model. XXV International Conference on Information, Communication and Automation Technologies, October 29-31, 2015 Sarajevo, Bosnia & Herzegovina

[12] Schwarz M.H., Börcsök J., 2017: Digital Controller Design Using A Reliable Code Generation Framework. 3rd Workshop & Symposium Safety and Integrity Management of Operations in Harsh Environments, C-RISE3, October 18-20, 2017, St. John’s, NL, Canada.

[13] Josef Börcsök, Muhammad Ikram Hafiz, Ahmed Alsuleiman, Michael Schwarz, and Mohamed Abdelawwad, “Safe Position Detection Based on Safety System-on-Chip (SSoC) for Wireless IoT Application,” International Journal of Circuits, Systems and Signal Processing, vol. 14, 2020, doi: 10.46300/9106.2020.14.132.

[14] Sheng H., Schwarz M., Börcsök J., 2012: New Concept to Develop a Safety Sensor Network for Continuous Noninvasive Blood Pressure Monitoring. In Proceedings17th IEEE International Conference on Emerging Technologies & Factory Automation, 17-21 September 2012, Krakow, Poland, 2013, ISBN: 978-1-4673-4735-8

[15] Hayek A., Suna Y., Schreiber M., Börcsök J., 2012: FPGA-Based Wireless Sensor Network for Safety-Related Cognitive Systems. In Proceedings BIHTEL 2012, IX international Symposium on Telecomunications, IEEE Catalog Number: CFP122U-USB, 25-27 October 2012, Sarajevo, Bosnia and Herzegovina, ISBN: 978-1-4673-4874-4

Anlagen immer noch unter Spannung und wenn diese nicht sicherheitstechnisch abgeschaltet werden, dürfen Feuerwehrleute nicht löschen, da die hohen Spannungen für sie lebensgefährlich sind.

Im ZIM-Entwicklungsprojekt „FOLSA“ (Future Oriented Logistics Safety Application, Fkz. ZF4379002DB7) wurde eine Sicherheitsarchitektur für die Smart Factory entwickelt, bspw. für intralogistische Maschinen und Anlagen (Anwendung: Kransysteme). Hierbei wurde eine dezentral einsetzbare Steuerung entwickelt, der Industriestandards genügt. Der Fokus lag auch auf der Reduktion des Aufwandes bei komplexen Zertifizierungsprozessen von Anlagen und Maschinen in industriellen Anwendungen. Aufgrund der sich ändernden Produktvarianten verkürzen sich Produktlebenszyklen, immer mehr Aufgaben werden dezentralisiert abgewickelt und sind gleichzeitig ebenfalls Teilnehmer des IoT.

2.3 Planung und Ablauf des Vorhabens

Das Verbundprojekt gliedert sich insgesamt in folgende Arbeitspakete mit den entsprechenden Zeitabschnitten.

Tabelle 1: Projektzeitplan.

	2018				2019												2020							
	Q3	Q4			Q1			Q2			Q3			Q4			Q1			Q2			Q3	
	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8
AP1																								
AP2																								
AP3																								
AP4																								
						M1						M2						M3						M4

- AP1 – Erforschung Systemaufbau, experimentelle Versuchsreihen
- AP2 – Entwicklung der elektronischen Komponenten und der Hardware
- AP3 – Integration zu ganzheitlichem Laborsystem,
    - Durchführung von Laborversuchen,
    - Vorbereitung von Feldversuchen.
- AP4 – Umsetzung von Feldtests in einer Demonstrationsumgebung
    - Verifikation & Validation, Optimierung

Hieraus ergaben sich folgende Meilensteine.

- M1 – ***Meilenstein 1:*** Grundaufbau des Gesamtsystems erforscht,
    - erste experimentelle Aufbauten evaluiert.
- M2 – ***Meilenstein 2:*** Die Entwicklung der Hard- und Software
- M3 – ***Meilenstein 3:*** Laboruntersuchungen abgeschlossen,
    - Vorbereitungen zur Überführung in die Feldebene abgeschlossen,
    - Grundsätzliche Funktionalität von Hardware und Software
- M4 – ***Meilenstein 4:*** Forschungstätigkeiten abgeschlossen.

Die Arbeiten wurden entsprechend einem mit den Partnern zeitlich und inhaltlich abgestimmten Arbeitsplan durchgeführt.

Im ersten Arbeitspaket wurden unterschiedliche Prozessoren und Hardware-Core auf notwendige Rechenleistung, Spannungsverbrauch, unterschiedliche Kommunikationskanäle und Echtzeitbedingungen untersucht. Weiterhin wurden Analysen, Vergleiche und Bewertungen der notwendigen Hardware- und Softwarearchitekturen unter Gesichtspunkten der Echtzeitfähigkeit, der funktionalen Sicherheit und der Datenübergabe durchgeführt und ein Sicherheitskonzept wurde entwickelt. Ziel war es, einen geeigneten Prozessor auszuwählen. Die Ergebnisse wurden bei einem gemeinsamen Treffen präsentiert und verifiziert.

Im zweiten Arbeitspaket wurde ein erster Entwurf der Hardware mit entsprechenden Sicherheitsmerkmalen durchgeführt und ein Betriebssystem portiert und Anpassungen sowie erste Tests abgeschlossen.

Im dritten Arbeitspaket wurden die einzelnen Hardwaremodule hergestellt und zu einem Gesamtsystem integriert. Es fanden unter Laborbedingungen erste Analysen bezüglich der Funktionalität der entwickelten Elektronik und der Software statt, die eine generelle Funktion nachweisen sollen.

Im vierten und letzten Arbeitspaket wurden Optimierungen und Ergänzungen durchgeführt und ein zweiter Hardwareentwurf entwickelt. Eingehende Tests wurden ausgeführt und das entworfene System validiert. Anschließend wurde eine umgehende Sicherheitsbetrachtung durchgeführt.

Alle im Arbeitsplan vorgesehenen Arbeiten wurden entsprechend dem vorgegebenen Zeitplan bearbeitet. Eine Verlängerung des Projektes wurde nicht beantragt.

2.4 Wissenschaftlicher und technischem Stand an den angeknüpft wurde

Der Stand der Technik im Bereich der Ladesäulen für E-Fahrzeuge wird u. a. durch verschiedenste Produkte definiert. Heute werden typischerweise folgende Komponenten für eine öffentliche low-cost Ladesäule benötigt:

- Eine SPS mit 16 DI/16 DO zur Steuerung der Ladesäule (2-3 Steckverbinder)
- Eine CP Box mit Ethernet um Lastmanagement zu ermöglichen
- Einfacher (tw. nicht geeichter) Zähler mit S0 Impulsausgang oder
- eHz mit SML, betrieben über serielle Schnittstelle
- Die übliche elektrische Ausstattung (FI, Sicherung, Leistungsschütz, Beleuchtung usw.) für EV7P und Schuko

Insbesondere im privaten Bereich weisen alle Angebote bezüglich Sicherheit ein deutliches Defizit auf. So hat keine der günstigen Ladestationen einen FI-Schalter, geschweige denn sind diese motorisch schaltbar. Die Anbieter gehen davon aus, dass die Sicherheitseinrichtungen im privaten Umfeld nicht unbedingt erforderlich sind, da diese vom Vorhandensein entsprechender

Sicherheitstechnik ausgeht. Allerdings ist diese in vielen Haushalten nach wie vor nicht existent, sodass hier gefährliche Zustände entstehen können oder umfangreiche Investitionen in die Haustechnik vorgenommen werden müssen. Somit bedarf es einer Lösung, welche den Sicherheitsanforderungen an eine Ladestation gerecht wird.

In den letzten Jahren haben immer mehr Halbleiterhersteller sicherheitsgerichtete, integrierte Lösungen auf den Markt gebracht, insbesondere nach der Einführung von der zweiten Edition der Norm IEC 61508 und der Norm ISO 26262 für die Automobilindustrie. Solche sicheren Chips sind vorwiegend auf die Bedürfnisse einer Zielbranche abgestimmt.

In diesem Zusammenhang haben führende Halbleiterhersteller in den letzten Jahren diverse Lösungen mit unterschiedlichen Lösungsansätzen zur Erfüllung von Sicherheitsanforderungen eingeführt. Die Firma NXP beispielsweise hat mit MPC564xL eine Serie von Chips für Anwendungen im Bereich der funktionalen Sicherheit in ihrem Programm. Diese bieten für die Erfassung von Sensordaten unterschiedliche Anschlussmöglichkeiten, wie zum Beispiel GPIO, LINFlexD, DSPI, FlexCAN und FlexRay. Auch einige Analog-/Digitalwandler sind auf diesem Chip integriert. Der Chip ist nach ISO 26262 mit ASIL D[16] zertifiziert. Die Produktserien RM46x und RM48x der Firma Texas Instruments bieten Chips, die es ermöglichen sicherheitsgerichtete Anwendungen bis SIL3 nach IEC 61508 zu implementieren. Als Anschlussmöglichkeiten stehen hierbei EMAC, USB, DCAN, SCI, LIN und GPIO zur Verfügung[17].

Die Firma Intel hat im Jahr 2016 mit dem Intel® Xeon® Processor D-1529 einen SIL2 zertifizierten Chip auf den Markt gebracht. Dieser bietet mit 8 USB-Ports, 2 SATA-Ports, GPIO und UART allerdings nur eingeschränkte Anschlussmöglichkeiten für industrielle Sensoren[18].

Die Reihe SPC5 der Firma STMicroelectronics bietet verschiedene Systeme die nach ISO 26262 mit ASIL B oder ASIL D zertifiziert sind. Die Spezifikationen variieren hier je nach Modell stark. Als Anschlüsse werden prinzipiell GPIO, FlexCAN, FlexRay, LINFlex und SPI zur Verfügung gestellt. Außerdem verfügen die Chips über eine unterschiedliche Anzahl an Analog-/Digitalwandlern [19].Diese Chips bieten zwar eine Vielzahl von Anschlussmöglichkeiten, sind aber nicht spezialisiert auf einzelne Anwendungen. Deshalb bieten sie oftmals nicht die optimalen Anschlüsse bzw. gehen weit über die Bedürfnisse hinaus. Dies führt zu einem größeren Platzbedarf, einer erhöhten Leistungsaufnahme und damit verbunden zu höheren Kosten.

Ein Schwerpunkt der aktuellen Forschung und Entwicklung liegt vorwiegend auf der Anwendung sicherheitsgerichtete Chips im Bereich der Sensorerfassung und Sensorsteuerung und der Nutzung in der Zusammenarbeit zwischen Menschen und Maschine. Mit diesem Hintergrund ist auch die sichere Kommunikation stets Gegenstand der Forschung.

[16] Product Brief von April 2011: https://www.nxp.com/docs/en/product-brief/MPC5643LPB.pdf Abruf 23.2.21
[17] TÜV Süd Zertifikat für RM48 von Februar 2016: http://www.ti.com/lit/ml/spnq004b/spnq004b.pdf Abruf 23.2.21
[18] Product Brief von November 2016: http://www.intel.com/content/dam/www/%20public/us/en/ documents/product-briefs/xeon-processor-d1529-industrial-61508-certification-product-brief.pdfAbruf 25.2.21
[19] St-Microcontrollers https://www.st.com/en/automotive-microcontrollers.html#documentation Abruf 25.2.21

Allgemein befindet sich heute eine Reihe sicherheitsgerichtete Kommunikationsprotokolle im industriellen Einsatz. Beispiele sind unteranderem PROFIsafe, CIP-Safety, FF-SIF, POWERLINK-Safety und FSoE. Manche von diesen Protokollen können sowohl kabelgebunden als auch über eine Funkstrecke übertragen werden[20]. Jedoch werden im industriellen Umfeld heutzutage größtenteils feldbusbasierte Systeme eingesetzt, besonders im sicherheitskritischen Kontext [21].

2.4.1 Angabe bekannter Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden

Es wurden auf keine existierenden Konstruktionen zurückgegriffen oder verwendet, da die Sicherheitsplatine komplett neu entwickelt wurde.

2.5 Zusammenarbeit mit anderen Stellen.

Das Projektkonsortium für das Projekt SiLiS setzte sich aus zwei Industriepartnern und universitären Instituten / Fachgebieten zusammen:

- ProSystems GmbH
- kortec Industrieelektronik GmbH & Co. KG
- Institut für Fördertechnik und Logistiksysteme (IFL)
- Fachgebiet Rechnerarchitektur und Systemprogrammierung (ICAS)

Mit den Verbundpartnern gab es eine intensive Zusammenarbeit, zum einen wurden wöchentliche Telefonkonferenzen abgehalten die das Fachgebiet Rechnerarchitektur und Systemprogrammierung (ICAS) geleitet hat und halbjährige Konsortialtreffen. Die Konsortialführung hatte die Firma ProSystems GmbH. Für die Vorstellung des Sicherheitskonzeptes wurde auch ein Treffen beim TÜV-Nord vereinbart, der das Verfahren positiv bewertet hat.

Die inhaltlichen Schwerpunkte der Arbeiten setzten sich wie folgt zusammen:

Die Firma ProSystems GmbH hat ihre Expertise im Bereich der Entwicklung von sicheren Bezahlsystemen, Kommunikation und Queueing Systemen. Dazu musste entsprechende Software entwickelt und auf geeignete Hardware portiert und angepasst werden. Vor allem wurde das Betriebssystem für das *Operational Board* (nicht sicherer Teil des Gesamtsystems) portiert und angepasst.

Die Entwicklung und Fertigung der Haupthardware (*Main Board*) und Peripherie wurde von der Firma kortec Industrieelektronik GmbH & Co. KG. Kortec durchgeführt, sie besitzt das Know-how zur Einhaltung aller relevanten Normen und EMV-Richtlinien. Ebenso wurden entsprechende Tests durchgeführt. Hier wurde vor allem das Hauptboard (*Operational Board*) und die Vorrichtung der Abschaltung der Ausgänge entwickelt.

[20] J. Wollert, "Wireless systems for machinery safety," in 2015 16th International Conference on Research and Education in Mechatronics (REM), 2015, pp. 88–91.
[21] J. Streib, "Wireless und funktionale Sicherheit," open automation, http://www.openautomation.de/uploads/pics/o30533zsh_safety_network.pdf. (accessed: Feb. 14 2021).

Das IFL konzentrierte sich auf die Applikationen, die auf dem sicheren Hardwareteil ausgeführt werden, ebenso wurde die FMEA für das *Operational Board* durchgeführt.

Das ICAS hat die Aufgabe die Sicherheitsplatine (*Safety Board*), die das sichere Laden überwacht, zu entwerfen, ein sicheres Betriebssystem zu portieren und das sichere System zu testen. Eine Sicherheitsbewertung mithilfe einer FMEA wurde für die Sicherheitsplatine erarbeitet, sowie Tests zur Validierung und Verifizierung des Sicherheitssystems. Weiterhin wurden Optimierungen und Anpassungen durchgeführt und ein zweiter optimierter Prototyp entwickelt, getestet und bewertet.

3. Eingehende Darstellung

Dieses Kapitel beschreibt die erzielten Ergebnisse, den voraussichtlichen Nutzen, sowie deren Vermarktung bzw. Veröffentlichungen. Im Allgemeinen wird zuerst der Zusammenhang zum Energiesektor bzw. Laden von E-Fahrzeugen gezogen, im nächsten Schritt aber die Betrachtung auf den Bereich der funktionalen Sicherheit bezogen.

3.1 Erzielte Ergebnisse

3.1.1 Sicherheitsarchitektur allgemein

Ein sicheres Prozessorsystem ist gekennzeichnet, im Vergleich zu einem normalen Mehrprozessorsystem, dadurch, dass die beiden Kerne in diesem Fall komplett eigene Ressourcen haben. Somit kann keiner den anderen beim Zugriff auf z.B. Speicher den anderen blockieren. Oft werden bei den Standardprozessoren Bus und Komponenten geteilt, bei einem Fehler kann dies zu sogenannten *„Single Point of Failure“* führen, das heißt, wenn der Bus versagt, können beide Prozessoren nicht mehr agieren. Solche Fehler gilt es entweder durch Design zu vermeiden oder die Fehler müssen detektiert werden und das Gesamtsystem muss anschließend in den sicheren Zustand überführt werden. Dieser sichere Zustand ist so zu gestalten, dass von dem System keine Gefahr für Mensch und Umwelt ausgeht.

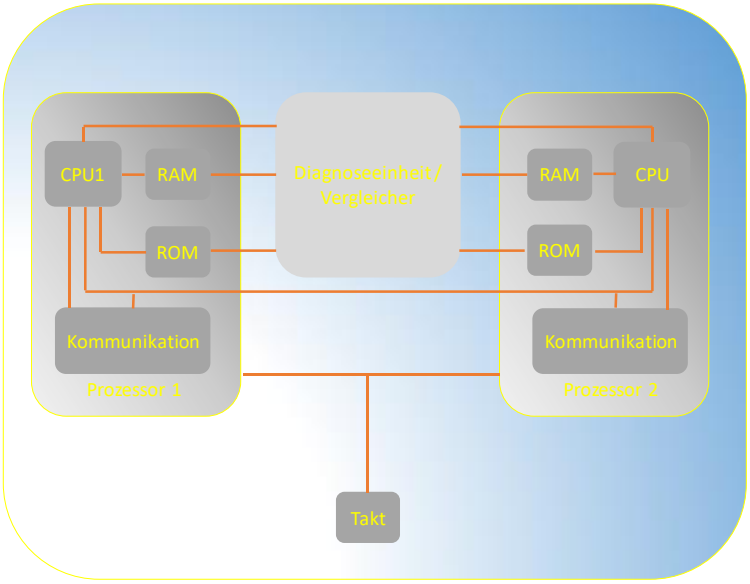


Abbildung 2: Sicherer Prozessorkern

Die Aktivitäten von Prozessor 1 und Prozessor 2 werden über die Diagnoseeinheit oder Vergleicher überwacht. Sind die errechneten Ergebnisse unterschiedlich, liegt ein Fehler vor und das Gesamtsystem wird sicher abgeschaltet. Auch wenn ein Prozessor ausfallen sollte, kann der

übriggebliebene ebenfalls das System abschalten und in den sicheren Zustand gehen. Der Vergleicher kann als Hardware-Vergleicher aber auch als Softwarevergleicher ausgelegt werden.

3.1.2 Architektur des Ladesäulensystems

Die gesamte Steuerung des Ladevorganges ist in der untenstehenden Abbildung skizziert, es besteht aus dem *Main Board* (MAB), den *Operational Board* (OPB) und dem *Safety Board* (SAB). Das *Main Board* ist das zentrale Kernstück und beherbergt den Hauptladestromkreis und die Fehlerstromschutzsensoren. Weiterhin versorgt es alle anderen Platinen mit der nötigen Grundspannung (diese wird dann auf den Boards noch entsprechend runtergeteilt). Weiterhin erfolgt die Kommunikation unter den einzelnen Komponenten über das *Main Board*.

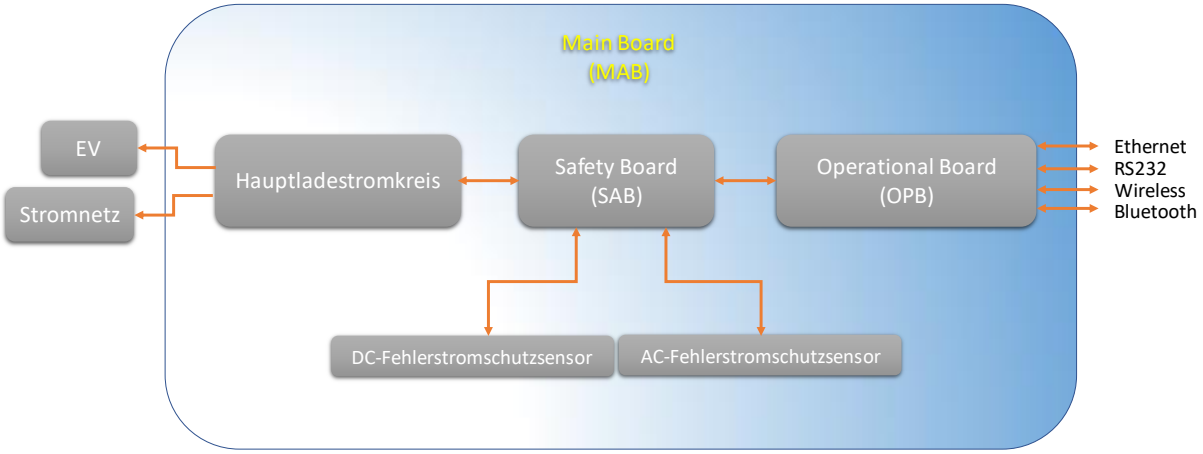


Abbildung 3: Gesamtsteuerung

Das *Operational Board* (OPB) besitzt mehrere Kommunikationsmöglichkeiten wie Ethernet, WiFi, RS232 und Bluetooth. Auf dem Board läuft aber auch die Abrechnungssoftware, SAP und die Kommunikation zu den Netzbetreibern. Weiterhin müssen das OPB und das *Safety Board* (SAB) miteinander kommunizieren, damit nur das abgerechnet wird, das auch verbraucht bzw. geladen wurde. Das *Safety Board* ist für die Bereitstellung des erforderlichen Sicherheitsniveaus für das gesamte System verantwortlich. Dies erfolgt durch die Verwendung eines Prozessors mit Sicherheitsarchitektur wie bereits generell beschrieben. Das Sicherheitssystem ist nach dem Fail-Safe-Prinzip aufgebaut, das heißt dass wenn ein Fehler erkannt wird, wird das Gesamtsystem in den sichern Zustand gebracht und damit der Ladeprozess sicher abgeschaltet, so dass weder Personen noch Umwelt zu Schaden kommen. Der Hauptladestromkreis und die Fehlerstromschutzsensoren sind auf dem *Main Board* integriert und geben die Informationen bzw. Prozesswerte an das *Safety Board*. Wird hier ein Fehler detektiert wird sofort der Ladeprozess sicher unterbrochen. Im Normalbetrieb kommunizieren das *Operational Board* und *Safety Board* miteinander. Soll ein Ladeprozess beginnen, wird das Start Signal vom *Operational Board* an das *Safety Board* gesendet und wenn alle Sicherheitsvoraussetzungen erfüllt sind, beginnt das Laden. Das *Safety Board* gibt hierfür das Steuersignal an den Ladestromkreis. Wird der Ladevorgang unterbrochen, bzw. ist der Ladevorgang beendet, erfolgt der Stopp-Befehl und der Ladevorgang wird beendet und die finale Abrechnung kann im *Operational Board* erfolgen.

