

FAT-Schriftenreihe 402

EMV-Nachweis der Störfestigkeit auf Komponenten-
und Systemebene für FailOp ab Level 3 im Hinblick auf
die Funktionssicherheit



EMV-Nachweis der Störfestigkeit auf Komponenten- und Systemebene für FailOp ab Level 3 im Hinblick auf die Funktionssicherheit

- Erster und zweiter Projektteil -

Forschungsstellen

Prof. Dr.-Ing. Matthias Richter

Forschungs- und Transferzentrum e.V.

an der Westsächsischen Hochschule Zwickau

Kornmarkt 5

08056 Zwickau

Silvain Jewoh Zekeyo

SANEON GmbH

Carl-Zeiss-Ring 14

85737 Ismaning b. München

Autoren

Dr. Bernd Körber, FTZ

Matthias Trebeck, FTZ

Sami Moslih, Saneon

Silvain Jewoh Zekeyo, Saneon

Das Forschungsprojekt wurde mit Mitteln der Forschungsvereinigung Automobiltechnik e.V. (FAT) gefördert.

Inhalt

1.	Abkürzungsverzeichnis	6
2.	Vorwort	7
3.	Einleitung.....	7
4.	Funktionale Sicherheit im Automobilbereich.....	8
4.1.	Einführung in die ISO 26262	8
4.2.	Vorgehen nach ISO 26262.....	9
4.2.1.	Produktentwicklung in der Konzeptphase	9
4.2.2.	Produktentwicklung auf Systemebene	11
4.2.3.	Produktentwicklung auf Hardwareebene	12
4.2.4.	Produktentwicklung auf Softwareebene	12
4.2.5.	Produktion, Betrieb, Service und Außerbetriebnahme	12
4.2.6.	Verifikation & Validierung und Testphase	13
5.	Funktionale Sicherheit und Prüfverfahren	14
5.1.	Anforderungen in der ISO 26262	14
5.1.1.	Bedeutung von Tests in ISO 26262.....	14
5.1.2.	Empfohlene Testabdeckung nach ISO 26262.....	15
5.2.	EMV und funktionale Sicherheit	16
5.2.1.	Qualitative und quantitative Sicherheitsanalysen in Bezug zu EMV.....	17
5.2.2.	Der Beta-Faktor als Sicherheitsmetrik	17
5.3.	Betrachtung der elektromagnetischen Phänomene.....	18
5.4.	EMV im Automobilbereich – eine langjährige Entwicklung.....	19
5.5.	EMV-Störfestigkeitsprüfverfahren und die Anforderungen an die funktionale Sicherheit.	19
5.6.	Fehler bei EMV-Prüfungen aus Sicht der funktionalen Sicherheit.....	21
5.7.	Prüfphilosophie für sicherheitsbezogene Systeme und EUT	22
5.8.	Sicherstellung der EMV-Vorgaben für die funktionale Sicherheit	23
5.9.	Welchen EMV-Bedrohungen könnten die Geräte vorhersehbar ausgesetzt sein?	23
5.9.1.	ISO 11452-2 Gestrahlte Störfestigkeit - Antennenmessverfahren	24
5.9.2.	ISO 11452-4 Stromzange (BCI)	25
5.9.3.	ISO 7637-2 Störungen auf Versorgungsleitungen.....	25
5.9.4.	ISO 7637-3 Impulsförmige Störungen auf anderen als Versorgungsleitungen.....	26
5.9.5.	ISO 10605 Elektrostatische Entladungen (ESD).....	27
5.10.	Bewertung von Prüfungen unter Berücksichtigung der funktionalen Sicherheit.....	28
5.10.1.	Messunsicherheiten von EMV-Prüfungen	28
5.10.2.	Folgen der Störfestigkeits-Bedrohungen	30
5.10.3.	Auswirkungen auf die Sicherstellung der funktionalen Sicherheit	31

5.10.4.	Methode zur Ermittlung des statistisch notwendigen Stichprobenumfanges	33
5.10.5.	Zusammenhang von FIT und Prüfpegel.....	34
5.10.6.	Erforderliche Maßnahmen für Integrität der funktionalen Sicherheit	36
5.10.7.	Zusammenfassung von EMV-Prüfungen unter Berücksichtigung der funktionalen Sicherheit	36
5.10.8.	Welche Unterlagen sind erforderlich, um das Vorgehen nachzuweisen?	37
5.10.9.	Bewertung von Störfestigkeitsprüfungen	38
5.11.	Offene Punkte	39
6.	Der Demonstrator	41
6.1.	Beschreibung des Demonstrators.....	41
6.2.	SerDes-Datenübertragung	42
7.	Eingesetzte Kommunikationssysteme.....	45
7.1.	SerDes Kanal A – Eigenschaften zur Einhaltung der Anforderungen der funktionalen Sicherheit.....	45
7.1.1.	SerDes Kanal A – Sicherheitsmechanismen	45
7.1.2.	Anwendung der Diagnosefunktionen für die Systemauslegung.....	46
7.1.3.	Zusammenfassung ASIL-Konformität:.....	47
7.2.	SerDes Kanal B – Eigenschaften zur Einhaltung der Anforderungen der funktionalen Sicherheit.....	47
7.2.1.	SerDes Kanal B – Sicherheitsmechanismen	47
7.2.2.	Umsetzung von Sicherheitsmechanismen	48
7.3.	Diagnosefunktionen und Fehlererkennung	49
7.3.1.	Failure Injection Tests	50
7.4.	Fehler in Kommunikationssystemen.....	51
7.5.	Umsetzung im Projekt.....	52
8.	Funktionale Sicherheitsanalyse des Demonstrators	54
8.1.	Definition des ITEM.....	54
8.2.	Gefahrenanalyse und Risikobewertung (HARA)	55
8.3.	Fehlerbaumanalyse (FTA)	57
8.4.	Demonstrator (System) – FSC Funktionales Sicherheitskonzept.....	58
8.5.	Demonstrator (System) – TSC Technisches Sicherheitskonzept.....	58
8.6.	Demonstrator (System) – FMEA Fehlermöglichkeits- und -Einflussanalyse.....	59
8.7.	Demonstrator (System) – FMEDA Fehlermöglichkeits-, Diagnose- und Einflussanalyse.....	60
8.8.	Demonstrator (System) – TTR Technische Testanforderungen.....	60
8.9.	Demonstrator (System) – Rückverfolgbarkeit der Elemente der Sicherheitsanalyse	62
8.10.	Demonstrator (System) – Qualitative Analyse.....	62
8.11.	Demonstrator (System) – Zusammenfassung Sicherheitsanalyse.....	64

9.	EMV-Prüfungen am Demonstrator	65
9.1.	Allgemeine Betrachtungen	65
9.2.	Softwareumsetzung der Kanalauswahl.....	65
9.3.	Prüfkriterien	66
9.4.	Prüfverfahren.....	69
9.5.	Testlevel für Prüfverfahren	69
9.6.	Demonstratorsystem als Prüfling	70
9.7.	EMV-Prüfungen.....	70
9.7.1.	ISO 11452-2 Antennenmethode – Prüfaufbauten	70
9.7.2.	ISO 11452-2 Antennenmethode – Ergebnisse	74
9.7.3.	ISO 11452-4 BCI-Methode – Prüfaufbauten	77
9.7.4.	ISO 11452-4 BCI-Methode – Ergebnisse	81
9.7.5.	ISO 7637-3 – Impulsförmige Störgrößen – Prüfaufbauten	82
9.7.6.	ISO 7637-3 – Leitungsgebundene Störungen – Ergebnisse.....	83
9.7.7.	ISO 10605 elektrostatische Entladungen – Prüfaufbauten.....	84
9.7.8.	ISO 10605 elektrostatische Entladungen – Ergebnisse	87
10.	Zusammenfassung.....	89
11.	Anhang zu Messunsicherheiten	94
12.	Quellen	108

1. Abkürzungsverzeichnis

ADAS	Advanced Driver Assistance System
AM	Amplitudenmodulation
ASIL	Automotive Safety Integrity Level
CCA	Common Cause Analysis
CSI-2	MIPI Camera Serial Interface – Schnittstelle Bildsensor - Prozessor
CW	Continuous Wave
DS	Defined State
ECU	Electronic Control Unit
EMV	Elektromagnetische Verträglichkeit
ESD	Elektrostatistische Entladung
EUT	Device Under Test – Prüfling
E/E	Elektrisch/Elektronisch
FIT	Fault in Time
FailOp	Fail-operational, fehlertolerant
FMEA	Fehlermöglichkeits- und Auswirkungsanalyse
FMEDA	Fehlermöglichkeits-, Auswirkungs- und Diagnoseanalyse
FSC	Funktionales Sicherheitskonzept
FTA	Fehlerbaumanalyse
FuSi	Funktionale Sicherheit
GPIO	General Purpose Input / Output
HARA	Hazard and Risk Analysis
I2C	Inter-Integrated Circuit - Datenbus
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OEM	Original Equipment Manufacturer
PHY	IC für die physikalische Schnittstelle der Datenübertragung
PM	Pulsmodulation
SerDes	Serializer-Deserializer, Übertragungstechnologie
TSC	Technisches Sicherheitskonzept
UART	Universal Asynchronous Receiver/Transmitter – Datenschnittstelle