Die Kommunikation zwischen *Safety Board* and *Operational Board* erfolgt über eine UART Kommunikation. Die Status Meldungen werden zusätzlich noch optisch angezeigt.

3.1.3 Evaluierung verschiedener Prozessoren

Zu Beginn des Projektes wurden mehrere sichere Mikrokontroller untersucht und nach den verfügbaren Sicherheitsmerkmalen analysiert. Zwei Mikroprozessor-Familien kamen in die engere Auswahl. Zum einen die MPC5643L Mikroprozessor Serie von NXP®/Freescale® und der RM48 Herkules® MCU von Texas Instruments®. Eine Auswahl der Eigenschaften der beiden Prozessoren ist in der untenstehenden Tabelle aufgeführt.

Tabelle 2: Prozessor Vergleich

Eigenschaft	MPC5643L	RM48Lx (RM48L95)
SIL/ASIL	SIL3/ASIL D	SIL3/ASIL D
Safety Architektur	Lockstep-Betrieb	Lockstep-Betrieb
CPU	2 × e200z4	ARM Cortex R4F
Core-Bus	32 Bit	16/32 Bit
Maximale Taktungsfrequenz	120 MHz	220 MHz
FPU	Ja	Ja
Flash	1 MByte mit Fehler-Erkennung/ -Korrektur (ECC)	3 MByte mit Fehler-Erkennung/-Korrektur (ECC)
SRAM	128 KByte mit Fehler-Erkennung/-Korrektur (ECC)	256 KByte mit Fehler-Erkennung/-Korrektur (ECC)
Einheit CRC Check	Ja	Ja, zwei Kanäle
Fault Control & Collection Unit (FCCU)	Fault Control & Collection Unit (FCCU)	Fehlersignalisierungsmodul mit Fehler-Pin
Integrierter Selbsttest (BIST)	1. Integrierter Selbsttest für Speicher (MBIST) und Logik (LBIST) getriggert durch Hardware 2. Integrierter Selbsttest für ADC und Flash-Speicher, getriggert durch Software 3. Eingebauter Selbsttest für ADC und Flash-Speicher, ausgelöst durch Software	1. Integrierter Selbsttest (BIST) für CPU und On-Chip-RAMs

Mithilfe von zwei Entwicklungsplatinen wurden beide Prozessoren hinreichend getestet und deren Sicherheitseigenschaften evaluiert.

Beide Prozessoren arbeiten mit redundanten ALUs im Lockstep-Betrieb, das heißt beide Prozessoren führen das gleiche Programm aus und überwachen sich gegenseitig. Weiterhin verfügen beide über Speicher mit Fehler-Erkennung/-Korrektur (ECC) und Selbstdiagnose (BIST).

Der TI RM48Lx hat jedoch einen 3fach größeren Speicher was für das zu portierende Betriebssystem komfortabler ist, ebenso ergeben sich durch die höhere Taktung schnelle Zykluszeiten und letztendlich auch eine schnellere Reaktionszeit (ist die Zeit die benötigt wird vom Auftreten des Fehlers bis zum sicheren Abschalten des Systems, um es in den sicheren Zustand zu überführen).

Aus diesen Gründen wurde sich für den TI RM48Lx als zentraler Prozessor für das *Safety Board* entschieden.

3.1.4 Architektur System 1

Nachdem die Entscheidung für den TI RM48Lx als zentraler Prozessor für das *Safety Board* getroffen wurde, ging es an das Design einer ersten Hardwareplatine. Aus den Projektanforderungen sind folgende Eigenschaften in das Design eingeflossen:

1. Galvanische Trennung aller Ein- und Ausgänge sowie der Spannungsversorgung
2. Spannungsüberwachung der Eingangsspannung und aller auf dem Modul erzeugten Spannungen
3. Zweistufiger Hardware Watchdog
4. Schnittstellen zum Programmieren des Mikrocontrollers sowie einer Diagnose-Schnittstelle (UART)
5. Visualisierung der wichtigsten Zustände des Moduls (LED)

Abbildung 4: Safety Board Version 1

Das Architekturdesign der RM48Lx-Familie basiert auf dem Safe-Insel-Ansatz (Abbildung 5). Bei diesem Ansatz wird ein hohes Maß an Diagnoseabdeckung der Hardware erreicht, um die Stromversorgungs-, Takt-, Reset- und Basisverarbeitungseinheiten zu schützen. Das Design unterstützt den Lockstep-Betriebsmodus durch die Verwendung von Dual Cortex-R4F CPUs. In der Lockstep-Betriebsart werden die Ausgänge der beiden CPUs bei jedem CPU-Taktzyklus verglichen. Wenn der Vergleich eine Differenz ergibt, wird ein Fehlerinterrupt der höchsten Prioritätsstufe erzeugt. Die gemeinsamen Fehlerursachen der logischen CPU und ihres Prüfers werden durch spezielle Maßnahmen im Prozessor-Layout, der Taktverteilung, der Stromverteilung, der Reset-Verteilung und der zeitlichen Diversität migriert. Darüber hinaus wird eine in die Hardware integrierte Selbsttest-Engine (BIST) für die CPUs und das SRAM verwendet, um ein hohes Maß an Diagnoseabdeckung zu gewährleisten. Ein solcher Ansatz ist im Vergleich zu softwarebasierten Selbsttestlösungen effizienter in Bezug auf den Strom- und Speicherverbrauch. Für die Fehlerkorrektur in SRAM- und Flash-Speichern wird ein Error Correction Code (ECC) Controller verwendet, der sich innerhalb der CPU befindet. Der Vorteil der Existenz des ECC-Controllers innerhalb der CPU ist die Fähigkeit, die Verbindung zwischen dem Speicher und der CPU abzudecken. Außerdem wird durch den Lockstep, der in der sicheren Insel vorgesehen ist, die ECC selbst in jedem Taktzyklus überprüft. Eine Onboard-Überwachungslogik für Spannung, Reset, Oszillator und PLL ist ebenfalls implementiert. Bei Erkennung eines Fehlers in der Oszillator- und PLL-Schaltung kann ein Backup-RC-Oszillator verwendet werden.

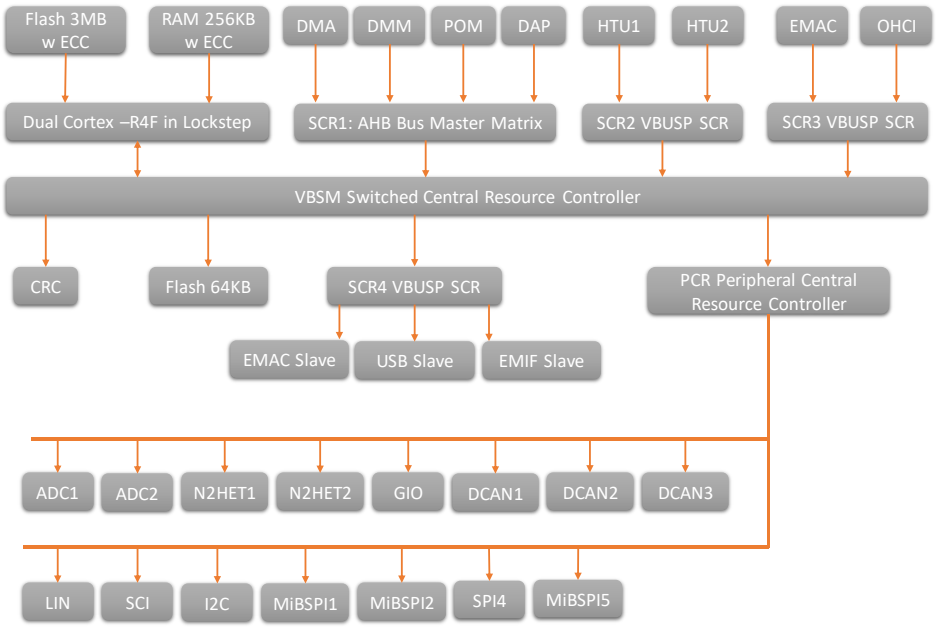


Abbildung 5: Architektur-Blockdiagramm des RM48Lx Mikrokontroller

Eine galvanische Trennung wurde im Design aufgenommen um zu verhindern, dass durch z.B. einen technischen Defekt im Ladestromkreis ein zu hoher Strom das *Safety Board* beschädigen würde und

dieses wiederum nicht mehr in der Lage wäre die Sicherheitsfunktion, als das sichere Abschalten durchzuführen.

Die Spannungsüberwachungen sind dafür da, um kleinere Spannungsschwankungen auszugleichen aber auch bei stärkeren Einbrüchen oder Spitzen, die den Prozessor gefährden könnten, diesen zu schützen und abzuschalten, so dass er nicht beschädigt wird und seine Funktion nicht mehr zuverlässig ausführen kann. Die Auswirkungen einer Übersteuerung können Datenverluste oder -korruption betreffen. Es ist auch möglich, dass sich die Lebensdauer der elektrischen Elemente verkürzt. Es kann zur Beschädigung der elektronischen Komponenten und sogar zur Verbrennung oder Zerstörung der Geräte sowie zur Entstehung eines Brandes führen. Die Versorgung der elektrischen Komponenten mit niedriger Spannung bedingt das Fließen eines höheren Stroms, um die Leistungsanforderungen zu erfüllen. Das Fließen eines höheren Stroms kann die Lebensdauer verkürzen. Eine andere Gefahr besteht darin, dass die elektronischen Bauteile in einem undefinierten Zustand belassen werden.

Ein zweistufiger Watchdog wurde für das Design verwendet. Der Hardware-Watchdog besteht aus zwei dual retriggerbaren monostabilen Multivibrator-Chips (Abbildung 6). Der Ausgang des ersten Chips ist mit der Diagnoseschaltung und mit dem Eingang des zweiten Chips verbunden. Der zweite Chip wird verwendet, um den Betrieb des WD zu überprüfen, indem sein Ausgang während des periodischen Tests von der CPU gelesen wird. Wenn die WD-Chips nicht getriggert werden, ist der Ausgang immer high. Der Ausgang ist nur dann Low, wenn die WD-Chips alle 10 ms getriggert werden (Abbildung 7). Beim periodischen Test wird das WD getriggert und das WD-Diagnosesignal gelesen, um die Funktionalität des WD zu testen.

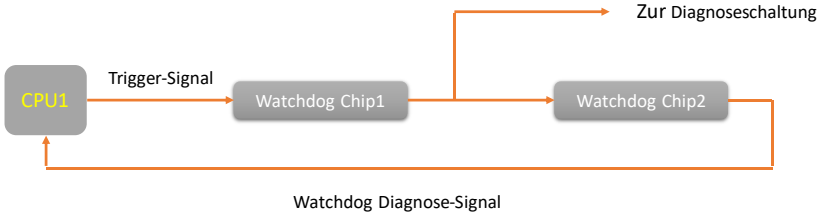


Abbildung 6: Hardware Watchdog

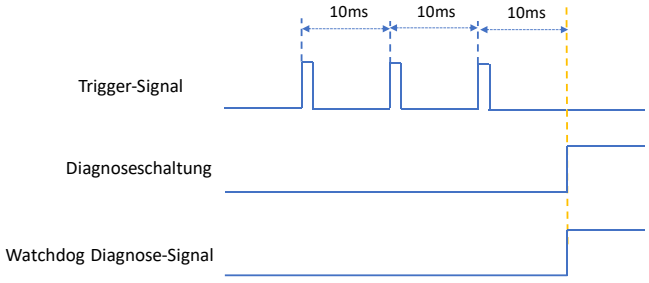


Abbildung 7: Signalverlauf des Watchdogs

Die beiden verfügbaren Schnittstellen sind zum einem zum Programmieren und zum anderen zum Aufspielen des Betriebssystems, diese Schnittstelle wird aber während des operativen Betriebs nicht genutzt.

Eine einfache Statusanzeige ist ebenfalls implementiert. Während der Entwicklung der Software ist die Bereitstellung von Informationen über den Mikrocontroller-Status und das SAB-Board für die entwickelte Software sehr hilfreich und wichtig, um die Funktionalitäten der Software zu testen. Außerdem sind diese Informationen sehr nützlich für die Phase der Hardware-Verifizierung und -Validierung. Deshalb wurden eine UART-Diagnoseschnittstelle und ein LED-Modul auf dem *Safety Board* implementiert

Das Safety Board wurde als Einsteckmodul entwickelt und kann auf das *Main Board* in den vorgesehenen Slot eingesteckt werden. Über diese Verbindungen zum Main Board werden folgende Daten bzw. Informationen gesendet.

Tabelle 3: Pins

PIN / Signalname	Typ	Funktionalitäten
FI_Error_Out	INPUT	Fehlerdiagnose-Signal des Fehlerstrom-Schutzschalters (RCD) Sensor. Das Signal wird gesetzt, wenn beim Sensor ein Fehler auftritt.
FI_6mA_OUT	INPUT	Falsches Diagnostiksignal. Es wird gesetzt, wenn der DC-Strom größer als 6 mA ist.
FI_PWM_OUT	INPUT	Signalisierung des Fehlerstroms wird mit einer Periodendauer von =8kHz erzeugt. Diese Funktion dient nur zu Überwachungszwecken und ist keine Sicherheitsfunktion.
FI_30mA_OUT	INPUT	Falsches Diagnostiksignal. Es wird gesetzt, wenn der AC-Strom größer als 30 mA ist.
FI_Test_in	OUTPUT	Fehlerstrom-Schutzschalter (RCD) Sensor -Testsignal
FI_Test_AC	OUTPUT	Stromfehler-Injektionssignal
Rel_K102	OUTPUT	Steuersignal des Relais K102.
Rel_K103	OUTPUT	Steuersignal des Relais K103.
Rel_K104	OUTPUT	Steuersignal des Relais K104.
Rel_K105	OUTPUT	Steuersignal des Relais K105.
U_Mess_S1.1	INPUT	Überwachungssignal der Stromphase 1 in der Relaissteuerung Stufe 1
U_Mess_S1.2	INPUT	Überwachungssignal der Stromphase 2 in der Relaissteuerung Stufe 1
U_Mess_S1.3	INPUT	Überwachungssignal der Stromphase 3 in der Relaissteuerung Stufe 1
U_Mess_S2.1	INPUT	Überwachungssignal der Stromphase 1 in der Relaissteuerung Stufe 2
U_Mess_S2.2	INPUT	Überwachungssignal der Stromphase 2 in der Relaissteuerung Stufe 2
U_Mess_S2.3	INPUT	Überwachungssignal der Stromphase 3 in der Relaissteuerung Stufe 2

EVM_CP_CONN1	INPUT	Control-Pilot-Signal von OPB-Platine
EVM_CP_CONN1	INPUT	Redundantes Control-Pilot-Signal von der OPB-Platine
SAB_UARTx_TX	OUTPUT	Sendersignal an die OPB-Platine.
SAB_UARRx_RX	INPUT	Empfängersignal von der OPB-Platine.

Architektur der Fehlerdiagnose im System ist wie folgt entwickelt worden. Die Systemdiagnose hat vier Signale:

- Watchdog-Signal,
- externes Spannungsüberwachungs-Fehlersignal,
- internes Spannungsüberwachungs-Fehlersignal und
- Fehlerstrom-Schutzschalter (RCD)-Sensor-Fehlersignal.

Die vier Signale, wie in Abbildung 8 gezeigt, werden über ein ODER-Gatter ausgekoppelt. Der Ausgang des ODER-Gatters wird invertiert und über ein UND-Gatter mit dem von der CPU kommenden Steuersignal des Relais verbunden. Der Ausgang des UND-Gatters liefert das Steuersignal für die Relais. Tritt ein Fehler in einem der vier Signale auf, ist der Ausgang des ODER-Gatters „TRUE“ und somit das Steuersignal der Relais immer niedrig. Dies bedeutet, dass sich das System im stromlosen Betriebsmodus befindet, der den sicheren Zustand darstellt.

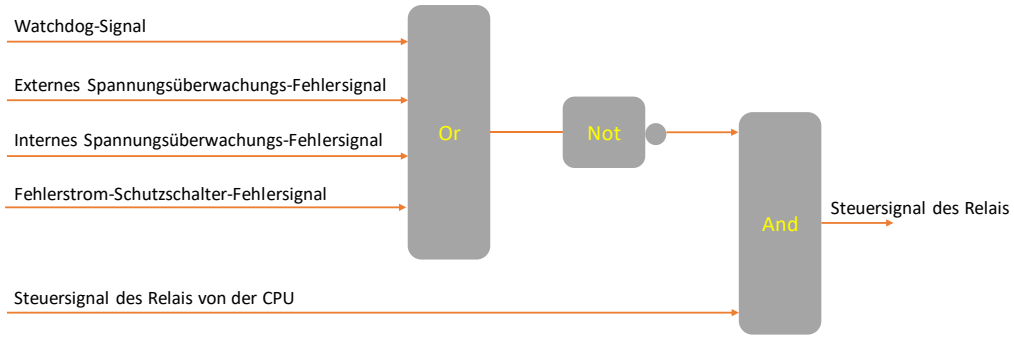


Abbildung 8: Architektur der Fehlerdiagnose

Das entworfene *Safety Board* und Safety Konzept wurde mit den Projektpartnern am 14.08.2019 beim TÜV Nord vorgestellt. Dieser hatte keine Bedenken, dass das Hardware-Design rechnerisch SIL3 einhalten wird. Weiterhin wurde vermutet, dass die Risikoanalyse lediglich SIL1 voraussetzen wird.

3.1.5 Architektur System 2

Im zweiten und finalen Entwurf wurden zuerst kleinere Designfehler, die sich durch das Testen ergeben hatten, eliminiert. Weiterhin stellte sich, dass die Leistung der zwangsgeführten Relais in Zukunft nicht dem Standard auf dem Markt entsprechen wird. Mangels einer leistungsstärkeren Alternative wurden die zwangsgeführten Relais durch normale Leistungsrelais ersetzt und um zusätzlicher Diagnose Kanäle erweitert, um die geforderte Sicherheit zu erreichen. Dadurch wurde das Design des Mainboards und des Safety Boards geändert. In Abbildung 9 ist die finale Version des Safety Boards mit den einzelnen Bereichen abgebildet. Es besitzt die gleichen funktionalen Sektionen wie die erste Version: Status-Anzeigen, Programmier-/Diagnoseschnittstelle, interne und externe

Spannungsüberwachung und eine Spannungsversorgung, den Safety Mikrokontroller, Ein- und Ausgänge, galvanische Trennung, die Kontrolllogik sowie den zweistufigen Watchdog. Erneut wurden alle Tests an dem Board durchgeführt. Ebenso sind entsprechende Sicherheitsanalysen ausgeführt worden, die in den nächsten Abschnitten genauer beschrieben werden.

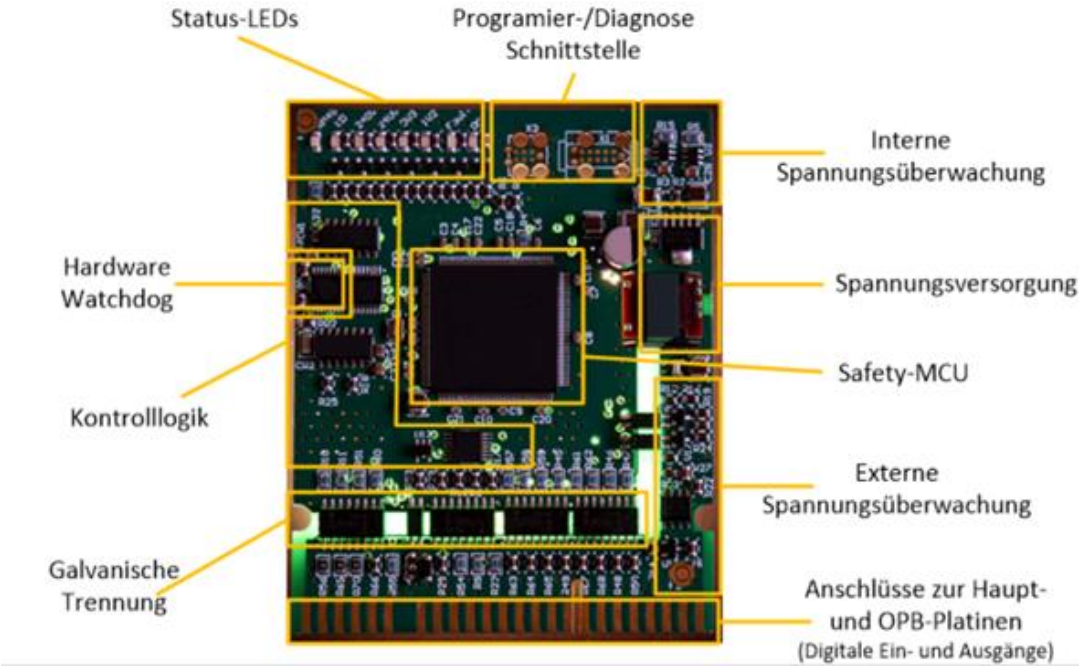


Abbildung 9: Safety Board Version 2

3.1.6 Software Portierung

Auf der Basis des ersten Prototyps wurde eine Testversion des SafeRTOS Betriebssystem der Firma WITTENSTEIN portiert. Das SafeRTOS ist ein IEC 61508-3 SIL 3 vorzertifiziertes Echtzeitbetriebssystem für Mikrocontroller. Das SAFERTOS basiert auf einem präemptiven Echtzeit-Scheduler. Es können beliebig viele Tasks, je nach Verfügbarkeit von ausreichend RAM-Speicher, ausgeführt werden. Jeder Task ist einer bestimmten Prioritätsstufe zugeordnet. Es ist auch möglich, die gleiche Prioritätsstufe zwischen mehreren Tasks zu teilen. Allerdings wird nur der Task mit der höchsten Prioritätsstufe vom Betriebssystem zuerst ausgeführt. In SafeRTOS wird eine zeitscheibenbasierte Round-Robin-Policy verwendet, bei der sich alle Tasks mit der gleichen Prioritätsstufe die Verarbeitungszeit teilen wie in Abbildung 10 verdeutlicht. Das Prinzip der Warteschlangen kann verwendet werden, um Daten zwischen Tasks oder zwischen Tasks und den Interrupt-Subroutinen zu senden. Es ist auch möglich, einige Tasks für eine bestimmte Zeit zu blockieren. Jede Aufgabe kann einen von vier Zuständen haben:

- Bereit: Bereit ist der Anfangszustand, wenn ein Task erstellt wird.
- Laufend: Die Aufgabe wird nun bearbeitet.

- Blockiert: Der Task wird für eine bestimmte Zeit gesperrt. Diese kann erst nach Ablauf der Zeitspanne vom Scheduler ausgewählt werden.
- Angehalten: Der Task ist blockiert. Er kann vom Scheduler erst ausgewählt werden, wenn dieser wieder freigegeben ist. Sie kann vom Scheduler ausgewählt werden, da eine freie Verarbeitungszeit basierend auf ihrer Prioritätsstufe zur Verfügung steht.

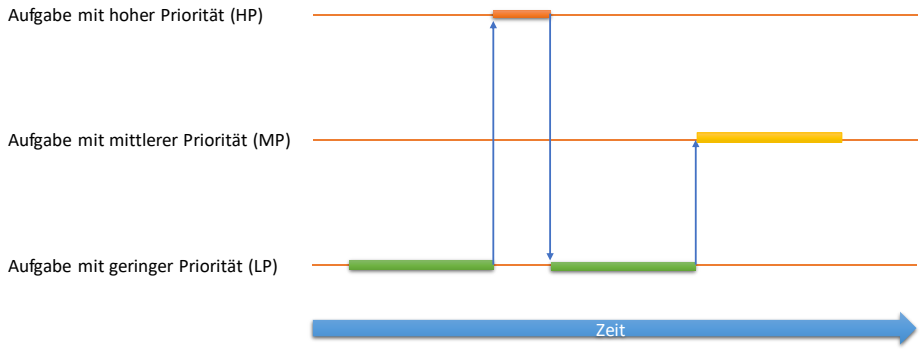


Abbildung 10:Durchführen von Aufgaben mit verschiedenen Prioritätsstufen in SafeROTS[22]

Zunächst wurde das Betriebssystem auf die Prozessoren portiert und die Funktionalität wurde getestet. Anschließend wurde es um einige Funktionen erweitert die die Eingänge, Ausgänge sowie die Hardware des Watchdogs betreffen. Die Änderungen erfolgten im Einklang mit dem V-Modell (Abbildung 1) und Anforderungen an die Software. Tests zur Verifizierung wurden ebenfalls durchgeführt.

3.1.7 Sicherheitsmodul Integration und Verifikation

Für alle Komponenten der beiden Versionen wurden Modultests geschrieben und die Funktionen der einzelnen Funktionsbereiche getestet. Beispiele für die Verifizierung verschiedener Module sind in den Abbildung 11, Abbildung 12, Abbildung 13 und Abbildung 14 zu sehen. Es wurden zwei Fehler im Schaltungsdesign entdeckt und in der zweiten Version korrigiert.

Abbildung 11 zeigt die Tests des Spannungsüberwachungsmoduls. Bei diesem Test wurde die Spannung von Unterspannung (< 12 Volt) bis Überspannung (>12 Volt) an die SAB angelegt und die Über- und Unterspannungssignale mit einem Oszilloskop aufgezeichnet. Die Ergebnisse zeigen die korrekte Funktion des Spannungsüberwachungsmoduls.

Das PWM-Überwachungssignal vom Stromsensor, der sich auf der Hauptplatine befindet, kann bis zu 8 KHz erreichen. Daher war es wichtig, die HF-Kopplung der galvanischen Trennung in der SAB-Platine zu testen. Mit einem Funktionsgenerator wurden Signale mit verschiedenen Perioden erzeugt. Diese Signale wurden über die galvanisch getrennten Pins in die SAB-Platine eingekoppelt. Die Resonanz wurde auf der anderen Seite mit einem Oszilloskop gemessen. Das Ergebnis bestätigt die gute HF-Kopplung bis 10 KHz, dies ist in den Abbildung 12 bis Abbildung 14 gezeigt.

[22] SafeRTOS, https://www.highintegritysystems.com/downloads/manuals_and_datasheets/Sample_SafeRTOS_User_Manual.pdf (accessed: Feb. 14 2021).

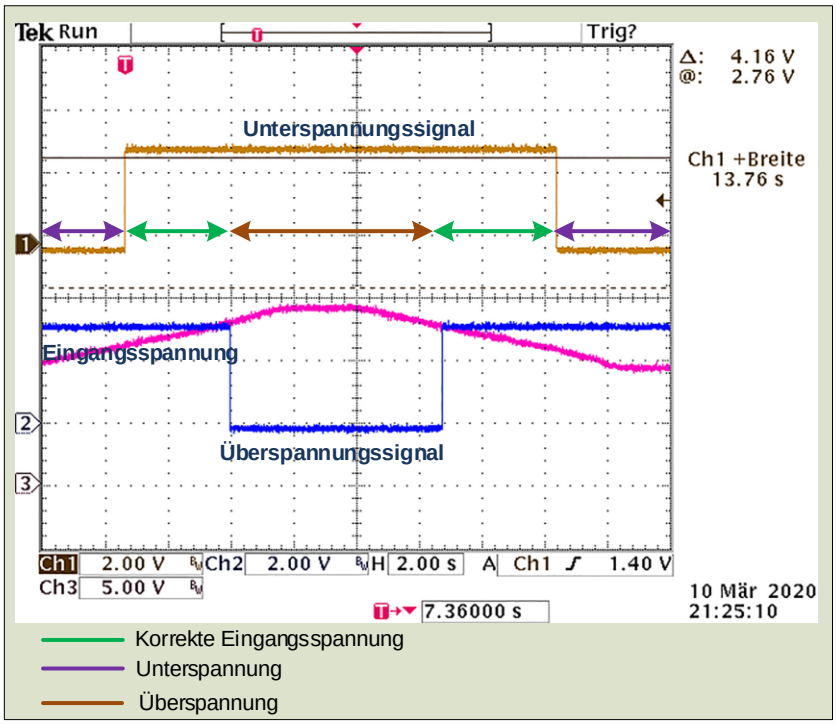


Abbildung 11: Verifikation der Spannungsüberwachung

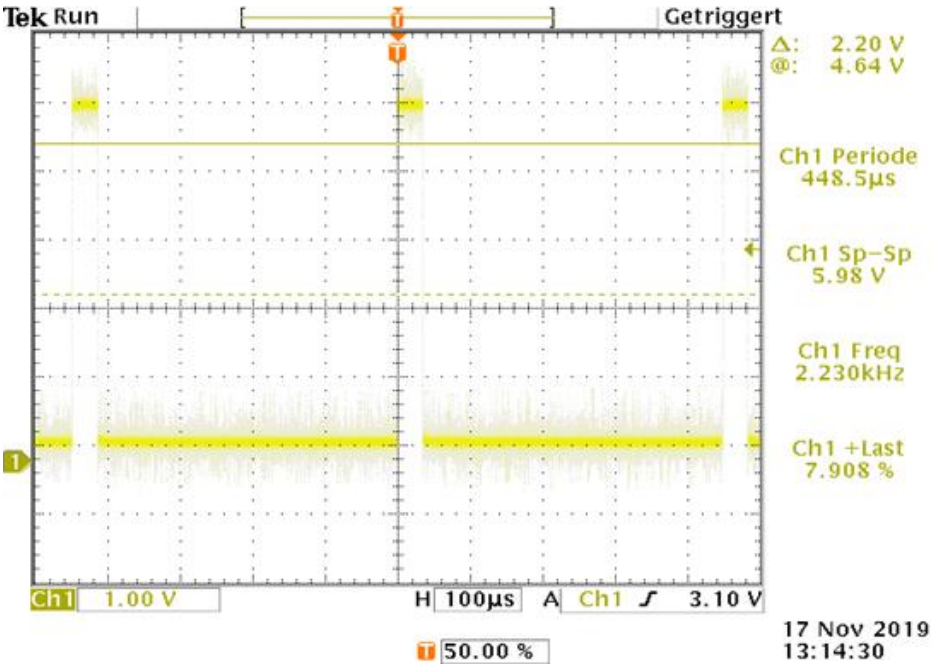


Abbildung 12: Verifizierung des PWM-Moduls (Periode = 448,5 µs & Arbeitszyklus = 92%).

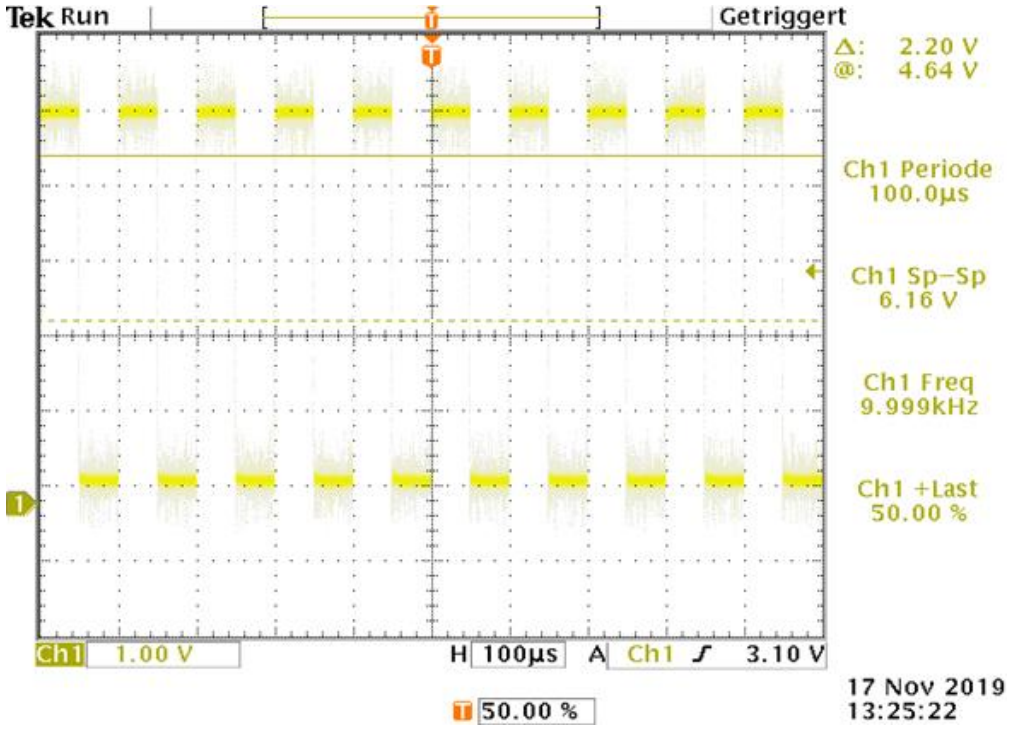


Abbildung 13: Verifizierung des PWM-Moduls (Periode = 98.9 µs & Arbeitszyklus = 50%).

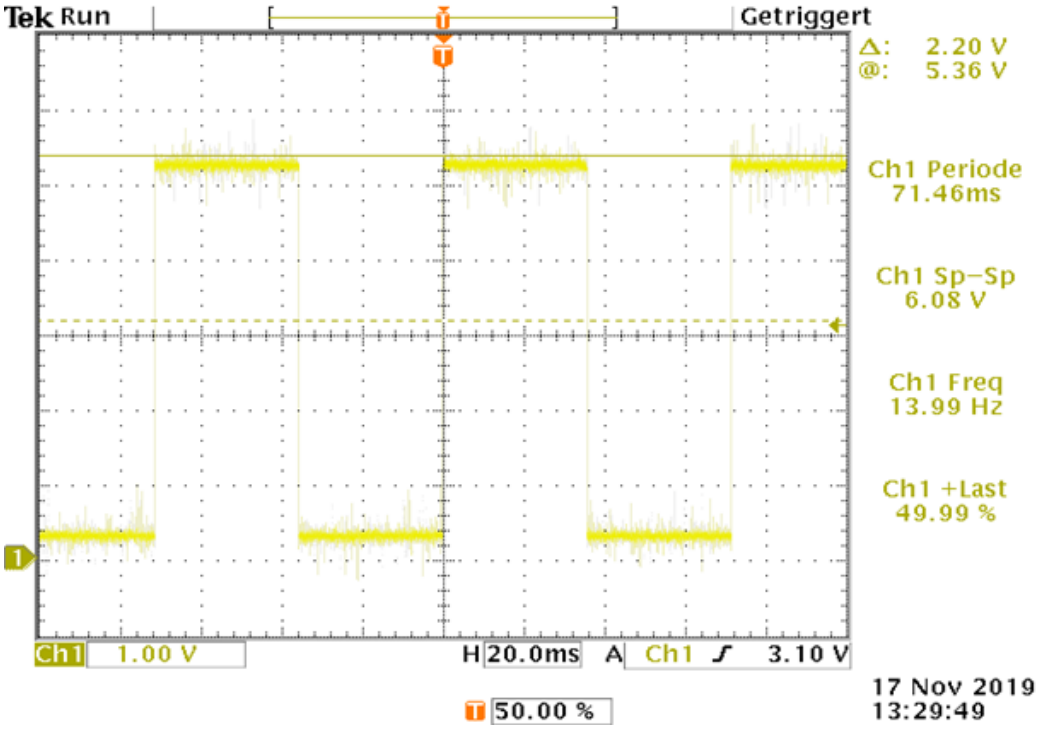


Abbildung 14: Verifizierung des PWM-Moduls (Periode = 71464,7 µs & Arbeitszyklus = 45 %).

3.1.8 FMEA allgemein

In diesem Abschnitt wird allgemein auf die Analysetechnik eingegangen, um diese dann im nächsten Abschnitt einzusetzen und das *Safety Board* zu bewerten. Eine der leistungsfähigen Techniken, die für die Risiko- und Gefahrenanalyse in der Hardware verwendet werden, ist die Fehlermöglichkeits- und -Einflussanalyse (engl. *Failure Mode and Effect Analyse*)[23] (FMEA). Es gibt verschiedene Arten von FMEA, d.h. Design-FMEA, Prozess-FMEA und System-FMEA[24]. In der Konstruktions-FMEA findet die Analyse der Funktionen des Systems, der Subsysteme und der Komponente statt, um den potenziellen Fehler in der Konstruktion zu identifizieren [25].

Die D-FMEA wird in sieben Schritten durchgeführt, d.h. Planung und Vorbereitung, Strukturanalyse, Funktionsanalyse, Fehleranalyse, Risikoanalyse und Optimierung. Im ersten Schritt werden der Umfang, die Zeitplanung, das Team, die Verantwortlichkeiten und die Werkzeuge festgelegt. Im zweiten Schritt wird die Struktur des Systems und seine Grenzen mit Hilfe von Block- oder Boundary-Diagrammen visualisiert (Abbildung 15). Die Funktionen der verschiedenen Subsysteme und Komponenten werden identifiziert, und schließlich wird die Fehleranalyse durchgeführt. In dieser Phase werden die Fehlermodi des fokussierten Elements, die Auswirkungen jedes Fehlers auf das System und die Ursachen spezifiziert. Basierend auf der Fehleranalyse werden die quantitativen Parameter, Schweregrad (S), Eintrittswahrscheinlichkeit (O) und Entdeckbarkeit (D), geschätzt. Jeder Parameter hat einen Wert zwischen 1 und 10, wobei der Wert von 1 die niedrigste Schwere und die Wahrscheinlichkeit des Auftretens sowie die höchste Erkennbarkeit des Fehlers darstellt. Der Wert von zehn steht dagegen für die höchste Schwere und Wahrscheinlichkeit und die geringste Erkennbarkeit dieser Störung[26]. Aus den drei Parametern wird die Reliabilitätsprioritätszahl (RPZ) berechnet, wie in Gleichung (1) dargestellt ist.

$$RPZ = S \cdot O \cdot D \tag{1}$$

Wenn der ermittelte RPZ-Wert größer als 125 (5 x 5 x 5) ist, ist das Risiko hoch und der Entwurf muss optimiert werden, um dieses Risiko zu verringern. Dies kann durch die Reduzierung der Eintrittswahrscheinlichkeit oder die Erhöhung der Erkennbarkeit des Fehlers erfolgen. Die Reduzierung der Auftretenswahrscheinlichkeit wird durch die Implementierung von Redundanz im System erreicht.

In einer anderen Implementierung der D-FMEA wird jedoch die Technik der Aktionspriorität (AP) verwendet, anstatt den Schwellenwert der RPZ zu verwenden. In diesem Fall werden alle möglichen Kombinationen von S, O und D berücksichtigt, um drei Stufen von AP zu bilden, d.h. Priorität hoch,

[23] FMEA – Fehlermöglichkeits- und Einflussanalyse. (PDF) Deutsche Gesellschaft für Qualität, 2012, (accessed: Feb. 14 2021).
[24] VDA, FMEA-Handbuch: Fehler-Möglichkeits- und Einfluss-Analyse: Design-FMEA, Prozess-FMEA, FMEA-Ergänzung - Monitoring & Systemreaktion, 1st Ed. Berlin, Germany: VDA, Verband der Automobilindustrie, 2019.
[25] F. Romeike and P. Hager, "Risiko-Management in der Produktion," in Erfolgsfaktor Risiko-Management 4.0, F. Romeike and P. Hager, Eds., Wiesbaden: Springer Fachmedien Wiesbaden, 2020, pp. 297–351.
[26] VDA, FMEA-Handbuch: Fehler-Möglichkeits- und Einfluss-Analyse: Design-FMEA, Prozess-FMEA, FMEA-Ergänzung - Monitoring & Systemreaktion, 1st ed. Berlin, Germany: VDA, Verband der Automobilindustrie, 2019.

Priorität mittel und Priorität niedrig. Weitere Informationen zu dieser Methodik ist in dem FMEA-Handbuch[23] zu finden.

3.1.9 FMEA des Systems

Die Struktur-Analyse des *Safety Boards* ist in Abbildung 15 dargestellt. Die Kommunikation mit der Betriebsplatine ist nicht dargestellt, da es sich nicht um ein sicherheitsrelevantes Modul handelt.

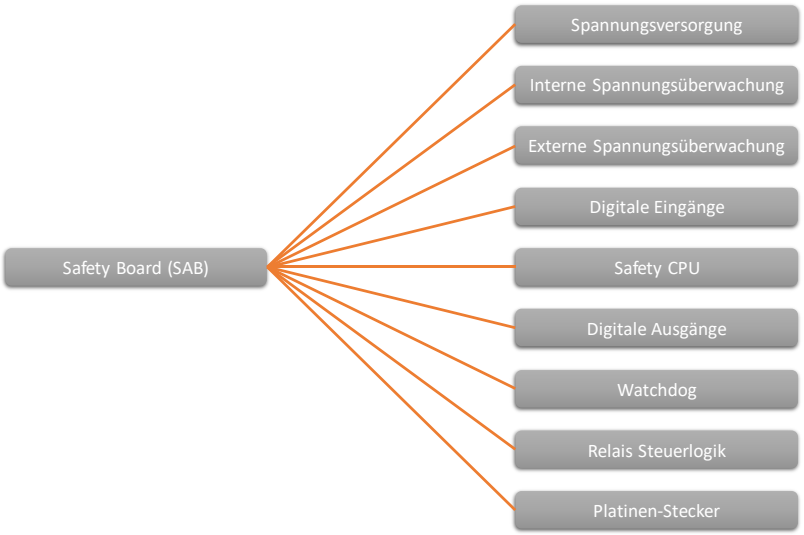


Abbildung 15: Struktur der Analyse

Alle Teilberechnungen werden nachfolgend berechnet. Die Berechnungstabellen werden im Bericht nur an-skizziert, die vollständigen Berechnungen befinden sich im Anhang des Berichtes.

3.1.9.1 Spannungsversorgung

Aufgabe: Die SAB-Platine wird mit 12 Volt von der Hauptplatine versorgt. Es wird benötigt, um den Safety-Chip mit 3,3 Volt und 1,2 Volt zu versorgen, während die anderen Chips mit 3,3 Volt versorgt werden. Daher befinden sich auf der SAB-Platine zwei Spannungswandler-Module, nämlich der DC-DC-WANDLER (wandelt von 12 Volt in 3,3 Volt um) und der Spannungsregler TPS73701DCQR (wandelt von 3,3 Volt in 1,2 Volt um).