2. Vorwort

Assistenzsysteme übernehmen immer mehr Funktionen im Fahrzeug. Damit werden die Fahrer entlastet und Gefahrensituationen vermieden. Das automatisierte Fahren ist nach SAE J3016 in fünf Stufen eingeteilt. Für Fahrerassistenzsysteme ab Level 3 entfällt der Fahrer als Rückfallebene bis zu einer definierten Übernahmezeit im Falle einer Fehlfunktion. Damit müssen diese Systeme immer einen Zustand haben, der ein kontrolliertes Verhalten (fail-operational) des Fahrzeuges bis zum Fahrereingriff ermöglicht. Die Absicherung dieses Verhaltens liegt in der Verantwortung der Fahrzeughersteller. Die technischen Systeme müssen entsprechend ausgelegt sein. Ist der Fahrereingriff im Fehlerfall gewährleistet, reicht für die elektronischen Assistenten ein Fail-Safe-Verhalten. Damit wird der Fahrer informiert und die Unterstützung deaktiviert. Der bisherige Testumfang in der Fahrzeugentwicklung richtet sich im Prinzip an diesen Systemen aus.

Fail-operational Systeme müssen fehlertolerant sein. Damit ergeben sich Herausforderungen im Bereich der Konzeption und für die Validierung der Systeme. Dazu müssen im Bereich der Entwicklung alle Arbeiten in den Kontext der funktionalen Sicherheit gestellt werden. Die Anforderungen und die Vorgehensweisen dafür sind für den Straßenfahrzeugbereich in der Norm ISO 26262 [1] festgelegt. Ziel ist, das immer verbleibende Restrisiko auf ein hinnehmbares, niedriges Maß abzusenken.

Daraus ergeben sich Fragestellungen. Müssen die Sicherheitsaktivitäten für solche Systeme insbesondere im Bereich der elektromagnetischen Verträglichkeit angepasst und erweitert werden? Und können diese möglichen Erweiterungen praktikabel umgesetzt werden?

3. Einleitung

Die Funktion von elektrischen und elektronischen sicherheitsrelevanten Systemen darf durch äußere Einwirkungen nicht in einer Weise beeinflusst werden, dass dies zu einem unannehmbaren Schadensrisiko für Personen und/oder die Umwelt führt. Eine akzeptable Störfestigkeitsschwelle gegenüber elektromagnetischen Störgrößen ist daher notwendig. Die Gefahrenanalyse und Risikobewertung (HARA) muss daher auch die elektromagnetische Umgebung der Systeme mit in Betracht ziehen.

Die Einordnung der EMV-Absicherung in die normativen Anforderungen zur funktionalen Sicherheit erfolgt in dieser Arbeit am Beispiel eines Frontkamarasystems. Es erfolgt die Bewertung auf Steuergeräteebene nach Vorgaben der funktionalen Sicherheit. Neben den notwendigen Untersuchungen nach der ISO 26262:

- Gefahrenanalyse und Risikobewertung (Hazard Analysis and Risk Assessment, HARA),
- Fehlerbaumanalyse (Fault Tree Analysis, FTA),
- Funktionelles Sicherheitskonzept (Functional Safety Concept, FSC),
- Technisches Sicherheitskonzept (Technical Safety Concept, TSC),
- Berechnung der Fehlermetriken

wurde der Fokus auf die daraus resultierenden Anforderungen im Bereich der Prüfungen gerichtet. Die vorliegende Arbeit untersucht, ob der bisherige Testansatz im Bereich der EMV-Prüfungen für solche Systeme ausreichend ist.

4. Funktionale Sicherheit im Automobilbereich

4.1. Einführung in die ISO 26262

ISO 26262 ist eine internationale Norm für funktionale Sicherheit in der Automobilindustrie. Sie bietet Richtlinien und Anforderungen für die Entwicklung sicherheitskritischer Automobilsysteme, mit dem Ziel, das Risiko systematischer und zufälliger Ausfälle während des gesamten Entwicklungszyklus von Automobilprodukten zu minimieren.

Diese Norm umfasst die gesamte Automobilwertschöpfungskette, vom Konzept bis zur Produktion, und behandelt Aspekte wie Management, Entwicklung, Produktion, Betrieb, Wartung und Stilllegung. Die Einhaltung von ISO 26262 stellt sicher, dass Sicherheitsrisiken, die mit elektrischen und elektronischen Systemen in Fahrzeugen verbunden sind, angemessen identifiziert, analysiert und gemindert werden, um letztendlich die Sicherheit der Verkehrsteilnehmer und die Zuverlässigkeit der Automobilsysteme zu verbessern.