Komponenten: Kondensator, Widerstände, Sicherung, Spule, Diode, DC-DC-Wandler, LDO

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 60, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

Tabelle 4: Berechnung skizziert für die Spannungsversorgung

Sub-sys.	Kom-ponente	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion
DC-DC-WANDLER	Sicherung	F3	Schutz (800mA)	Kein Durchbrennen (Kurzschluss)	keine	Unsicherer Zustand	4	1	nicht erkennbar
				Unterbrechung	keine Versorgungsspannung	Spannungsfreier (sicherer) Zustand	5	3	extern erkennbar, da das SAB Board nicht mehr antwortet
	Konden-sator	C35	Glättungskondensator und Teil des Eingangsfilters für den DC/DC Wandler U4	Kurzschluss	Sicherung F3 wird ausgelöst	Spannungsfreier (sicherer) Zustand	5	3	extern erkennbar, da das SAB Board nicht mehr antwortet
				Unterbrechung	3V3 Spannungsversorgung möglicherweise nicht stabil oder Spannungseinbrüche möglich / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset
				Zufällige Änderung des Wertes	3V3 Spannungsversorgung möglicherweise nicht stabil oder Spannungseinbrüche möglich / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset
	Konden-sator	C29	3V3	Kurzschluss	Spannungsabfall an 3,3V Leitung / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset
	Gesamtberechnung im Anhang								

In Tabelle 4 wird ein Teil der Analyse gezeigt. Die vollständige Analyse ist im Anhang zu finden.

3.1.9.2 Interne Spannungsüberwachung

Aufgabe: Überwachung der internen Spannung auf den Safety Board. In diesem Modul gibt es zwei Untermodule, nämlich die Spannungsüberwachung der 3,3 Volt und die Spannungsüberwachung der 1,2 Volt.

Komponenten: Widerstände, Kondensatoren,

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 80, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

In Tabelle 5 wird ein Teil der Analyse gezeigt. Die vollständige Analyse ist im Anhang zu finden.

Tabelle 5: Berechnung skizziert für die interne Spannungsüberwachung

Subsystem	Komponente	Be.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Überwachungsschaltung TPS3808G33DBVR	Überwachungsschaltung	U8	Spannungsüberwachung für 3,3V Spannung	Unterbrechung eines einzelnen Anschlusses	Im schlimmsten Fall (VDD, GND oder Reset unterbrochen) wird das Reset Signal nicht auf Low gesetzt. Im Falle der Spannungsversorgungspins ist das verhalten undefiniert (Datenblatt s. 13)	keine Erkennung der 3V3 Unterspannung möglich	4	2	nicht erkennbar	10	80
				Kurzschluss zwischen zwei benachbarten Anschlüssen	Bei Kurzschluss zwischen Pin 1 und 2 wird ein Reset Impuls ausgelöst	Spannungsfreier (sicherer) Zustand	4	2	in Software erkennbar	7	56
				"Stuck" at Fehler	Im schlimmsten Fall (Pin 1 stuck at high impedance) wird das Reset Signal nicht auf Low gesetzt	keine Erkennung der 3V3 Unterspannung möglich	5	1	nicht erkennbar	10	50
				Gesamtberechnung im Anhang							

3.1.9.3 Externe Spannungsüberwachung

Aufgabe: Überwachung der Spannungen die vom Main Board geliefert werden.

Komponenten: Fotokoppler, Widerstände, Bipolartransistoren, analoger Komparator, z-Diode,

Resultat: Für die Widerstände R13, 19, 20, 22, 25, 26, 27 beträgt die RPZ-Zahl 120, was sehr nahe am maximal erlaubten Grenzwert liegt. Daher müssen folgende Maßnahmen in Betracht gezogen werden:

- Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
- hochwertige MELF Widerstände verwenden. Alternativ können auch zwei parallele Widerstände verwendet werden.

In Tabelle 6 wird ein Teil der Analyse gezeigt. Da die externe Spannungsüberwachung keine Subsysteme besitzt, sondern nur aus einzelnen Komponenten besteht, besitzt die Tabelle eine Spalte weniger. Die vollständige Analyse ist im Anhang zu finden.

Tabelle 6: Berechnung skizziert für externe Spannungsüberwachung

Komponente	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN	Empfohlene Aktion
Fotokoppler	U11	Optokoppler für Unterspannungssignal	Unterbrechung eines einzelnen Anschlusses	12V Unterspannungserkennung wird dauerhaft ausgelöst	Unterspannungsfehler wird dauerhaft ausgelöst	2	2	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	12	
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal für Unterspannungsfehler dauerhaft Low	Unterspannungsfehler wird dauerhaft ausgelöst	2	2	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	12	
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal für Unterspannungsfehler dauerhaft High	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	2	Keine Erkennung möglich	10	80	
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Eingangs und Ausgangs	12V könnten an D3 Eingang anliegen.	Unterspannungsfehler wird nicht möglicherweise nicht erkannt. Potentieller Ausfall von D3 und Aufhebung der galvanischen Trennung	9	1	Keine Erkennung möglich	10	90	
			Gesamtberechnung im Anhang								

3.1.9.4 Digitale Eingänge

Aufgabe: Die digitalen Eingänge dienen für diverse Fehlerdiagnose und Überwachungssignale, sowie als Empfängerkanal der Kommunikation mit dem *Operational Board*.

Komponenten: Logische Gatter, Optokoppler, Widerstände

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 60, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

In Tabelle 7 wird ein Teil der Analyse gezeigt. Da die externe Spannungsüberwachung keine Subsysteme besitzt, sondern nur aus einzelnen Komponenten besteht, besitzt die Tabelle eine Spalte weniger. Die vollständige Analyse ist im Anhang zu finden.

Tabelle 7: Berechnung skizziert für digitale Eingänge

Komponent	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Optokoppler	U13D	Signal-status U_MESS S2.4	Unterbrechung eines einzelnen Anschlusses	Relais Rückesung nicht möglich	Relais Dignose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwichen zwei beleibigen eingängsseitigen Anschlüssen (LED)	Optokoppler ausser funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler ausser funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüsen des Eingangs und Ausgansg	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
		Gesamtberechnung im Anhang								

3.1.9.5 Sicherheits-CPU

Aufgabe: Die Sicherheits-CPU führt die Sicherheitsfunktionen aus und führt das Gesamtsystem bei Gefahr in den sicheren Zustand.

Komponente: Mikroprozessor der RM48Lx-Familie

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 75, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

In Tabelle 8 wird ein Teil der Analyse gezeigt. Die vollständige Analyse ist im Anhang zu finden.

Tabelle 8: Berechnung skizziert für Sicherheits-CPU

Subsystem	Bez	Komponente	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Core	U1	REL_K 102 (Pin 2)	Output-Steuerung von Relais K102 (High)	Stuck-at 0	Relais K102 wird nicht geschaltet	Spannungfreier (sicherer) Zustand	1	1	Rücklesung Diagnosesignal von Relais. HW loopback	3	3
				Stuck-at 1	Relais K102 wird geschaltet	Spannungfreier (sicherer) Zustand	5	1	Rücklesung Diagnosesignal von Relais. HW loopback	3	15
		REL_K 103 (Pin 9)	Output-Steuerung von Relais K103 (High)	Stuck-at 0	Relais K103 wird nicht geschaltet	Spannungfreier (sicherer) Zustand	1	1	Rücklesung Diagnosesignal von Relais. HW loopback	3	3
				Stuck-at 1	Relais K103 wird geschaltet	Spannungfreier (sicherer) Zustand	5	1	Rücklesung Diagnosesignal von Relais. HW loopback	3	15
		FI Error (Pin 14)	Input-Fehlerstrom	Stuck-at 0	falsche FI-Auslösung erkannt	Spannungfreier (sicherer) Zustand	1	1	Erkennbar durch Rücklesung von Signal bei FI Test	3	3

			Sensor selbsttestsignal (Low)	Stuck-at 1	Fehlerstrom nicht erkannt	unsicher Zustand	10	1	Erkennbar durch Rücklesung von Signal bei FI Test	3	30
		WD-TRG(Pin 16)	Output-Watchdog (Toggle)	Stuck-at 0	Watchdog kann nicht mehr getriggert werden	Watchdog fehlerhaft - nach Erkennung spannungfreier (sicherer) Zustand	1	1	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	2
				Stuck-at 1	Watchdog kann nicht mehr getriggert werden	Watchdog fehlerhaft - nach Erkennung spannungfreier (sicherer) Zustand	1	1	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	2
		EVM CP CONN1 (Pin 22)	Input-Erkennung der Anschluss eines Autos	Stuck-at 0	Signal kann nicht gelesen werden	Ohne korrektes EVM CP Signal werden Relais nicht freigegeben; Spannungfreier (sicherer) Zustand	1	1	Signal wird redundant eingelesen. PWM Signal muss anliegen	2	2
				Stuck-at 1	Signal kann nicht gelesen werden	Ohne korrektes EVM CP Signal werden Relais nicht freigegeben; Spannungfreier (sicherer) Zustand	1	1	Signal wird redundant eingelesen. PWM Signal muss anliegen	2	2
	Gesamtberechnung im Anhang										

3.1.9.6 Digitale Ausgänge

Aufgabe: Die digitalen Ausgänge dienen als Steuersignale, sowie als Sendekanal der Kommunikation mit dem *Operational Board*.

Komponenten: Logische Gatter, Optokoppler, Widerstände

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 60, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

In Tabelle 9 wird ein Teil der Analyse gezeigt. Da die externe Spannungsüberwachung keine Subsysteme besitzt, sondern nur aus einzelnen Komponenten besteht, besitzt die Tabelle eine Spalte weniger. Die vollständige Analyse ist im Anhang zu finden.

Tabelle 9:Berechnung skizziert für digitale Ausgänge

Komponent	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Logische Gatter AND	U5A		Unterbrechung eines einzelnen Anschlusses	Möglicher Ausfall der AND-Gatter	Relais Ansteuerung ist nicht möglich / Sicherer Zustand	1	4	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	0	8
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Kurzschluss (3V3/GND) auf dem Safety Board	Versogungspannung fällt ab / Relaisfreigabe wird entzogen	2	4	nicht erkennbar, außer durch Brownout Reset	8	64

Optokoppler	U6A	REL K103 EXT; REL K105 EXT	Unterbrechung eines einzelnen Anschlusses	Relais Ansteuerung ist nicht möglich. Signal dauerhaft Low	Relais Ansteuerung ist nicht möglich	2	2	Rücklesen der Relais Diagnosesignale	2	8
			Kurzschluss zwischen zwei beliebigen eingängsseitigen Anschlüssen (LED)	Optokoppler ausser Funktion. Signal dauerhaft Low		2	2		2	8
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler ausser funktion. Signal dauerhaft High		7	2		2	28
			Kurzschluss zwischen zwei belibigen Anschlüssen des Eingangs und Ausgangs	Möglicher Ausfall des Optokopplers / AND-Gatter möglicherweise defekt durch zu hohe Spannung am Ausgangspin (12V)		5	1		2	10
Logische Gatter AND	U5B	REL K103 EXT; REL K105 EXT	Unterbrechung eines einzelnen Anschlusses	Funktion des AND-Gatters ist nicht garantiert	Ansteuerung der Relais REL K103 und REL K105 nicht möglich	2	4	Rücklesen der Relais Diagnosesignale	2	16
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des AND-Gatters ist nicht garantiert	Ungewollte Ansteuerung der Relais REL K103 und REL K105 ist möglich	7	4		2	56
	Gesamtberechnung im Anhang									

3.1.9.7 Watchdog

Aufgabe: Überwachen und triggern der CPU

Komponente: Watchdog-Baustein

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 48, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

Tabelle 10: Komplette Betrachtung des Watchdogs

Subsyt	Komp.	Bezeichnung	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Watchdog	Monostabiler Multivibrator	DW1B	Teil des Watchdog-Timers	Unterbrechung eines einzelnen Anschlusses	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus	Watchdog fehlerhaft	8	2	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	32
				Kurzschluss zwischen zwei beliebigen Anschlüssen			8	2		2	32
				"Stuck" at Fehler			8	2		2	32
	Widerstand	RW2	Bestimmung der Zeitkonstante für den Watchdog	Unterbrechung	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Zufällige Änderung des Wertes			8	3		2	48
				Kurzschluss			8	3		2	48

	Kondensator	CW2	Bestimmung der Zeitkonstante für den Watchdog	Kurzschluss	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Unterbrechung			8	3		2	48
				Zufällige Änderung des Wertes			8	3		2	48
	Monostabiler Multivibrator	DW1A	Teil des Watchdog Timers	Unterbrechung eines einzelnen Anschlusses	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus	Watchdog fehlerhaft	8	2	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	32
				Kurzschluss zwischen zwei beliebigen Anschlüssen			8	2		2	32
				"Stuck" at Fehler			8	2		2	32
	Widerstand	RW1	Pull-Up für WD Trigger Eingang	Unterbrechung	Watchdog Timer könnte ungewollt triggern	Watchdog fehlerhaft	1	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	6
				Zufällige Änderung des Wertes	Watchdog Timer löst nicht oder möglicher-weise fehlerhaft aus (niederohmig)		8	3		2	48
				Kurzschluss	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus		8	1		2	16
	Widerstand	RW3	Bestimmung der Zeitkonstante für den Watchdog	Unterbrechung	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Zufällige Änderung des Wertes			8	3		2	48
				Kurzschluss			8	1		2	16
	Kondensator	CW1	Bestimmung der Zeitkonstante für den Watchdog	Kurzschluss	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Unterbrechung			8	3		2	48
				Zufällige Änderung des Wertes			8	3		2	48

In Tabelle 10 wird die gesamte Analyse gezeigt, diese ist aber auch vollständigkeitshalber nochmals im Anhang aufgeführt.

3.1.9.8 Relais Kontrolllogik

Aufgabe: Sichere Ansteuerung der Relais

Komponenten: Logische Gatter, Kondensatoren,

Resultat: Bei den logischen NAND-Gattern (D2A, D2D, D3A, D3C, D3D) und logischen ODER-Gattern (U15A, U15B, U15C) liegt die RPZ-Zahl zwischen 96 und 120, nahe am maximal erlaubten Grenzwert liegt. Daher müssen die folgenden Maßnahmen in Betracht gezogen werden:

- Einbauen eines Pull-up-Widerstandes an der Leitung 3V3_UV vor dem Eingang von U15A
- Einbauen eines Pull-Down-Widerstandes an der nFault-Leitung

- Einbauen eines Pull-up-Widerstandes an der 1V2_UV-Leitung vor dem Eingang von U15B
- Einbauen eines Pull-up-Widerstandes am Ausgang des OR-Gatters

Tabelle 11: Berechnung skizziert Steuerlogik

Subsystem	Komponent	Bezeichnung	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN	Empfohlene Aktion
Relais Steuerlogik	Logische Gatter NAND	D2A	Negierer für nUV_33 Signal	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	nUV_33 Fehlersignal könnte unerkannt bleiben (Pin 3 unterbrochen) / LED Ansteuerung ist nicht möglich	4	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Unterspannung durch Brown-out Reset	6	96	Pull-Up Widerstand an der 3V3_UV Leitung vor dem Eingang von U15A
				Kurzschluss zwischen zwei beliebigen Anschlüssen		nUV_33 Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4		6	96	Pull-Up Widerstand an der 3V3_UV Leitung vor dem Eingang von U15A
	Kondensator	C32	Stützkondensator	Kurzschluss	Kurzschluss auf dem Safety Board	Versorgungspannung fällt ab / Relaisfreigabe wird entzogen	2	3	nicht erkennbar, außer durch Brownout Reset	2	12	
				Unterbrechung	Funktion des NAND-Gatters ist nicht garantiert (unwahrscheinlich)	nUV_33 Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	3	nUV_33 Fehlersignal kann zusätzlich über nPORRST des Safety Controllers erkannt werden	5	60	
				Zufällige Änderung des Wertes			4	3		5	60	

In Tabelle 11 wird ein Teil der Analyse gezeigt. Die vollständige Analyse ist im Anhang zu finden.

3.1.9.9 Platinen-Stecker

Aufgabe: Stecker der Pins.

Komponente: Stecker

Resultat: Die maximale RPZ aller Ausfälle in diesem Modul beträgt 60, was unter dem kritischen Grenzwert (125) liegt. Das bedeutet, dass kein Fehlermodus der Komponenten dieses Moduls kritisch ist und daher keine Maßnahmen ergriffen werden müssen.

Tabelle 12: Berechnung skizziert Platinen-Stecker

Subsystem	Bez.	Komponente	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion
Connector	J1	VIN12 (PIN1)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkannbar
				Kurzschluss zwischen benachbarten Pins (1 / 3)	keine Auswirkung (gleiches Potential)		1	1	nicht erkannbar
		VIN12 (PIN3)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkannbar
				Kurzschluss zwischen benachbarten Pins (3 / 5)	keine Auswirkung (gleiches Potential)		1	1	nicht erkannbar
		VIN12 (PIN5)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkannbar
				Kurzschluss zwischen benachbarten Pins (5 / 7)	keine Auswirkung (gleiches Potential)		1	1	nicht erkannbar
		VIN12 (PIN7)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkannbar
				Kurzschluss zwischen benachbarten Pins (7 / 9)	keine Auswirkung (gleiches Potential)		1	1	nicht erkannbar
		VIN12 (PIN9)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkannbar
				Kurzschluss zwischen benachbarten Pins (9 / 11)	keine Auswirkung (gleiches Potential)		1	1	nicht erkannbar
		VIN12 (PIN11)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkannbar
				Kurzschluss zwischen benachbarten Pins (11 / 13)	keine Auswirkung (gleiches Potential)		1	1	nicht erkannbar

In Tabelle 12 wird ein Teil der Analyse gezeigt. Die vollständige Analyse ist im Anhang zu finden.

Fazit:

Insgesamt kann festgehalten werden, dass die Analyse ergeben hat, dass das System die geforderten Sicherheitsanforderungen erfüllt, jedoch können noch einige kleinere Verbesserungen dazu beitragen diese weiter zu erhöhen.

3.2 Voraussichtlicher Nutzen, insbesondere der Verwertbarkeit des Ergebnisses und der Erfahrungen

Intelligente und sichere Ladestationen sind ein wichtiger Bestandteil, um E-Mobilität weiter ausbreiten zu lassen. Nur wenn genügend Ladestationen vorhanden sind, werden mehr Menschen auf Elektrofahrzeuge umsteigen. Dies stellt einen wichtigen Baustein der Reduzierung de CO_2 Emissionen dar um die Klimaziele der Bundesregierung zu erreichen.

Die immer steigende elektrische Energieversorgung der künftige E-Fahrzeuge und das immer schnellere aber dennoch sichere Laden ermöglicht notwendige, zukunftsträchtige und interessante Bereiche in der Forschung und Entwicklung.

Insgesamt zeigt aber auch der Bereich der sicheren und zuverlässigen Mikrosysteme ein hohes Potential für einen breiten Markt aber auch für Forschung und Entwicklung. Anfänglich in der Luftfahrt und besonders in der Prozessindustrie geforderten Sicherheitssystemen nach Norm, werden in mehr Branchen und Bereichen neue Sicherheitsnormen eingeführt, die an die IEC 61508 angelehnt sind. Das sichere und zuverlässige verarbeiten von Werten wird in immer mehr Bereichen gefordert, sei es in der Automobilindustrie, Medizintechnik, Logistik aber auch in neuen Bereichen wie beim intelligenten, mobilen Gesundheitsmonitoring, Smart Home, Sportdiagnostik, Telemedizin, Vitalfunktions-überwachung und intelligenten Textilien.

Weiterhin dehnt sich die funktionale Sicherheit von der verarbeitenden Einheit (Steuerung, Rechner) in der Sensorik und Aktorik aus, um intelligente sichere und zuverlässige Gesamtsysteme zu erzielen.

Durch den Einsatz von funktional sicheren Schaltungen, Komponenten und Systemen aber auch deren Miniaturisierungen (Safety Chips) in unterschiedlichen Bereichen und auch der Wiederverwendung und Erweiterung sorgen letztendlich dafür, dass es zwar keine Massenprodukte aber dennoch preiswerte und gut verfügbare Komponenten werden, die in zahllosen Bereichen eingesetzt werden können.

Die unmittelbare Ergebnisverwertung erfolgte zunächst in Form von gemeinsamen Konferenzauftritten, Präsentationen sowie in der weiteren Projektakquisition, um die Industrie auf diese Forschungsarbeiten aufmerksam zu machen oder auch als künftige Investoren zu interessieren. Nach Abschluss des Projektes sollen die erzielten Forschungsergebnisse in verschiedenen Applikationsfeldern und Forschungsbereichen weiterentwickelt und verwendet werden. Auch in der Lehre und Abschlussarbeiten können solche Sicherheitsboards gebraucht werden, um Studenten weiter mit der Funktionalen Sicherheit vertraut zu machen.

3.3 Während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordenen Fortschritts auf diesem Gebiet bei anderen Stellen,

Es gibt Ladestationen unterschiedlicher Anbieter, die entweder den FI-Schalter des Hauses oder einen zusätzlichen, eingebauten FI-Schalter benutzen. Es ist nicht bekannt, dass es Ladestationen gibt, die für die Stromüberwachung explizit eine Sicherheitsschaltung verwenden. Die im Projekt angestrebte Lösung wird davon somit nicht berührt.

3.4 Erfolgte oder geplante Veröffentlichungen des Ergebnisses.

3.4.1 Akzeptierte Veröffentlichung

Functional Safety and Electric Vehicle Charging: Developing a Safe, Compact, Electronically Controlled Charging Station for EVs.

Tommi Kivelä, Marvin Sperling, Mohamed Abdelawwad, Marvin Sperling, Malte Drabesch, Michael H. Schwarz, Josef Börcösk, and Kai Furmans

7th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS). 28-30. April. 2021 Online Conference.

3.4.2 Geplante Veröffentlichung

- The IEEE PES ISGT Europe 2021 (ISGT Europe 2021), Espoo Finnland, 18-21 Oktober 2021 – Online Konferenz mit dem Thema: Smart Grids: Towards a Carbon-free Future

- The IEEE 6th International Conference on Smart and Sustainable Technologies (SpliTech), Bol und Split, 8-11. September 2021, - Online Konferenz mit den Themen: Energie, Smart Cities, e-Health, Engineering Modeling

Referenzen

[1] D. Welle, Germany aims for 1 million e-cars by 2020 | DW | 27.05.2013. [Online]. Available: https://www.dw.com/en/germany-aims-for-1-million-e-cars-by-2020/a-16841141 (accessed: Feb. 11 2021).

[2] IEA, Global EV Outlook 2020 – Analysis - IEA. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2020 (accessed: Oct. 4 2020).

[3] Neue Welten, "80 Prozent der Ladevorgänge von Elektroautos finden zuhause statt“. [Online]. Available: https://www.journalistenakademie.de/dossiers/neue-welten/elektroautos-zuhause-laden/ (accessed: Feb. 14 2021).

[4] Normgerechte Errichtung von Ladeinfrastruktur | Elektroauto Wiki | GoingElectric.de. [Online]. Available: https://www.goingelectric.de/wiki/Normgerechte-Errichtung-von-Ladeinfrastruktur/ (accessed: Feb. 14 2021)

[5] TÜVSÜD, www.tuvsud.com, E-Mobility | Alles zu Ladesäulen. [Online]. Available: https://www.tuvsud.com/de-de/indust-re/gebaeudeausruestung-info/ladesaeulen (accessed: Feb. 14 2021).

[6] Hayek A. and Börcsök J., 2016: Miniaturized Safety PLC on a Chip for Industrial Control Applications. 13th International Conference of Distributed Computing and Artificial Intelligence (DCAI16), June 01-04. Sevilla, Spain.

[7] Josef Börcsök, Miniaturized Safety Systems: A Way for Future Tasks in Safety Engineering, 2015 XXV International Conference on Information, Communication and Automation Technologies (ICAT) October 29 – October 31, 2015, Sarajevo, Bosnia and Herzegovina

[8] M. Abdelawwad, A. Hayek, A. Alsuleiman and J. Börcsök, FPGA Implementation of a Safety System-on-Chip Based on 1oo4 Architecture Using LEON3 Processor, 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 2018, pp. 231-235. doi: 10.1109/COMAPP.2018.8460288

[9] Josef Börcsök, Waldemar Müller, Eike Hahn, Michael Schwarz, and Mohamed Abdelawwad, Approach for a Safe-SoC for Cyber-physical Application according to IEC 61508. International Journal of Computers, vol. 14, 2020, doi: 10.46300/9108.2020.14.12.

[10] Larissa Gaus, Michael Schwarz and Josef Börcsök, Estimation of Optimal Safety Parameters for a Communication Channel with Required SIL 3 at runtime. 29th European Safety and Reliability Conference, (ESREL), 22 – 26 September 2019, Hannover, Germany

[11] Krini J. and Börcsök J., 2015: Contribution to reducing the critical faults in critical Software Systems Model. XXV International Conference on Information, Communication and Automation Technologies, October 29-31, 2015 Sarajevo, Bosnia & Herzegovina

[12] Schwarz M.H., Börcsök J., 2017: Digital Controller Design Using A Reliable Code Generation Framework. 3rd Workshop & Symposium Safety and Integrity Management of Operations in Harsh Environments, C-RISE3, October 18-20, 2017, St. John’s, NL, Canada.

[13] Josef Börcsök, Muhammad Ikram Hafiz, Ahmed Alsuleiman, Michael Schwarz, and Mohamed Abdelawwad, “Safe Position Detection Based on Safety System-on-Chip (SSoC) for

Wireless IoT Application," International Journal of Circuits, Systems and Signal Processing, vol. 14, 2020, doi: 10.46300/9106.2020.14.132.

[14] Sheng H., Schwarz M., Börcsök J., 2012: New Concept to Develop a Safety Sensor Network for Continuous Noninvasive Blood Pressure Monitoring. In Proceedings17th IEEE International Conference on Emerging Technologies & Factory Automation, 17-21 September 2012, Krakow, Poland, 2013, ISBN: 978-1-4673-4735-8

[15] Hayek A., Suna Y., Schreiber M., Börcsök J., 2012: FPGA-Based Wireless Sensor Network for Safety-Related Cognitive Systems. In Proceedings BIHTEL 2012, IX international Symposium on Telecomunications, IEEE Catalog Number: CFP122U-USB, 25-27 October 2012, Sarajevo, Bosnia and Herzegovina, ISBN: 978-1-4673-4874-4

[16] Product Brief von April 2011: https://www.nxp.com/docs/en/product-brief/MPC5643LPB.pdf Abruf 23.2.21

[17] TÜV Süd Zertifikat für RM48 von Februar 2016: http://www.ti.com/lit/ml/spnq004b/spnq004b.pdf Abruf 23.2.21

[18] Product Brief von November 2016: http://www.intel.com/content/dam/www/%20public/us/en/documents/product-briefs/xeon-processor-d1529-industrial-61508-certification-product-brief.pdf Abruf 24.2.17

[19] St-Microcontrollers, https://www.st.com/en/automotive-microcontrollers.html#documentation Abruf 25.2.21

[20] J. Wollert, "Wireless systems for machinery safety," in 2015 16th International Conference on Research and Education in Mechatronics (REM), 2015, pp. 88–91.

[21] J. Streib, "Wireless und funktionale Sicherheit," open automation, http://www.openautomation.de/uploads/pics/o30533zsh_safety_network.pdf. (accessed: Feb. 14 2021).

[22] SafeRTOS, https://www.highintegritysystems.com/downloads/manuals_and_datasheets/Sample_SafeRTOS_User_Manual.pdf (accessed: Feb. 14 2021).

[23] FMEA – Fehlermöglichkeits- und Einflussanalyse. (PDF) Deutsche Gesellschaft für Qualität, 2012, (accessed: Feb. 14 2021).

[24] VDA, FMEA-Handbuch: Fehler-Möglichkeits- und Einfluss-Analyse: Design-FMEA, Prozess-FMEA, FMEA-Ergänzung - Monitoring & Systemreaktion, 1st Ed. Berlin, Germany: VDA, Verband der Automobilindustrie, 2019.

[25] F. Romeike and P. Hager, "Risiko-Management in der Produktion," in Erfolgsfaktor Risiko-Management 4.0, F. Romeike and P. Hager, Eds., Wiesbaden: Springer Fachmedien Wiesbaden, 2020, pp. 297–351.

[26] VDA, FMEA-Handbuch: Fehler-Möglichkeits- und Einfluss-Analyse: Design-FMEA, Prozess-FMEA, FMEA-Ergänzung - Monitoring & Systemreaktion, 1st ed. Berlin, Germany: VDA, Verband der Automobilindustrie, 2019.

A. Spannungsversorgung

Subsystem	Komponente	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
DC-DC-WANDLER	Sicherung	F3	Schutz (800mA)	Kein Durchbrennen (Kurzschluss)	keine	Unsicherer Zustand	4	1	nicht erkennbar	10	40
				Unterbrechung	keine Versorgungs-spannung	Spannungsfreier (sicherer) Zustand	5	3	extern erkennbar, da das SAB Board nicht mehr antwortet	2	30
	Kondensator	C35	Glättungskonden-sator und Teil des Eingangsfilters für den DC/DC Wandler U4	Kurzschluss	Sicherung F3 wird ausgelöst	Spannungsfreier (sicherer) Zustand	5	3	extern erkennbar, da das SAB Board nicht mehr antwortet	2	30
				Unterbrechung	3V3 Spannungsversorgung möglicherweise nicht stabil oder Spannungseinbrüche möglich / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	5	60
				Zufällige Änderung des Wertes	3V3 Spannungsversorgung möglicherweise nicht stabil oder Spannungseinbrüche möglich / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	5	60
	Kondensator	C29	3V3	Kurzschluss	Spannungsabfall an 3,3V Leitung / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	5	60
				Unterbrechung	3V3 Spannungsversorgung möglicherweise nicht stabil oder Spannungseinbrüche möglich	Brownout Reset des Safety Controllers möglich	4	3	nicht erkennbar, außer durch Brownout Reset	5	60
				Zufällige Änderung des Wertes	3V3 Spannungsversorg-ung möglicherweise nicht stabil oder Spannungseinbrüche möglich	Brownout Reset des Safety Controllers möglich	4	3	nicht erkennbar, außer durch Brownout Reset	5	60
	Induktivität	L1	Teil des Eingangsfilters für den DC/DC Wandler U4	Unterbrechung	keine Versorgungs-spannung	Spannungsfreier (sicherer) Zustand	5	2	extern erkennbar, da das SAB Board nicht mehr antwortet	2	20
				Zufällige Änderung des Wertes	Eingangsfilter hat nicht mehr die vorgesehenen Eigenschaften (EMV)	keine Auswirkung auf die Sicherheit	1	2	nicht erkennbar	10	20
				Kurzschluss	Eingangsfilter hat nicht mehr die vorgesehenen Eigenschaften	keine Auswirkung auf die Sicherheit	1	2	nicht erkennbar	10	20

	Z-Diode	D1	Überspannungsschutz	Bruch der Verpolungs-schutz	kein Überspannungsschutz (DC/DC Wandler arbeitet bis 18V)	keine Auswirkung / Wenn Überspannung vorliegt schaltet Software nach Erkennung in sicheren Zustand	6	2	nicht erkennbar / nur bei gleichzeitiger Überspannung durch Überspannungsüberwachung erkennbar	5	60
				Kurzschluss	Sicherung F3 wird ausgelöst	Spannungsfreier (sicherer) Zustand	5	2	extern erkennbar, da das SAB Board nicht mehr antwortet	2	20
	DC-DC-WANDLER	U4	Spannungswandler (DC-DC)	Unterbrechung eines einzelnen Anschlusses	keine Versorgungs-spannung für SAB Board	Spannungsfreier (sicherer) Zustand	5	3	extern erkennbar, da das SAB Board nicht mehr antwortet	2	30
				Kurzschluss zwischen zwei beliebigen Anschlüssen	keine Versorgungs-spannung für SAB Board	Spannungsfreier (sicherer) Zustand	5	3	extern erkennbar, da das SAB Board nicht mehr antwortet	2	30
											0
Spannungs-regler TPS73701DCQR	LDO	U3	Spannungswandler für 1,2V Versorgungsspannung	Unterbrechung	1,2V Versorgungsspannung wird nicht erzeugt / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Falsche Ausgangspannung	Falsche Ausgangsspannung / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Kurzschluss	Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
	Widerstand	R1	Pull-Up Widerstand für EN Eingang von U3	Unterbrechung	1,2V Versorgungsspannung wird nicht erzeugt / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Zufällige Änderung des Wertes	geringere Strombegrenzung für EN-Eingang	keine Auswirkung	1	3	nicht erkennbar	10	30
				Kurzschluss	keine Strombegrenzung für EN-Eingang	keine Auswirkung	1	1	nicht erkennbar	10	10
	Widerstand	R2	Brückenwiderstand für FB Eingang von U3 (0R)	Unterbrechung	1,2V Versorgungsspannung wird nicht erzeugt / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Zufällige Änderung des Wertes	1,2V Versorgungsspannung wird nicht erzeugt / Brownout Reset des Safety Controllers möglich (hochohmig)	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24

				Kurzschluss	keine Auswirkung	keine Auswirkung	1	1	muss nicht erkannt werden	1	1
	Widerstand	R3	nicht bestückt	Unterbrechung	nicht bestückt	keine Auswirkung					
				Zufällige Änderung des Wertes	nicht bestückt	keine Auswirkung					
				Kurzschluss	nicht bestückt	keine Auswirkung					
	Kondensator	C25	Ausgangs-kondensator für U3	Kurzschluss	Spannungsabfall an 1,2V Leitung / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Unterbrechung	Stabilität der Ausgangsspannung nicht mehr garantiert / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Zufällige Änderung des Wertes	Stabilität der Ausgangsspannung nicht mehr garantiert / Brownout Reset des Safety Controllers möglich	Spannungsfreier (sicherer) Zustand	4	3	nicht erkennbar, außer durch Brownout Reset	2	24
				Alterung							0

B. Interne Spannungsüberwachung

Subsystem	Komponente	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Überwachungsschaltung TPS3808G33DBVR	Überwachungs-schaltung	U8	Spannungsüber-wachung für 3,3V Spannung	Unterbrechung eines einzelnen Anschlusses	Im schlimmsten Fall (VDD, GND oder Reset unterbrochen) wird das Reset Signal nicht auf Low gesetzt. Im Falle der Spannungsversorgungspins ist das Verhalten undefiniert (Datenblatt s. 13)	keine Erkennung der 3V3 Unterspannung möglich	4	2	nicht erkennbar	10	80
				Kurzschluss zwischen zwei benachbarten Anschlüssen	Bei Kurzschluss zwischen Pin 1 und 2 wird ein Reset Impuls ausgelöst	Spannungsfreier (sicherer) Zustand	4	2	in Software erkennbar	7	56
				"Stuck" at Fehler	Im schlimmsten Fall (Pin 1 stuck at high impedance) wird das Reset Signal nicht auf Low gesetzt	keine Erkennung der 3V3 Unterspannung möglich	5	1	nicht erkennbar	10	50
											0
											0
	Widerstand	R15	Pull-up Widerstand für Reset Ausgang von U8	Unterbrechung	kein Pull-Up für Reset Ausgang	Spannungsfreier (sicherer) Zustand	5	3	Rück-lesung Diagnose-signal von Relais. HW loopback	4	60
				Zufällige Änderung des Wertes	geringe Strombegrenzung für Pull-Up an Reset Ausgang (bei niederohmigen Widerstand)	keine Auswirkung	1	3	nicht erkennbar	10	30
				Kurzschluss	keine Strombegrenzung für Pull-Up an Reset Ausgang	keine Auswirkung	1	1	nicht erkennbar	10	10
	Kondensator	C30	Kondensator für das Delay Timing von U8	Kurzschluss	im Datenblatt nicht definiert / Im schlimmsten Fall wird das Reset Signal nicht auf Low gesetzt	keine Erkennung der 3,3V Unterspannung möglich	3	3	nicht erkennbar	10	90
				Unterbrechung	Änderung des Delay Timings für das Reset Signal	keine Auswirkung	1	3	nicht erkennbar	10	30
				Zufällige Änderung des Wertes	Änderung des Delay Timings für das Reset Signal	keine Auswirkung	1	3	nicht erkennbar	10	30
Überwachungsschaltung TPS3808G12DBVR	Überwachungsschaltung	U2	Spannungsüber-wachung für 1,2V Spannung	Unterbrechung eines einzelnen Anschlusses	Im schlimmsten Fall (VDD, GND oder Reset unterbrochen) wird das Reset Signal nicht auf Low gesetzt. Im Falle der Spannungsversorgungspins ist das Verhalten undefiniert (Datenblatt s. 13)	keine Erkennung der 1,2V Unterspannung möglich	4	2	nicht erkennbar	10	80
				Kurzschluss zwischen zwei beliebigen Anschlüssen	Bei Kurzschluss zwischen Pin 1 und 2 wird ein Reset Impuls ausgelöst	Spannungsfreier (sicherer) Zustand	4	2	in Software erkennbar	7	56

				"Stuck" at Fehler	Im schlimmsten Fall (Pin 1 stuck at high impedance) wird das Reset Signal nicht auf Low gesetzt	keine Erkennung der 3,3V Unterspannung möglich	5	1	nicht erkennbar	10	50
											0
											0
	Wider-stand	R5	Pull-up Widerstand für Reset Ausgang von U2	Unterbrechung	kein Pull-Up für Reset Ausgang	Spannungsfreier (sicherer) Zustand	5	3	Rück-lesung Diagnose-signal von Relais. HW Loopback	4	60
				Zufällige Änderung des Wertes	geringe Strombegrenzung für Pull-Up an Reset Ausgang (bei niederohmigen Widerstand)	keine Auswirkung	1	3	nicht erkennbar	10	30
				Kurzschluss	keine Strombegrenzung für Pull-Up an Reset Ausgang	keine Auswirkung	1	1	nicht erkennbar	10	10
	Kondens ator	C28	Kondensator für das Delay Timing von U2	Kurzschluss	im Datenblatt nicht definiert / Im schlimmsten Fall wird das Reset Signal nicht auf Low gesetzt	keine Erkennung der 1,2V Unterspannung möglich	3	3	nicht erkennbar	10	90
				Unterbrechung	Änderung des Delay Timings für das Reset Signal	keine Auswirkung?	1	3	nicht erkennbar	10	30
				Zufällige Änderung des Wertes	Änderung des Delay Timings für das Reset Signal	keine Auswirkung	1	3	nicht erkennbar	10	30

C. Externe Spannungsüberwachung

Komponente	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN	Empfohlene Aktion
Fotokoppler	U11	Optokoppler für Unterspannungssignal	Unterbrechung eines einzelnen Anschlusses	12V Unterspannungs-erkennung wird dauerhaft ausgelöst	Unterspannungs-fehler wird dauerhaft ausgelöst	2	2	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	12	
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal für Unterspannungsfehler dauerhaft Low	Unterspannungs-fehler wird dauerhaft ausgelöst	2	2	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	12	
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal für Unterspannungs-fehler dauerhaft High	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	2	Keine Erkennung möglich	10	80	
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Eingangs und Ausgangs	12V könnten an D3 Eingang anliegen.	Unterspannungsfehler wird nicht möglicherweise nicht erkannt. Potentieller Ausfall von D3 und Aufhebung der galvanischen Trennung	9	1	Keine Erkennung möglich	10	90	
Widerstand	R18	Pull-Down Widerstand für Unterspannungssignal	Unterbrechung	n24V_UV Signal Timing verändert sich / kann nicht auf Low gesetzt werden	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	3	Keine Erkennung möglich	10	120	hochwertige MELF Widerstände verwenden / in Redesign zwei parallele Widerstände verwenden
			Zufällige Änderung des Wertes	n24V_UV Signal Timing verändert sich / kann nicht auf Low gesetzt werden	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	3	Keine Erkennung möglich	10	120	hochwertige MELF Widerstände verwenden / in Redesign zwei parallele Widerstände verwenden
			Kurzschluss	n24V_UV Signal dauerhaft Low / Optokoppler könnte beschädigt werden	Unterspannungsfehler wird dauerhaft ausgelöst	2	1	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	6	

Widerstand	R12	Strombegrenzung für Diode in Optokoppler U11	Unterbrechung	Optokoppler U11 kann nicht geschaltet werden	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Optokoppler U11 kann nicht geschaltet werden (hochohmig)	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss	Optokoppler U11 könnte beim Schalten beschädigt werden	Unterspannungsfehler wird dauerhaft ausgelöst	2	1	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	6	
Bipolartransistor	V16	Teil der Unterspannungserkennung	Unterbrechung eines einzelnen Anschlusses	Optokoppler U11 kann nicht geschaltet werden	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Optokoppler U11 könnte schalten trotz Unterspannung (KS zwischen Kollektor und Emitter)	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	2	Keine Erkennung möglich	10	80	Regel-mäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Änderung der Charakteristika	Optokoppler U11 kann nicht geschaltet werden	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
Widerstand	R16	Strombegrenzung für V16	Unterbrechung	Optokoppler U11 kann nicht geschaltet werden	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	

			Zufällige Änderung des Wertes	Optokoppler U11 kann nicht geschaltet werden (hochohmig)	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss	Erhöhter Strom über V16	Kein Einfluss auf die Sicherheitsfunktionen	1	1	keine Erkennung möglich	10	10	
Widerstand	R14	Strombegrenz-ung für Referenzspan-nungsdiode U12	Unterbrechung	Referenzspannung für beide Komparatoren fällt auf 0V und Transistoren V16 und V17 werden nicht mehr geschaltet	Über- und Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Referenzspannung von U12 verändert sich (niederohmig)	Über- und Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss	U12 kann beschädigt werden (I_KA: max. 100mA) oder Referenzspannung verändert sich	Möglicher Über- oder Unterspannungsfehler wird nicht erkannt	6	1	Keine Erkennung möglich	10	60	
Analoge Komparator	N2B	Komparator für Unterspannungserkennung der externen 12V Versorgungsleitung	Unterbrechung eines einzelnen Anschlusses	Komparator N2B kann nicht auf High schalten (wenn Pin 5 offen ist)	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungsversorgung	4	2	Keine Erkennung möglich	10	80	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Komparator N2B kann nicht auf High schalten (bei Kurzschluss zwischen Pin 6 und 7)	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	2	Keine Erkennung möglich	10	80	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Änderung der Charakteristika	Komparator-Schaltschwelle könnte sich verändern	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	2	Keine Erkennung möglich	10	80	
Widerstand	R19	Teil der Hysterese-schaltung für Komparator N2B	Unterbrechung	Am nicht-invertierenden Eingang des Komparators N2B liegt keine Referenzspannung an	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	3	Keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen

			Zufällige Änderung des Wertes	Hysterese von Komparator N2B verändert sich	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	3	Keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	Hysterese von Komparator N2B verändert sich	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	1	Keine Erkennung möglich	10	40	
Widerstand	R20	Teil der Hysterese-schaltung für Komparator N2B	Unterbrechung	keine Hysterese mehr an Komparator N2B	Kein Einfluss außer möglicher Jitter an Schaltschwelle von Komparator N2B	1	3	keine Erkennung möglich	10	30	
			Zufällige Änderung des Wertes	Hysterese von Komparator N2B verändert sich	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungs-versorgung	4	3	keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	Hysterese von Komparator N2B verändert sich	Kleine Unterspannungen können nicht erkannt werden, kritische führen zu Spannungsabfall der 3V3 Spannungsversorgung	4	1	keine Erkennung möglich	10	40	
Widerstand	R13	Teil des Spannungsteilers für die Überwachung der 12V Versorgungsspannung	Unterbrechung	Eingangsspannung an Komparatoren N2A und N2B ist 0V	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Komparator-Schaltschwellen verändern sich	Spezifizierte Fensterbreite verändert sich und kleiner möglicher Über- oder Unterspannungsfehler wird nicht erkannt, kritische Über- oder Unterspannung führen zu Spannungsabfall der 3V3 Leitung oder zum Auslösen der Sicherung F3	4	3	keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüber-wachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	Komparator-Schaltschwellen verändern sich	Überspannungsfehler wird dauerhaft ausgelöst	4	1	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	12	

Widerstand	R22	Teil des Spannungsteilers für die Überwachung der 12V Versorgungsspannung	Unterbrechung	Am nicht-invertierenden Eingang des Komparators N2A liegt keine Eingangsspannung an	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Fensterbreite der beiden Komparatoren (N2A und N2B) verändert sich	Spezifizierte Fensterbreite verändert sich und kleiner möglicher Über- oder Unterspannungsfehler wird nicht erkannt, kritische Über- oder Unterspannung führen zu Spannungsabfall der 3V3 Leitung oder zum Auslösen der Sicherung F3	4	3	keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	Fensterbreite der beiden Komparatoren (N2A und N2B) verändert sich	Spezifizierte Fensterbreite verändert sich und kleiner möglicher Über- oder Unterspannungsfehler wird nicht erkannt, kritische Über- oder Unterspannung führen zu Spannungsabfall der 3V3 Leitung oder zum Auslösen der Sicherung F3	4	1	keine Erkennung möglich	10	40	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
Widerstand	R26	Teil des Spannungsteilers für die Überwachung der 12V Versorgungsspannung	Unterbrechung	Eingangsspannung an Komparatoren N2A und N2B ist 12V	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Eingangsspannung an Komparatoren N2A und N2B ist verändert sich	Spezifizierte Fensterbreite verändert sich und kleiner möglicher Über- oder Unterspannungsfehler wird nicht erkannt, kritische Über- oder Unterspannung führen zu Spannungsabfall der 3V3 Leitung oder zum Auslösen der Sicherung F3	4	3	keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	Eingangsspannung an Komparatoren N2A und N2B ist verändert sich (0V und 0.44V bei 12V Versorgung)	Unterspannungsfehler wird dauerhaft ausgelöst	2	1	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	6	

Fotokoppler	U9	Optokoppler für Überspannungssignal	Unterbrechung eines einzelnen Anschlusses	12V Überspannungserkennung wird dauerhaft ausgelöst	Überspannungsfehler wird dauerhaft ausgelöst	2	2	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	2	8	
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer funktion. Signal für Überspannungsfehler dauerhaft Low	Überspannungsfehler wird dauerhaft ausgelöst	2	2	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	2	8	
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer funktion. Signal für Überspannungsfehler dauerhaft High	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	2	Keine Erkennung möglich	10	80	
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgang	12V könnten an D3 Eingang anliegen.	Überspannungsfehler wird nicht möglicherweise nicht erkannt. Potentieller Ausfall von D3 und Aufhebung der galvanischen Trennung (gefährlich)	9	1	Keine Erkennung möglich	10	90	
Widerstand	R21	Strombegrenzung für Diode in Optokoppler U9	Unterbrechung	Optokoppler U9 kann nicht geschaltet werden	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Optokoppler U9 kann nicht geschaltet werden (hochohming)	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss	Optokoppler U9 könnte beim Schalten beschädigt werden	Überspannungsfehler wird dauerhaft ausgelöst	2	1	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	6	
Widerstand	R25	Pull-Down Widerstand für Überspannungssignal	Unterbrechung	n24V_OV Signal Timing verändert sich / kann nicht auf Low gesetzt werden	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	3	Keine Erkennung möglich	10	120	hochwertige MELF Widerstände verwenden / in Redesign zwei parallele Widerstände verwenden

			Zufällige Änderung des Wertes	n24V_OV Signal Timing verändert sich / kann nicht auf Low gesetzt werden	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	3	Keine Erkennung möglich	10	120	hochwertige MELF Widerstände verwenden / in Redesign zwei parallele Widerstände verwenden
			Kurzschluss	n24V_OV Signal dauerhaft Low / Optokoppler könnte beschädigt werden	Überspannungsfehler wird dauerhaft ausgelöst	2	1	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	6	
Bipolartransistor	V17	Teil der Unterspannungserkennung	Unterbrechung eines einzelnen Anschlusses	Optokoppler U9 kann nicht geschaltet werden	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Optokoppler U9 könnte schalten trotz Unterspannung (KS zwischen Kollektor und Emitter)	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	2	Keine Erkennung möglich	10	80	
			Kurzschluss zwischen allen Anschlüssen	Optokoppler U9 kann nicht geschaltet werden	Überspannungsfehler wird dauerhaft ausgelöst	6	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	54	
Widerstand	R24	Strombegrenzung für V17	Unterbrechung	Optokoppler U9 kann nicht geschaltet werden	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Zufällige Änderung des Wertes	Optokoppler U9 kann nicht geschaltet werden (hochohming)	Überspannungsfehler wird dauerhaft ausgelöst	2	3	Keine Erkennung möglich	10	60	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	höherer Strom über V17	Kein Einfluss auf die Sicherheitsfunktionen	1	1	keine Erkennung möglich	10	10	

Analoge Komparator	N2A	Komparator für Überspannungserkennung der externen 12V Versorgungsleitung	Unterbrechung eines einzelnen Anschlusses	Komparator N2A kann nicht auf High schalten (wenn Pin 2 offen ist)	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	2	Keine Erkennung möglich	10	80	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Komparator N2A kann nicht auf High schalten (bei Kurzschluss zwischen Pin 1 und 2)	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	2	Keine Erkennung möglich	10	80	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Änderung der Charakteristika	Komparator-Schaltschwelle könnte sich verändern	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	2	Keine Erkennung möglich	10	80	
Widerstand	R27	Teil der Hysterese-schaltung für Komparator N2A	Unterbrechung	keine Hysterese mehr an Komparator N2A	kein Einfluss außer Jitter an Schaltschwelle von Komparator N2A?	1	3	keine Erkennung möglich	10	30	
			Zufällige Änderung des Wertes	Hysterese von Komparator N2A verändert sich	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	3	keine Erkennung möglich	10	120	Regelmäßiger Test der Spannungsüberwachung durch absichtliche Überschreitung der Schaltschwellen
			Kurzschluss	Hysterese von Komparator N2A verändert sich	Kleine Überspannungen können nicht erkannt werden, kritische führen zum Auslösen der Sicherung F3	4	1	keine Erkennung möglich	10	40	
Z-Diode	U12	Erzeugt Referenzspannung (2.495V) für Komparatoren N2A und N2B	Unterbrechung eines einzelnen Anschlusses	Erzeugung der 2.495V Referenzspannung nicht möglich (12V liegt als Referenzspannung an den Komparatoren an)	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Erzeugung der 2.495V Referenzspannung nicht möglich (0V liegt als Referenzspannung an den Komparatoren an bei Kurzschluss zwischen Pin 1 und 3)	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	
			Bruch der Verpolungsschutz	Erzeugung der 2.495V Referenzspannung nicht möglich (0V liegt als Referenz-spannung an den Komparatoren an bei Kurzschluss zwischen Pin 1 u. 3)	Unterspannungsfehler wird dauerhaft ausgelöst	2	3	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	3	18	

D. Digitale Eingänge

Komp	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Optokoppler	U13D	Signalstatus U_MESS S2.4	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Eingangs und Ausgangs	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R45	Signalstatus U_MESS S2.4	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Widerstand	R49	Signalstatus U_MESS S2.4	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U14C	Signalstatus U_MESS S2.1	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low		4	2		4	32

			Kurzschluss zwischen zwei beliebigen Anschlüssen des Eingangs und Ausgangs	Core bekommt falsche U Mess. S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R46	Signalstatus U_MESS S2.1	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Widerstand	R48	Signalstatus U_MESS S2.1	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U13A	Signalstatus U_MESS S1.1	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Eingangs und Ausgangs	Core bekommt falsche U Mess. S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R57	Signalstatus U_MESS S1.1	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16

Widerstand	R63	Signalstatus U_MESS S1.1	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U13B	Signalstatus U_MESS S2.2	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R58	Signalstatus U_MESS S2.2	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Widerstand	R64	Signalstatus U_MESS S2.2	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U13C	Signalstatus U_MESS S2.3	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft High		4	2		4	32

			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R59	Signalstatus U_MESS S2.3	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Widerstand	R65	Signalstatus U_MESS S2.3	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U10D	Signalstatus U_MESS S1.4	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R60	Signalstatus U_MESS S1.4	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher	Relais Diagnose ist nicht möglich	4	1		4	16

				Ausfall des Optokopplers						
Widerstand	R66	Signalstatus U_MESS S1.4	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U14A	Signalstatus U_MESS S1.2	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft High		4	2		4	32
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R61	Signalstatus U_MESS S1.2	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Widerstand	R67	Signalstatus U_MESS S1.2	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U14B	Signalstatus U_MESS S1.3	Unterbrechung eines einzelnen Anschlusses	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	2	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	32
			Kurzschluss zwischen zwei beliebigen eingangsseitigen	Optokoppler außer Funktion. Signal		4	2		4	32

			Anschlüssen (LED)	dauerhaft High						
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low		4	2		4	32
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche U Mess S2.4 Signal (12V) (gefährlich)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R62	Signalstatus U_MESS S1.3	Unterbrechung	Relais Rücklesung nicht möglich. Signal dauerhaft Low / kein Signal	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (abhängig von der Widerstandswert)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Widerstand	R68	Signalstatus U_MESS S1.3	Unterbrechung	Relais Rücklesung nicht möglich	Relais Diagnose ist nicht möglich	4	3	Zustandswechsel beim Schalten muss erkannt werden. Andernfalls sicherer Zustand	4	48
			Zufällige Änderung des Wertes	Relais Rücklesung möglich / nicht möglich (bei niederohmig / hochohmig)	Relais Diagnose ist möglich / nicht möglich	4	3		4	48
			Kurzschluss	Relais Rücklesung vorübergehend möglich. Möglicher Ausfall des Optokopplers	Relais Diagnose ist nicht möglich	4	1		4	16
Optokoppler	U10A	Signalstatus FI_6mA	Unterbrechung eines einzelnen Anschlusses	FI 6mA Erkennung ist nicht möglich	Safety Controller kann den DC-Stromfehler (FI 6mA) nicht erkennen	4	2	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	40
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. FI 6mA Signal dauerhaft High		4	2		5	40
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. FI 6mA Signal dauerhaft Low		4	2		5	40
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche FI 6mA Signal (5V)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R10	Signalstatus FI_6mA	Unterbrechung	FI 6mA Erkennung ist nicht möglich. Signal dauerhaft Low / kein Signal	unsicher Zustand / Safety Controller kann den DC-Stromfehler nicht erkennen	4	3	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	60
			Zufällige Änderung des Wertes	FI 6mA Erkennung ist möglich / nicht möglich (abhängig von der Widerstandswert)	unsicher Zustand / Safety Controller kann den DC-Stromfehler erkennen / nicht	4	3		5	60

					erkennen					
			Kurzschluss	FI 6mA Erkennung ist vorübergehend möglich. Möglicher Ausfall des Optokopplers	unsicher Zustand / Safety Controller kann den DC-Stromfehler nicht erkennen	4	1		5	20
Widerstand	R56	Signalstatus FI_6mA	Unterbrechung	FI 6mA Erkennung ist nicht möglich. Signal dauerhaft High	unsicher Zustand / Safety Controller kann den DC-Stromfehler nicht erkennen	4	3	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	60
			Zufällige Änderung des Wertes	FI 6mA Erkennung ist nicht möglich (bei Hochohmig)		4	3		5	60
			Kurzschluss	Kein Einfluss	DC-Stromfehler Erkennung ist möglich	1	1		1	1
Optokoppler	U10B	Signalstatus FI_30mA	Unterbrechung eines einzelnen Anschlusses	FI 6mA Erkennung ist nicht möglich	Safety Controller kann den DC-Stromfehler (FI 30mA) nicht erkennen	4	2	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	40
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. FI 30mA Signal dauerhaft High		4	2		5	40
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. FI 30mA Signal dauerhaft Low		4	2		5	40
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche FI 6mA Signal (5V)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R11	Signalstatus FI_30mA	Unterbrechung	FI 30mA Erkennung ist nicht möglich. Signal dauerhaft Low / kein Signal	unsicher Zustand / Safety Controller kann den DC-Stromfehler nicht erkennen	4	3	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	60
			Zufällige Änderung des Wertes	FI 30mA Erkennung ist möglich / nicht möglich (abhängig von der Widerstandswert)	unsicher Zustand / Safety Controller kann den DC-Stromfehler erkennen / nicht erkennen	4	3		5	60
			Kurzschluss	FI 30mA Erkennung ist vorübergehend möglich. Möglicher Ausfall des Optokopplers	unsicher Zustand / Safety Controller kann den DC-Stromfehler nicht erkennen	4	1		5	20
Widerstand	R69	Signalstatus FI_30mA	Unterbrechung	FI 30mA Erkennung ist nicht möglich. Signal dauerhaft High	unsicher Zustand / Safety Controller kann den DC-Stromfehler nicht erkennen	4	3	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	60
			Zufällige Änderung des Wertes	FI 30mA Erkennung ist nicht möglich (bei Hochohmig)		4	3		5	60
			Kurzschluss	Kein Einfluss	DC-Stromfehler Erkennung ist möglich	1	1		1	1

Optokoppler	U10C	Signalstatus FI_ERROR	Unterbrechung eines einzelnen Anschlusses	FI_ERROR Erkennung ist nicht möglich	Safety Controller kann den FI_ERROR nicht erkennen	4	2	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	40
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. FI_ERROR Signal dauerhaft High		4	2		5	40
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. FI_ERROR Signal dauerhaft Low		4	2		5	40
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Core bekommt falsche FI_ERROR Signal (5V)	Möglicher Ausfall des Safety Prozessors (Überspannung)	5	1	Spannungsüberwachung und Watchdog erzwingen sicheren Zustand	1	5
Widerstand	R70	Signalstatus FI_ERROR	Unterbrechung	FI_ERROR Erkennung ist nicht möglich. Signal dauerhaft High	unsicher Zustand / Safety Controller kann den FI_ERROR nicht erkennen	4	3	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	60
			Zufällige Änderung des Wertes	FI_ERROR Erkennung ist nicht möglich (bei Hochohmig)		4	3		5	60
			Kurzschluss	Kein Einfluss	FI_ERROR Erkennung ist möglich	1	1		1	1
Widerstand	R51	Signalstatus FI_ERROR	Unterbrechung	FI_ERROR Erkennung ist nicht möglich. Signal dauerhaft Low / kein Signal	unsicher Zustand / Safety Controller kann den FI_ERROR nicht erkennen	4	3	Zustandswechsel beim Auslösen des FI_Test Signals muss erkannt werden. Andernfalls sicherer Zustand	5	60
			Zufällige Änderung des Wertes	FI_ERROR Erkennung ist möglich / nicht möglich (abhängig von der Widerstandswert)	unsicher Zustand / Safety Controller kann den FI_ERROR erkennen / nicht erkennen	4	3		5	60
			Kurzschluss	FI_ERROR Erkennung ist vorübergehend möglich. Möglicher Ausfall des Optokopplers	unsicher Zustand / Safety Controller kann den FI_ERROR nicht erkennen	4	1		5	20

E. Safety CPU

Sub	Bez.	Komponente	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Core	U1	REL_K102 (Pin 2)	Output-Steuerung von Relais K102 (High)	Stuck-at 0	Relais K102 wird nicht geschaltet	Spannungsfreier (sicherer) Zustand	1	1	Rücklesung Diagnosesignal von Relais. HW Loopback	3	3
				Stuck-at 1	Relais K102 wird geschaltet	Spannungsfreier (sicherer) Zustand	5	1	Rücklesung Diagnosesignal von Relais. HW Loopback	3	15
		REL_K103 (Pin 9)	Output-Steuerung von Relais K103 (High)	Stuck-at 0	Relais K103 wird nicht geschaltet	Spannungsfreier (sicherer) Zustand	1	1	Rücklesung Diagnosesignal von Relais. HW Loopback	3	3
				Stuck-at 1	Relais K103 wird geschaltet	Spannungsfreier (sicherer) Zustand	5	1	Rücklesung Diagnosesignal von Relais. HW Loopback	3	15
		FI Error (Pin 14)	Input-Fehlerstrom Sensor Selbsttestsignal (Low)	Stuck-at 0	falsche FI-Auslösung erkannt	Spannungsfreier (sicherer) Zustand	1	1	Erkennbar durch Rücklesung von Signal bei FI Test	3	3
				Stuck-at 1	Fehlerstrom nicht erkannt	unsicher Zustand	10	1	Erkennbar durch Rücklesung von Signal bei FI Test	3	30
		WD-TRG (Pin 16)	Output-Watchdog (Toggle)	Stuck-at 0	Watchdog kann nicht mehr getriggert werden	Watchdog fehlerhaft - nach Erkennung spannungsfreier (sicherer) Zustand	1	1	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	2
				Stuck-at 1	Watchdog kann nicht mehr getriggert werden	Watchdog fehlerhaft - nach Erkennung spannungsfreier (sicherer) Zustand	1	1	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	2
		EVM CP CONN1 (Pin 22)	Input-Erkennung der Anschluss eines Autos	Stuck-at 0	Signal kann nicht gelesen werden	Ohne korrektes EVM CP Signal werden Relais nicht freigegeben; spannungsfreier (sicherer) Zustand	1	1	Signal wird redundant eingelesen. PWM Signal muss anliegen	2	2
				Stuck-at 1	Signal kann nicht gelesen werden	Ohne korrektes EVM CP Signal werden Relais nicht freigegeben; spannungsfreier (sicherer) Zustand	1	1	Signal wird redundant eingelesen. PWM Signal muss anliegen	2	2
		WD RB (Pin 126)	Input-Rücklesung von Watchdog	Stuck-at 0	Watchdog Fehler wird nicht erkannt	Die Funktion des externen Watchdog kann nicht garantiert werden - nach Erkennung spannungsfreier (sicherer) Zustand	8	1	Testroutine für den Hardware-Watchdog	3	24
				Stuck-at 1	Watchdog Fehler wird immer erkannt	Spannungsfreier(sicherer) Zustand	1	1		5	5

		FI Test (Pin 133)	Output-Testfunktion von Fehlerstrom Sensor	Stuck-at 0	Testsignal immer geschaltet	FI-Test kann nicht durchgeführt werden	1	1	Testbar über FI-Error, FT_06mA, FI30mA	3	3
				Stuck-at 1	Testsignal immer nicht geschaltet	FI-Test kann nicht durchgeführt werden	1	1	Testbar über FI-Error, FT_06mA, FI30mA	3	3
		FI 6mA (Pin 142)	Input-Fehlerstrom Sensor 6mA (High)	Stuck-at 0	6mA Fehlerstrom nicht Erkannt	unsicher Zustand - Safety Controller kann den DC-Stromfehler nicht erkennen	3	1	Testbar über FI-Test vor- und nach dem Ladungsvorgang	3	9
				Stuck-at 1	falsche FI-Auslösung erkannt (6mA)	Spannungsfreier (sicherer) Zustand	1	1	Testbar über FI-Test vor- und nach dem Ladungsvorgang	3	3
		FI 30mA (Pin 1)	Input-Fehlerstrom Sensor 30mA (High)	Stuck-at 0	30mA Fehlerstrom nicht Erkannt	unsicher Zustand-Safety Controller kann den RMS-Stromfehler nicht erkennen	3	1	Testbar über FI-Test vor- und nach dem Ladungsvorgang	3	9
				Stuck-at 1	falsche FI-Auslösung erkannt (30mA)	Spannungsfreier (sicherer) Zustand	1	1	Testbar über FI-Test vor- und nach dem Ladungsvorgang	3	3
		U Mess S1.2 (Pin 95)	Input-Rücklesung von Relais 1 Leiter L2	Stuck-at 0	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
				Stuck-at 1	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
		U Mess S1.3 (Pin 96)	Input-Rücklesung von Relais 1 Leiter L3	Stuck-at 0	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
				Stuck-at 1	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
		U Mess S1.1 (Pin 94)	Input-Rücklesung von Relais 1 Leiter L1	Stuck-at 0	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
				Stuck-at 1	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
		U Mess S2.3 (Pin 100)	Input-Rücklesung von Relais 2 Leiter L3	Stuck-at 0	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
				Stuck-at 1	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
		U Mess S2.2 (Pin 99)	Input-Rücklesung von Relais 2 Leiter L2	Stuck-at 0	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier	3	1	Vergleich mit Sollwert beim Relaistest	3	9

						(sicherer) Zustand					
				Stuck-at 1	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
		U Mess S2.1 (Pin 98)	Input-Rücklesung von Relais 2 Leiter L1	Stuck-at 0	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
				Stuck-at 1	Relais Rücklesung ist nicht möglich	Relais Diagnose ist nicht möglich-spannungsfreier (sicherer) Zustand	3	1	Vergleich mit Sollwert beim Relaistest	3	9
		FI_Test_AC (Pin140)	Output-Fehlerinjektion für FI Stromsensor (High)	Stuck-at 0	FI-Test wird nicht ausgeführt	Nach Erkennung des fehlerhaften FI-Tests schaltet Software in den spannungsfreien (sicheren) Zustand	1	1	Testbar über FI-Test vor- und nach dem Ladungsvorgang	3	3
				Stuck-at 1	FI-Test wird nicht ausgeführt	Nach Erkennung des fehlerhaften FI-Tests schaltet Software in den spannungsfreien (sicheren) Zustand	1	1	Testbar über FI-Test vor- und nach dem Ladungsvorgang	3	3
		NPORRST (Pin46)	Input-Safety Chip Reset (Low)	Stuck-at 0	Controller wird nicht eingeschaltet	Spannungsfreier (sicherer) Zustand	1	1	Extern erkennbar	5	5
				Stuck-at 1	Ein Reset aufgrund einer Unterspannung wird nicht durchgeführt	Controller kann außerhalb der Spezifikation laufen	3	1	Erkennbar wenn Relais durch die Überwachungsschaltung nicht geschaltet werden können	2	6
		nRM48-Fault (Pin117)	Output-RM48 Fehlersignal (Low)	Stuck-at 0	Fehlersignal vom Chip ausgelöst	Spannungsfreier (sicherer) Zustand	1	1	Erkennbar durch Testauslösung von nRM48_Fault Signal	5	5
				Stuck-at 1	Internes Fehlersignal vom Chip wird nicht ausgegeben	Unsicherer Zustand	5	1	Erkennbar durch Testauslösung von nRM48_Fault Signal	5	25
		NRST (Pin116)	Externes bidirektional Reset-Signal (Nicht benutzt)	Stuck-at 0	Controller wird nicht eingeschaltet	Spannungsfreier (sicherer) Zustand	1	1	Extern erkennbar	2	2
				Stuck-at 1	Kein Einfluss	Kein Einfluss	1	1	nicht erkennbar	10	10
		OSCIN (Pin 18)	Input/Output - Oszillator Pins	Stuck-at X	Falsche Frequenz	Unsicherer Zustand	8	1	Erkennbar durch falsches Timing von Watchdog	5	40
		Kelvin_GND			Keine Frequenz						
		OSCOUT				Spannungsfreier (sicherer) Zustand	1	1	Erkennbar bei Initialisierung des Controllers	2	2

	Q1, C26, C27	Oscillator	16 Mhz Quarzoszillator für U1	Keine Frequenz	Safety-Chip startet nicht	Spannungsfreier (sicherer) Zustand	1	3	Extern erkennbar	2	6
				Falsche Frequenz	Safety-Chip ist nicht in definierten Zustand	Unsicherer Zustand	5	3	Erkennbar durch falsches Timing von Watchdog	5	75
	R4	Widerstand	Pull up Widerstand für die externe Reset Funktion	Unterbrechung	Zufälliger Interrupt bei Reset Funktion	Spannungsfreier (sicherer) Zustand	5	3	Reset-Quelle ist durch Software erkennbar	2	30
				Zufällige Änderung des Wertes	veränderte Strombegrenz-ung für nRST Signal	Kein Einfluss	1	3	nicht erkennbar	10	30
				Kurzschluss	keine Strombegrenz-ung für nRST Signal	Kein Einfluss	1	1	nicht erkennbar	10	10

F. Digitale Ausgänge

Kom.	Bez.	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Logische Gatter AND	U5A		Unterbrechung eines einzelnen Anschlusses	Möglicher Ausfall der AND-Gatter	Relais Ansteuerung ist nicht möglich / Sicherer Zustand	1	4	Fehler führt dazu, dass Relais nicht mehr geschaltet werden können und kann über die Relaisdiagnose erkannt werden.	0	8
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Kurzschluss (3V3/GND) auf dem Safety Board	Versorgungspannung fällt ab / Relaisfreigabe wird entzogen	2	4	nicht erkennbar, außer durch Brownout Reset	8	64
Optokoppler	U6A	REL K103 EXT; REL K105 EXT	Unterbrechung eines einzelnen Anschlusses	Relais Ansteuerung ist nicht möglich. Signal dauerhaft Low	Relais Ansteuerung ist nicht möglich	2	2	Rücklesen der Relais Diagnosesignale	2	8
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft Low		2	2		2	8
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft High		7	2		2	28
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Möglicher Ausfall des Optokopplers / AND-Gatter möglicherweise defekt durch zu hoher Spannung am Ausgangspin (12V)		5	1		2	10
Logische Gatter AND	U5B	REL K103 EXT; REL K105 EXT	Unterbrechung eines einzelnen Anschlusses	Funktion des AND-Gatters ist nicht garantiert	Ansteuerung der Relais REL K103 und REL K105 nicht möglich	2	4	Rücklesen der Relais Diagnosesignale	2	16
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des AND-Gatters ist nicht garantiert	Ungewollte Ansteuerung der Relais REL K103 und REL K105 ist möglich	7	4		2	56
Widerstand	R17	REL K103 EXT; REL K105 EXT	Unterbrechung	Optokoppler außer Funktion / Signal dauerhaft Low	Ansteuerung der Relais REL K103 und REL K105 nicht möglich	2	3	Rücklesen der Relais Diagnosesignale	2	12
			Zufällige Änderung des Wertes	Optokoppler außer Funktion / Signal dauerhaft Low (bei Hochohmig)		2	3		2	12
			Kurzschluss	Möglicher Ausfall des Optokopplers durch zu hoher Spannung am Eingangs-Pin (LED)		5	1		2	10
Widerstand	R23	REL K103 EXT; REL K105 EXT	Unterbrechung	Widerstand der Pull-Down Parallelschaltung wird größer	keine Auswirkung	1	3	Diagnose nicht nötig	2	6
			Zufällige Änderung des Wertes	Widerstand der Pull-Down Parallelschaltung verändert sich	keine Auswirkung	1	3	Diagnose nicht nötig	2	6
			Kurzschluss	Signal dauerhaft Low	Ansteuerung der Relais REL K103 und REL K105 nicht möglich	1	1	Rücklesen der Relais Diagnosesignale	2	2
oko pple r	U6B	REL K102 EXT; REL	Unterbrechung eines einzelnen Anschlusses	Relais Ansteuerung ist nicht möglich. Signal dauerhaft	Relais Ansteuerung ist nicht möglich	2	2	Rücklesen der Relais Diagnosesignale	2	8

		K104 EXT		Low							
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft Low		2	2		2	8
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft High		7	2		2	28
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Möglicher Ausfall des Optokopplers / AND-Gatter möglicherweise defekt durch zu hoher Spannung am Ausgangs-Pin (12V)		5	1		2	10
Logische Gatter AND	U5C	REL K102 EXT; REL K104 EXT	Unterbrechung eines einzelnen Anschlusses	Funktion des AND-Gatters ist nicht garantiert	Ansteuerung der Relais REL K102 und REL K104 nicht möglich	2	4	Rücklesen der Relais Diagnosesignale	2	16
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des AND-Gatters ist nicht garantiert	Ungewollte Ansteuerung der Relais REL K102 und REL K104 ist möglich	7	4		2	56
Widerstand	R8	REL K102 EXT; REL K104 EXT	Unterbrechung	Optokoppler außer Funktion / Signal dauerhaft Low	Ansteuerung der Relais REL K102 und REL K104 nicht möglich	2	3	Rücklesen der Relais Diagnosesignale	2	12
			Zufällige Änderung des Wertes	Optokoppler außer Funktion / Signal dauerhaft Low (bei Hochohmig)		2	3		2	12
			Kurzschluss	Möglicher Ausfall des Optokopplers durch zu hoher Spannung am Eingangs-Pin (LED)		5	1		2	10
Widerstand	R9	REL K102 EXT; REL K104 EXT	Unterbrechung	Widerstand der Pull-Down Parallelschaltung wird größer	keine Auswirkung	1	3	Diagnose nicht nötig	2	6
			Zufällige Änderung des Wertes	Widerstand der Pull-Down Parallelschaltung verändert sich	keine Auswirkung	1	3	Diagnose nicht nötig	2	6
			Kurzschluss	Signal dauerhaft Low	Ansteuerung der Relais REL K102 und REL K104 nicht möglich	2	1	Rücklesen der Relais Diagnosesignale	2	4
Optokoppler	U6C	FI Test AC EXT	Unterbrechung eines einzelnen Anschlusses	FI TEST AC Ansteuerung ist nicht möglich. Signal dauerhaft Low	Fehlerstromsimulation nicht möglich	4	2	Fehlerstromsensor löst nicht aus	3	24
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft Low	Fehlerstromsimulation nicht möglich	4	2	Fehlerstromsensor löst nicht aus	3	24
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft High	Fehlerstromsimulation wird dauerhaft ausgeführt	4	2	Fehlerstromsensor löst dauerhaft aus	3	24
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Möglicher Ausfall des Optokopplers / AND-Gatter möglicherweise defekt durch zu hoher Spannung am Ausgangspin (12V)	Fehlerstromsimulation nicht möglich	5	1	Fehlerstromsensor löst nicht aus	3	15

Logische Gatter AND	U5C	FI Test AC EXT	Unterbrechung eines einzelnen Anschlusses	Funktion des AND-Gatters ist nicht garantiert	Fehlerstromsimulation nicht möglich	4	4	Fehlerstromsensor löst nicht aus	3	48
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des AND-Gatters ist nicht garantiert	Ungewollte Fehlerstromsimulation möglich	5	4	Fehlerstromsensor löst aus, obwohl nicht geschaltet	3	60
Widerstand	R52	FI Test AC EXT	Unterbrechung	Optokoppler außer Funktion / Signal dauerhaft Low	Fehlerstromsimulation nicht möglich	2	3	Fehlerstromsensor löst nicht aus	3	18
			Zufällige Änderung des Wertes	Optokoppler außer Funktion / Signal dauerhaft Low (bei Hochohmig)		2	3		3	18
			Kurzschluss	Möglicher Ausfall des Optokopplers durch zu hoher Spannung am Eingangs-Pin (LED)		5	1		2	10
Widerstand	R54	FI Test AC EXT	Unterbrechung	Widerstand der Pull-Down Parallelschaltung wird größer	keine Auswirkung	1	3	Diagnose nicht nötig	1	3
			Zufällige Änderung des Wertes	Widerstand der Pull-Down Parallelschaltung verändert sich	keine Auswirkung	1	3	Diagnose nicht nötig	1	3
			Kurzschluss	Signal dauerhaft Low	Fehlerstromsimulation nicht möglich	2	1	Fehlerstromsensor löst nicht aus	3	6
Optokoppler	U6D	FI Test EXT	Unterbrechung eines einzelnen Anschlusses	FI TEST Ansteuerung ist nicht möglich. Signal dauerhaft High	Fehlerstromsimulation nicht möglich	4	2	Fehlerstromsensor löst nicht aus	3	24
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft High	Fehlerstromsimulation nicht möglich	4	2	Fehlerstromsensor löst nicht aus	3	24
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft Low	Fehlerstromsimulation nicht möglich (da Low Impuls zw. 30ms und 1,2s benötigt wird)	4	2	Fehlerstromsensor löst nicht aus	3	24
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Möglicher Ausfall des Optokopplers / AND-Gatter möglicherweise defekt durch zu hoher Spannung am Ausgangs-Pin	Fehlerstromsimulation nicht möglich	5	1	Fehlerstrom-Sensor löst nicht aus	3	15
Logische Gatter AND	U5D	FI Test EXT	Unterbrechung eines einzelnen Anschlusses	Funktion des AND-Gatters ist nicht garantiert	Fehlerstromsimulation nicht möglich	4	4	Fehlerstrom-Sensor löst nicht aus	3	48
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des AND-Gatters ist nicht garantiert	Ungewollte Fehlerstromsimulation möglich	5	4	Fehlerstromsensor löst aus, obwohl nicht geschaltet	3	60
Widerstand	R29	FI Test EXT	Unterbrechung	Optokoppler außer Funktion / Signal dauerhaft High	Fehlerstromsimulation nicht möglich	4	3	Fehlerstrom-Sensor löst nicht aus	3	36
			Zufällige Änderung des Wertes	Optokoppler außer Funktion / Signal dauerhaft High (bei Hochohmig)		4	3		3	36
			Kurzschluss	Möglicher Ausfall des Optokopplers durch zu hoher Spannung am Eingangs-Pin (LED)		5	1		3	15

Widerstand	R28	FI Test EXT	Unterbrechung	kein High Signal für FI Test möglich	Fehlerstromsimulation nicht möglich	4	3	Fehlerstrom-Sensor löst nicht aus	3	36
			Zufällige Änderung des Wertes	Optokoppler außer Funktion / Signal dauerhaft High (bei zu niederohmig)	Fehlerstromsimulation nicht möglich	4	3	Fehlerstromsensor löst nicht aus	3	36
			Kurzschluss	Optokoppler außer Funktion / Signal dauerhaft High (bei zu niederohmig)	Fehlerstromsimulation nicht möglich	4	1	Fehlerstromsensor löst nicht aus	3	12
Optokoppler	U18	FI TEST DC EXT	Unterbrechung eines einzelnen Anschlusses	FI TEST DC Ansteuerung ist nicht möglich. Signal dauerhaft Low	Signal nicht verbunden auf Silis Main Board	1	2	Erkennung nicht nötig	1	2
			Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen (LED)	Optokoppler außer Funktion. Signal dauerhaft Low	Signal nicht verbunden auf Silis Main Board	1	2	Erkennung nicht nötig	1	2
			Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen (Transistor)	Optokoppler außer Funktion. Signal dauerhaft High	Signal nicht verbunden auf Silis Main Board	1	2	Erkennung nicht nötig	1	2
			Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Möglicher Ausfall des Optokopplers / AND-Gatter möglicherweise defekt durch zu hoher Spannung am Ausgangspin (12V)	Signal nicht verbunden auf Silis Main Board	5	1	Erkennung nicht nötig	1	5
Logische Gatter AND	U17	FI TEST DC EXT	Unterbrechung eines einzelnen Anschlusses	Funktion des AND-Gatters ist nicht garantiert	Signal nicht verbunden auf Silis Main Board	1	1	Erkennung nicht nötig	1	1
			Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des AND-Gatters ist nicht garantiert	Signal nicht verbunden auf Silis Main Board	1	1	Erkennung nicht nötig	1	1
Widerstand	R53	FI TEST DC EXT	Unterbrechung	Optokoppler außer Funktion / Signal dauerhaft Low	Signal nicht verbunden auf Silis Main Board	3	3	Erkennung nicht nötig	1	9
			Zufällige Änderung des Wertes	Optokoppler außer Funktion / Signal dauerhaft Low (bei Hochohmig)		3	3		1	9
			Kurzschluss	Möglicher Ausfall des Optokopplers durch zu hoher Spannung am Eingangs-Pin (LED)		3	1		1	3
Widerstand	R55	FI TEST DC EXT	Unterbrechung	FI Test EXT Signal dauerhaft Low / kein Signal	Signal nicht verbunden auf Silis Main Board	1	3	Erkennung nicht nötig	1	3
			Zufällige Änderung des Wertes	FI Test EXT Ansteuerung ist möglich / nicht möglich (abhängig von Widerstandswert)	Signal nicht verbunden auf Silis Main Board	1	3	Erkennung nicht nötig	1	3
			Kurzschluss	FI Test EXT Ansteuerung ist vorübergehend möglich. Möglicher Ausfall des Optokopplers	Signal nicht verbunden auf Silis Main Board	1	1	Erkennung nicht nötig	1	1

G. Watchdog

Sub	Komponente	Bez.	Funktion	Potentielle Fehler	Lokale Auswirk	System Auswirk	S	O	Erkennungsfkt	D	RPN
Watchdog	Monostabiler Multivibrator	DW1B	Teil des Watchdog Timers	Unterbrechung eines einzelnen Anschlusses	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus	Watchdog fehlerhaft	8	2	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	32
				Kurzschluss zwischen zwei beliebigen Anschlüssen			8	2		2	32
				"Stuck" at Fehler			8	2		2	32
	Widerstand	RW2	Bestimmung der Zeitkonstante für den Watchdog	Unterbrechung	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Zufällige Änderung des Wertes			8	3		2	48
				Kurzschluss			8	3		2	48
	Kondensator	CW2	Bestimmung der Zeitkonstante für den Watchdog	Kurzschluss	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Unterbrechung			8	3		2	48
				Zufällige Änderung des Wertes			8	3		2	48
	Monostabiler Multivibrator	DW1A	Teil des Watchdog Timers	Unterbrechung eines einzelnen Anschlusses	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus	Watchdog fehlerhaft	8	2	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	32
				Kurzschluss zwischen zwei beliebigen Anschlüssen			8	2		2	32
				"Stuck" at Fehler			8	2		2	32
	Widerstand	RW1	Pull-Up für WD Trigger Eingang	Unterbrechung	Watchdog Timer könnte ungewollt triggern	Watchdog fehlerhaft	1	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	6
				Zufällige Änderung des Wertes	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus (niederohmig)		8	3		2	48
				Kurzschluss	Watchdog Timer löst nicht oder möglicherweise fehlerhaft aus		8	1		2	16
	Widerstand	RW3	Bestimmung der Zeitkonstante für den Watchdog	Unterbrechung	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Zufällige Änderung des Wertes			8	3		2	48
				Kurzschluss			8	1		2	16
	Kondensator	CW1	Bestimmung der Zeitkonstante für den Watchdog	Kurzschluss	Watchdog Timer Zykluszeit verändert sich	Watchdog fehlerhaft	8	3	Rücklesen des Watchdog Signals (Periodischer Test der WD Funktion)	2	48
				Unterbrechung			8	3		2	48
				Zufällige Änderung des Wertes			8	3		2	48

H. Relais Steuerlogik

Sub	Komp.	Bez	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN	Empfohlene Aktion
Relais Steuerlogik	Logisch. Gatter NAND	D2A	Negierer für nUV_33 Signal	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	nUV_33 Fehlersignal könnte unerkannt bleiben (Pin 3 unterbrochen) / LED Ansteuerung ist nicht möglich	4	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Unterspannung durch Brown-out Reset	6	96	Pull-Up Widerstand an der 3V3_UV Leitung vor dem Eingang von U15A
				Kurzschluss zwischen zwei beliebigen Anschlüssen		nUV_33 Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4		6	96	Pull-Up Widerstand an der 3V3_UV Leitung vor dem Eingang von U15A
	Kon-densator	C32	Stützkondensator	Kurzschluss	Kurzschluss auf dem Safety Board	Versorgungspannung fällt ab / Relaisfreigabe wird entzogen	2	3	nicht erkennbar, außer durch Brownout Reset	2	12	
				Unterbrechung	Funktion des NAND-Gatters ist nicht garantiert (unwahrscheinlich)	nUV_33 Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	3	nUV_33 Fehlersignal kann zusätzlich über nPORRST des Safety Controllers erkannt werden	5	60	
				Zufällige Änderung des Wertes			4	3		5	60	
	Logisch. Gatter NAND	D2D	nFault (Negierer für Fault Signal)	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Down Widerstand an der nFault Leitung
				Kurzschluss zwischen zwei beliebigen Anschlüssen		Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Down Widerstand an der nFault Leitung
	Logisch. Gatter NAND	D3A	Negierer für nUV_12 Signal	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	nUV 12 Fehlersignal könnte unerkannt bleiben (Pin 3 unterbrochen) / LED Ansteuerung ist nicht möglich	4	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Unterspannung durch Brown-out Reset	6	96	Pull-Up Widerstand an der 1V2_UV Leitung vor dem Eingang von U15B
				Kurzschluss zwischen zwei beliebigen Anschlüssen		nUV 12 Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Unterspannung durch Brown-out Reset	6	96	Pull-Up Widerstand an der 1V2_UV Leitung vor dem Eingang von U15B

	Kon-densator	C33	Stütz-kondensator	Kurzschluss	Kurzschluss auf dem Safety Board	Versorgungsspannung fällt ab / Relaisfreigabe wird entzogen	2	3	nicht erkennbar, außer durch Brownout Reset	2	12	
				Unterbrechung	Funktion des NAND-Gatters ist nicht garantiert (unwahrscheinlich)	nUV_12 Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	3	nicht erkennbar, außer durch Brownout Reset	5	60	
				Zufällige Änderung des Wertes			4	3		5	60	
	Logisch. Gatter NAND	D3B	nRM48 Fault	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	nRM48 Fault' Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	Hier wird der externe WD nicht mehr getriggert. Was auch zum sicheren Zustand führt	5	80	
				Kurzschluss zwischen zwei beliebigen Anschlüssen		nRM48 Fault' Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	Hier wird der externe WD nicht mehr getriggert. Was auch zum sicheren Zustand führt	5	80	
	Logisch. Gatter NAND	D3C	n24V 0V	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	n24V OV Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	nicht erkennbar, außer durch Brownout Reset	6	96	Pull-Up Widerstand an der 24V_OV Leitung vor dem Eingang von U15B
				Kurzschluss zwischen zwei beliebigen Anschlüssen		n24V OV Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	nicht erkennbar, außer durch Brownout Reset	6	96	Pull-Up Widerstand an der 24V_OV Leitung vor dem Eingang von U15B
	Logisch. Gatter NAND	D3D	n24V UV	Unterbrechung eines einzelnen Anschlusses	Funktion des NAND-Gatters ist nicht garantiert	n24V UV Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	nicht erkennbar, außer durch Brownout Reset	6	96	Pull-Up Widerstand an der 24V_UV Leitung vor dem Eingang von U15B
				Kurzschluss zwischen zwei beliebigen Anschlüssen		n24V UV Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	4	nicht erkennbar, außer durch Brownout Reset	6	96	Pull-Up Widerstand an der 24V_UV Leitung vor dem Eingang von U15B
	Logisch. Gatter OR	U15A	OR-Gatter für Fault Signal	Unterbrechung eines einzelnen Anschlusses	Funktion des OR-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Up am Ausgang des OR-Gatters
				Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des OR-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs	5	120	Pull-Up am Ausgang des OR-Gatters

									erkennbar				
	Logisch. Gatter OR	U15B	OR-Gatter für OR LINK Signal	Unterbrechung eines einzelnen Anschlusses	Funktion des OR-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Up am Ausgang des OR-Gatters
				Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des OR-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Up am Ausgang des OR-Gatters
	Logisch. Gatter OR	U15C	3V3	Unterbrechung eines einzelnen Anschlusses	Funktion des OR-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Up am Ausgang des OR-Gatters
				Kurzschluss zwischen zwei beliebigen Anschlüssen	Funktion des OR-Gatters ist nicht garantiert	Fault Fehlersignal könnte unerkannt bleiben	6	4	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	120	Pull-Up am Ausgang des OR-Gatters
	Kon-densator	C34	Stütz-kondensator	Kurzschluss	Kurzschluss auf dem Safety Board	Versorgungsspannung fällt ab / Relaisfreigabe wird entzogen	2	3	nicht erkennbar, außer durch Brownout Reset	2	12	
				Unterbrechung	Funktion des OR-Gatters ist nicht garantiert (unwahrscheinlich)	Fehlersignal könnte unerkannt bleiben / LED Ansteuerung ist nicht möglich	4	3	Falsches Fehlersignal lässt sich durch Relaistest erkennen / Einzelfehler durch LEDs erkennbar	5	60	
				Zufällige Änderung des Wertes			4	3		5	60	

I. Platinen-Stecker

Subsys	Bezeich.	Komponente	Funktion	Potentielle Fehler	Lokale Auswirkung	System Auswirkung	S	O	Erkennungsfunktion	D	RPN
Connector	J1	VIN12 (PIN1)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (1 / 3)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		VIN12 (PIN3)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (3 / 5)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		VIN12 (PIN5)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (5 / 7)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		VIN12 (PIN7)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (7 / 9)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		VIN12 (PIN9)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (9 / 11)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		VIN12 (PIN11)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (11 / 13)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		VIN12 (PIN13)	12V Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (13 / 15)	Kurzschluss der 12V Versorgungsspannung	Sicherung F3 löst aus / Software schaltet nach Erkennung in Spannungs-freien (sicheren)	6	1	nicht erkennbar, außer durch Brownout Reset	10	60

					Zustand						
		EXT_GND (PIN15)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (15 / 17)	Kurzschluss der 3V3 Versorgungsspannung	Sicherung F3 löst aus / Software schaltet nach Erkennung in spannungsfreiern (sicheren) Zustand	5	1	nicht erkennbar, außer durch Brownout Reset	10	50
		3V3_EXT (PIN17)	3V3 Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (17 / 19)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		3V3_EXT (PIN19)	3V3 Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (19 / 21)	keine Auswirkung (PIN21 nicht belegt)		1	1	nicht erkennbar	10	10
		SAB TEST GPIO1 (PIN21)	Keine Funktion	Unterbrechung einzelner Pins	keine Auswirkung (PIN21 nicht belegt)	keine Auswirkung	1	2	Nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (21 / 23)			1	1	nicht erkennbar	10	10
		SAB TEST GPIO2 (PIN23)	Keine Funktion	Unterbrechung einzelner Pins	keine Auswirkung (PIN23 / 25 nicht belegt)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (23 / 25)			1	1	nicht erkennbar	10	10
		SAB TEST GPIO3 (PIN25)	Keine Funktion	Unterbrechung einzelner Pins	keine Auswirkung (PIN 25 nicht belegt)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (25 / 27)			1	1	nicht erkennbar	10	10
		U Mess S2.3 EXT (PIN27)	Input - Diagnosesignal von Relais K105	Unterbrechung einzelner Pins	Rücklesung von Relais K105 ist nicht möglich	Diagnose von Relais K105 schlägt fehl/ Software schaltet in spannungsfreien Zustand	6	2	Erkennbar in Software durch Relaistest	3	36
				Kurzschluss zwischen benachbarten Pins (27 / 29)	Relais K105 Diagnose und EVM_CP_CONN 2 Signal werden immer gemeinsam geschaltet	Software schaltet nach Erkennung in spannungsfreien Zustand	6	1	Erkennbar in Software durch Relaistest oder Auswertung des EVM_CP_CONN Signals	2	12

		U Mess S2.4 EXT (PIN29)	Input - EVM_CP_CONN Signal der Ladeüberwachung	Unterbrechung einzelner Pins	Rücklesung von EVM_CP_CONN 2 Signal nicht möglich	Software schaltet nach Erkennung in spannungsfreien Zustand	6	2	Erkennbar durch redundantes lesen des EVM_CP_CONN Signals und erwartet PWM Frequenz von 1kHz	3	36
				Kurzschluss zwischen benachbarten Pins (29 / 31)	keine Auswirkung (PIN 31 nicht belegt)	keine Auswirkung	1	1	nicht erkennbar	10	10
		FI PWM EXT (PIN33)	Input - PWM Signalausgang von Fehlerstromsensor	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (33 / 35)	Beide SAB Eingänge FI_PWM_EXT und FI_30mA_OUT_EXT werden verbunden/ Pull-Up Widerstand für diese Leitungen auf Home Platine halbiert sich	Software schaltet nach Erkennung in sicheren Zustand	4	1	Erkennbar in Software durch falsche PWM Signale	3	12
		FI 30 mA OUT EXT (PIN35)	Input - Fehlerstromsensor 30mA Fehlerstrom Signal (High)	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (35 / 37)	Beide SAB Eingänge FI_6mA_OUT_EXT und FI_30mA_OUT_EXT werden verbunden/ Pull-Up Widerstand für diese Leitungen auf Home Platine halbiert sich	Jeder 6mA Fehlerstrom wird auch als 30mA Fehlerstrom erkannt/ System bleibt sicher	1	1	Nicht erkennbar, da 6mA Fehlerstrom nicht separat getestet werden kann	10	10
		FI 6mA OUT EXT (PIN37)	Input - Fehlerstromsensor 6mA Fehlerstrom Signal (High)	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (37 / 39)	SAB Eingang FI_6mA_OUT_EXT und Ausgang FI_TEST_EXT werden verbunden / 6mA Fehlerstromerkennung nicht möglich	Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch FI Testroutine	3	24
		FI TEST EXT [39]	Output - Signal zum an triggern des internen Selbsttests des FI Sensors	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant ausgegeben)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (39 / 41)	SAB Eingang FI_ERROR_OUT_EXT und Ausgang FI_TEST_EXT werden verbunden / Lesen des Fehlersignals des Fehlerstromsensor (FI_ERROR_OUT_EXT) nicht	Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch FI Testroutine	3	24

				möglich							
		FI ERROR OUT EXT [41]	Input - Fehlerstromsensor Systemfehler Ausgang	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant ausgegeben)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (41 / 43)	Signal FI_ERROR_OUT_EXT ist mit GND kurzgeschlossen und kann nicht gelesen werden	Software schaltet nach Erkennung in sicheren Zustand	7	1	Erkennbar in Software durch FI Testroutine	3	21
		EXT_GND (PIN43)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (43 / 45)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		EXT_GND (PIN45)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (45 / 47)	keine Auswirkung (gleiches Potential)		1	1	nicht erkennbar	10	10
		EXT_GND (PIN47)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (47 / 49)	UART_TX Signal wird mit GND kurzgeschlossen	UART Kommunikation nicht mehr möglich/ Keine Beeinträchtigung der Sicherheitsfunktion	1	1	Erkennbar in Software durch UART Test	3	3
		UART1_EXT (TX) (PIN49)	Input - Signal UART TX	Unterbrechung einzelner Pins	UART_TX Signal nicht verbunden	UART Kommunikation nicht mehr möglich/ Keine Beeinträchtigung der Sicherheitsfunktion	1	2	Erkennbar in Software durch UART Test	3	6
		FI ERROR OUT EXT (PIN2)	Input - Fehlerstromsensor Systemfehler Ausgang	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant ausgegeben)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (2 / 4)	Beide SAB Eingänge FI_6mA_OUT_EXT und FI_ERROR_OUT_EXT werden verbunden/ 6mA Fehlerstrom wird nicht erkannt, wenn FI_ERROR_OUT_EXT keinen Systemfehler des FI Sensors ausgibt	Software schaltet nach Erkennung in spannungsfreien Zustand	8	1	Erkennbar in Software durch FI Testroutine	3	24

		FI 6mA OUT EXT (PIN4)	Input - Fehlerstromsensor 6mA Fehlerstrom Signal (High)	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (4 / 6)	Beide SAB Eingänge FI_6mA_OUT_EXT und FI_PWM_EXT werden verbunden/ 6mA Fehlerstrom wird nicht erkannt, wenn der FI_PWM Ausgang des Fehlerstromsensors auf LOW ist/ PWM Signal triggert 6mA Fehler-Storm Erkennung auf SAB Board	Software schaltet nach Erkennung in spannungsfreien Zustand	8	1	Erkennbar in Software durch falsches Verhalten der beiden Fehlerstromsensor Signale	3	24
		FI PWM EXT (PIN6)	Input - PWM Signalausgang von Fehlerstromsensor	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (6 / 8)	Beide SAB Eingänge FI_30mA_OUT_EXT und FI_PWM_EXT werden verbunden/ 30mA Fehlerstrom wird nicht erkannt, wenn der FI_PWM Ausgang des Fehlerstromsensors auf LOW ist/ PWM Signal triggert 30mA Fehler-Storm Erkennung auf SAB Board	Software schaltet nach Erkennung in spannungsfreien Zustand	8	1	Erkennbar in Software durch falsches Verhalten der beiden Fehlerstromsensor Signale	3	24
		FI 30 mA OUT EXT (PIN8)	Input - Fehlerstromsensor 30mA Fehlerstrom Signal (High)	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (8 / 10)	SAB Eingang FI_30mA_OUT_EXT und Ausgang FI_TEST_EXT werden verbunden / 30mA Fehlerstromerkennung nicht möglich	Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch FI Testroutine	3	24
		FI TEST EXT (PIN10)	Output - Signal zum an triggern des internen Selbsttests des FI Sensors	Unterbrechung einzelner Pins	keine Auswirkung (Signal wird redundant eingelesen)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (10 / 12)	FI-Test EXT wird nicht ausgeführt. Signal dauerhaft Low	Software schaltet nach Erkennung in spannungsfreien Zustand	4	1	Erkennbar in Software durch FI Testroutine	3	12
		EXT_GND (PIN12)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20

				Kurzschluss zwischen benachbarten Pins (12 / 16)	FI_TEST_DC_EXT wird nicht verwendet / keine Auswirkung	keine Auswirkung	1	2	nicht erkennbar	10	20
		FI_TEST_DC_EXT (PIN16)	Output - Signal zum an triggern des externen Tests des FI Sensors (nicht mehr verwendet)	Unterbrechung einzelner Pins	FI_TEST_DC_EXT wird nicht verwendet/ keine Auswirkung	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (16 / 18)	Ausgänge für 6mA und 30mA Selbsttest werden verbunden / Pull-Down Widerstand für FI_TEST_AC_EXT Signal halbiert sich	keine Auswirkung da DC (6mA) Test nicht verwendet wird	1	1	nicht erkennbar	10	10
		FI_TEST_AC_EXT (PIN18)	Output - Signal zum an triggern des externen Tests des FI Sensors (nicht mehr verwendet)	Unterbrechung einzelner Pins	Externer Test des FI Sensors kann nicht durchgeführt werden	Software schaltet nach Erkennung in sicheren Zustand	4	2	Erkennbar in Software durch FI Testroutine	3	24
				Kurzschluss zwischen benachbarten Pins (18 / 20)	Kurzschluss der 12V Versorgungsspannung / Optokoppler U6 kann beschädigt werden und ausfallen	Externer Test des FI Sensors kann nicht durchgeführt werden/ Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch FI Testroutine	3	24
		EXT_GND (PIN20)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar		0
				Kurzschluss zwischen benachbarten Pins (20 / 22)	S1.4_EXT wird nicht verwendet / keine Auswirkung	keine Auswirkung	1	2	nicht erkennbar	10	20
		U Mess S1.4_EXT (PIN22)	Input - wird nicht mehr verwendet	Unterbrechung einzelner Pins	S1.4_EXT wird nicht verwendet / keine Auswirkung	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (22 / 24)	S1.4_EXT wird nicht verwendet / keine Auswirkung	keine Auswirkung	1	2	nicht erkennbar	10	20
		Rel K102_EXT (PIN24)	Output - Ansteuerung von Relais K102	Unterbrechung einzelner Pins	Ansteuerung von Relais K102 nicht möglich	Ausfall ist nicht gefährlich und Software schaltet nach Erkennung in sicheren Zustand	4	2	Erkennbar in Software durch Relaisdiagnose	3	24
				Kurzschluss zwischen benachbarten Pins (24 / 26)	SAB Eingang U_Mess_S1.1_EXT und Ausgang Rel_K102_EXT werden verbunden / Optokoppler U6B wird überbrückt und Relais K102 und K104 werden geschaltet / Rel_K102_EXT wird über Optokoppler OKT1.1 (auf	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24

					Home Board) auf GND gezogen, wenn das Relais geschaltet ist						
		U Mess S1.1_EXT (PIN26)	Input -Rücklesung der Diagnose von Relais K102 an Leitung L1	Unterbrechung einzelner Pins	Relais K102 Rücklesung ist nicht möglich	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	2	Erkennbar in Software durch Relaistest	3	48
				Kurzschluss zwischen benachbarten Pins (26 / 28)	Die beiden Diagnosesignale (U_Mess_S1.1_EXT und U_Mess_S2.2_EXT) werden immer gemeinsam ausgelöst	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24
		U Mess S2.2_EXT (PIN28)	Input -Rücklesung der Diagnose von Relais K105 an Leitung L2	Unterbrechung einzelner Pins	Relais K105 Rücklesung ist nicht möglich	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	2	Erkennbar in Software durch Relaistest	3	48
				Kurzschluss zwischen benachbarten Pins (28 / 30)	SAB Eingang U_Mess_S2.2_EXT und Ausgang Rel_K103_EXT werden verbunden / Optokoppler U6A wird überbrückt und Relais K103 und K105 werden geschaltet / Rel_K105_EXT wird über Optokoppler OKT2.2 (auf Home Board) auf GND gezogen, wenn das Relais geschaltet ist	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24
		Rel K103_EXT (PIN30)	Output - Ansteuerung von Relais K103	Unterbrechung einzelner Pins	Ansteuerung von Relais K103 nicht möglich	Ausfall ist nicht gefährlich und Software schaltet nach Erkennung in sicheren Zustand	4	2	Erkennbar in Software durch Relaisdiagnose	3	24
				Kurzschluss zwischen benachbarten Pins (30 / 32)	SAB Eingang U_Mess_S1.2_EXT und Ausgang Rel_K103_EXT werden verbunden / Optokoppler U6A wird überbrückt und Relais K103 und K105 werden geschaltet / Rel_K103_EXT wird über Optokoppler OKT1.2 (auf Home Board) auf GND gezogen, wenn das Relais geschaltet ist	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24

		U Mess S1.2_EXT (PIN32)	Input -Rücklesung der Diagnose von Relais K104 an Leitung L2	Unterbrechung einzelner Pins	Relais K104 Rücklesung ist nicht möglich	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	2	Erkennbar in Software durch Relaistest	3	48
				Kurzschluss zwischen benachbarten Pins (32 / 34)	Relaisdiagnosesignal löst dauerhaft aus, da U_Mess_S1.2_EXT auf GND gezogen wird	Software schaltet nach Erkennung in sicheren Zustand	4	1	Erkennbar in Software durch falsches Relaisdiagnosesignal	3	12
		EXT_GND (PIN34)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (34 / 36)	Ansteuerung von Relais K104 nicht möglich, da REL_K104_EXT auf GND gezogen wird	Fehler führt zu spannungsfreiem Relais / Software schaltet nach Erkennung in sicheren Zustand	4	1	Erkennbar in Software durch Relaistest	3	12
		Rel K104_EXT (PIN36)	Output - Ansteuerung von Relais K104	Unterbrechung einzelner Pins	Ansteuerung von Relais K104 nicht möglich	Ausfall ist nicht gefährlich und Software schaltet nach Erkennung in sicheren Zustand	4	2	Erkennbar in Software durch Relaisdiagnose	3	24
				Kurzschluss zwischen benachbarten Pins (36 / 38)	SAB Eingang U_Mess_S1.3_EXT und Ausgang Rel_K104_EXT werden verbunden / Optokoppler U6B wird überbrückt und Relais K102 und K104 werden geschaltet / Rel_K104_EXT wird über Optokoppler OKT1.3 (auf Home Board) auf GND gezogen, wenn das Relais geschaltet ist	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24
		U Mess S1.3_EXT (PIN38)	Input -Rücklesung der Diagnose von Relais K104 an Leitung L3	Unterbrechung einzelner Pins	Relais K104 Rücklesung ist nicht möglich	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	2	Erkennbar in Software durch Relaistest	3	48
				Kurzschluss zwischen benachbarten Pins (38 / 40)	SAB Eingang U_Mess_S1.3_EXT und Ausgang Rel_K105_EXT werden verbunden / Optokoppler U6A wird überbrückt und Relais K103 und K105 werden geschaltet / Rel_K105_EXT wird über Optokoppler OKT1.3 (auf Home Board) auf GND gezogen, wenn das Relais	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24

					geschaltet ist						
		Rel K105_EXT (PIN40)	Output - Ansteuerung von Relais K105	Unterbrechung einzelner Pins	Ansteuerung von Relais K105 nicht möglich	Ausfall ist nicht gefährlich und Software schaltet nach Erkennung in sicheren Zustand	4	2	Erkennbar in Software durch Relaisdiagnose	3	24
				Kurzschluss zwischen benachbarten Pins (40 / 42)	SAB Eingang U_Mess_S1.3_EXT und Ausgang Rel_K105_EXT werden verbunden / Optokoppler U6A wird überbrückt und Relais K103 und K105 werden geschaltet / Rel_K105_EXT wird über Optokoppler OKT1.3 (auf Home Board) auf GND gezogen, wenn das Relais geschaltet ist	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	1	Erkennbar in Software durch Relaisdiagnose	3	24
		U Mess S2.1_EXT (PIN42)	Input -Rücklesung der Diagnose von Relais K103 an Leitung L1	Unterbrechung einzelner Pins	Relais K103 Rücklesung ist nicht möglich	Unsicherer Zustand / Software schaltet nach Erkennung in sicheren Zustand	8	2	Erkennbar in Software durch Relaistest	3	48
				Kurzschluss zwischen benachbarten Pins (42 / 44)	Relaisdiagnosesignal löst dauerhaft aus, da U_Mess_S2.1_EXT auf GND gezogen wird	Software schaltet nach Erkennung in sicheren Zustand	4	1	Erkennbar in Software durch falsches Relaisdiagnosesignal	3	12
		EXT_GND (PIN44)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (44 / 46)	keine Auswirkung (gleiches Potential)	keine Auswirkung	1	1	nicht erkennbar	10	10
		EXT_GND (PIN46)	GND Versorgungsspannung Eingang	Unterbrechung einzelner Pins	keine Auswirkung (redundante Versorgungspins)	keine Auswirkung	1	2	nicht erkennbar	10	20
				Kurzschluss zwischen benachbarten Pins (46 / 48)	Rücklesung von EVM_CP_CONN Signal nicht möglich, da Signal auf GND liegt	Software schaltet nach Erkennung in sicheren Zustand	6	1	Erkennbar durch redundantes lesen des EVM_CP_CONN Signals und erwartete PWM Frequenz von 1kHz	2	12
		EVM CP CONN_EXT (PIN48)	Input - EVM_CP_CONN Signal der Ladeüberwachung	Unterbrechung einzelner Pins	Rücklesung von EVM_CP_CONN Signal nicht möglich	Software schaltet nach Erkennung in sicheren Zustand	6	2	Erkennbar durch redundantes lesen des EVM_CP_CONN Signals und erwartete PWM Frequenz von 1kHz	2	24
				Kurzschluss zwischen benachbarten Pins (48 / 50)	Rücklesung von EVM_CP_CONN Signal nicht möglich / UART Kommunikation nicht möglich	UART Kommunikation nicht mehr möglich/ Keine Beeinträchtigung der Sicherheits-funktion	2	1	Erkennbar durch redundantes lesen des EVM_CP_CONN Signals und erwartete PWM Frequenz von 1kHz/ Erkennbar in Software durch UART Test	2	4

		UART1_EXT (RX) (PIN50)	OUTPUT - Signal UART RX	Unterbrechung einzelner Pins	UART_RX Signal nicht verbunden	UART Kommunikation nicht mehr möglich/ Keine Beeinträchtigung der Sicherheitsfunktion	1	2	Erkennbar in Software durch UART Test	3	6