Die ISO 26262 ist die Überarbeitung von IEC 61508, um den spezifischen Anforderungen des Anwendungsbereichs von elektrischen und/oder elektronischen Systemen in Straßenfahrzeugen zu entsprechen.

Diese Anpassung gilt für alle Aktivitäten während des Sicherheitslebenszyklus sicherheitsrelevanter Systeme, die aus elektrischen, elektronischen und Softwarekomponenten bestehen.

Sicherheit ist eine der Schlüsselfragen der zukünftigen Automobilentwicklung. Neue Funktionalitäten, nicht nur in Bereichen wie Fahrerassistenz, Antrieb, Fahrzeugdynamikregelung sowie aktive und passive Sicherheitssysteme, berühren zunehmend das Gebiet des Systemsicherheitsingenieurwesens. Die Entwicklung und Integration dieser Funktionalitäten werden die Anforderungen an Entwicklungsprozesse erhöhen und den Nachweis notwendig machen, dass alle vernünftigen Systemsicherheitsziele erfüllt sind.

Mit dem Trend zunehmender technologischer Komplexität, Softwareanteilen und mechatronischer Umsetzung gibt es zunehmende Risiken durch systematische Ausfälle und zufällige Hardwareausfälle. ISO 26262 enthält Anleitungen, um diese Risiken zu vermeiden, indem geeignete Anforderungen und Prozesse bereitgestellt werden.

ISO 26262 befasst sich mit der funktionalen Sicherheit von E/E-Systemen und bietet einen Rahmen, innerhalb dessen sicherheitsrelevante Systeme auf Basis anderer Technologien betrachtet werden können. Die ISO 26262:

- stellt einen Automobil-Sicherheitslebenszyklus bereit (Management, Entwicklung, Produktion, Betrieb, Service, Stilllegung) und unterstützt die Anpassung der erforderlichen Aktivitäten während dieser Lebenszyklusphasen;
- bietet einen automobilspezifischen risikobasierten Ansatz zur Bestimmung von Integritätsstufen (Automotive Safety Integrity Levels – ASIL);
- verwendet ASILs, um anwendbare Anforderungen von ISO 26262 festzulegen, um unangemessene Restrisiken zu vermeiden;
- stellt Anforderungen an Validierungs- und Bestätigungsmaßnahmen bereit, um ein ausreichendes und akzeptables Sicherheitsniveau zu gewährleisten;
- stellt Anforderungen an die Beziehungen zu Lieferanten.

Die funktionale Sicherheit wird durch den Entwicklungsprozess (einschließlich Aktivitäten wie Anforderungsspezifikation, Design, Implementierung, Integration, Verifikation, Validierung und Konfiguration), die Produktions- und Serviceprozesse sowie durch die Managementprozesse beeinflusst.

4.2. Vorgehen nach ISO 26262

Die ISO-26262-Reihe von Normen legt Anforderungen hinsichtlich bestimmter Phasen und Teilphasen des Sicherheitslebenszyklus fest, umfasst aber auch Anforderungen, die auf mehrere oder alle Phasen des Sicherheitslebenszyklus zutreffen, wie z. B. die Anforderungen für das Management der funktionalen Sicherheit.

Die wichtigsten Aufgaben des Sicherheitsmanagements bestehen darin, die Aktivitäten im Zusammenhang mit der funktionalen Sicherheit zu planen, zu koordinieren und zu verfolgen. Diese Managementaufgaben gelten für alle Phasen des Sicherheitslebenszyklus.

Der V-Zyklus, auch als V-Modell bekannt, ist ein grundlegendes Rahmenwerk innerhalb der ISO-26262-Norm für die Entwicklung sicherheitskritischer Automobilsysteme. Er skizziert einen systematischen Ansatz für den Entwicklungsprozess und betont die Bedeutung der Integration von Sicherheitsaspekten in jeder Phase des Produktlebenszyklus. Das V-förmige Diagramm stellt den sequenziellen Fortschritt der Aktivitäten dar, beginnend mit der Definition der Systemanforderungen auf der linken Seite, über das detaillierte Design und die Implementierung bis hin zu Tests und Verifikation auf der rechten Seite.

Abbildung 1 zeigt eine Aufschlüsselung der wichtigsten Phasen und Sicherheitsanalyseaktivitäten innerhalb des V-Zyklus:

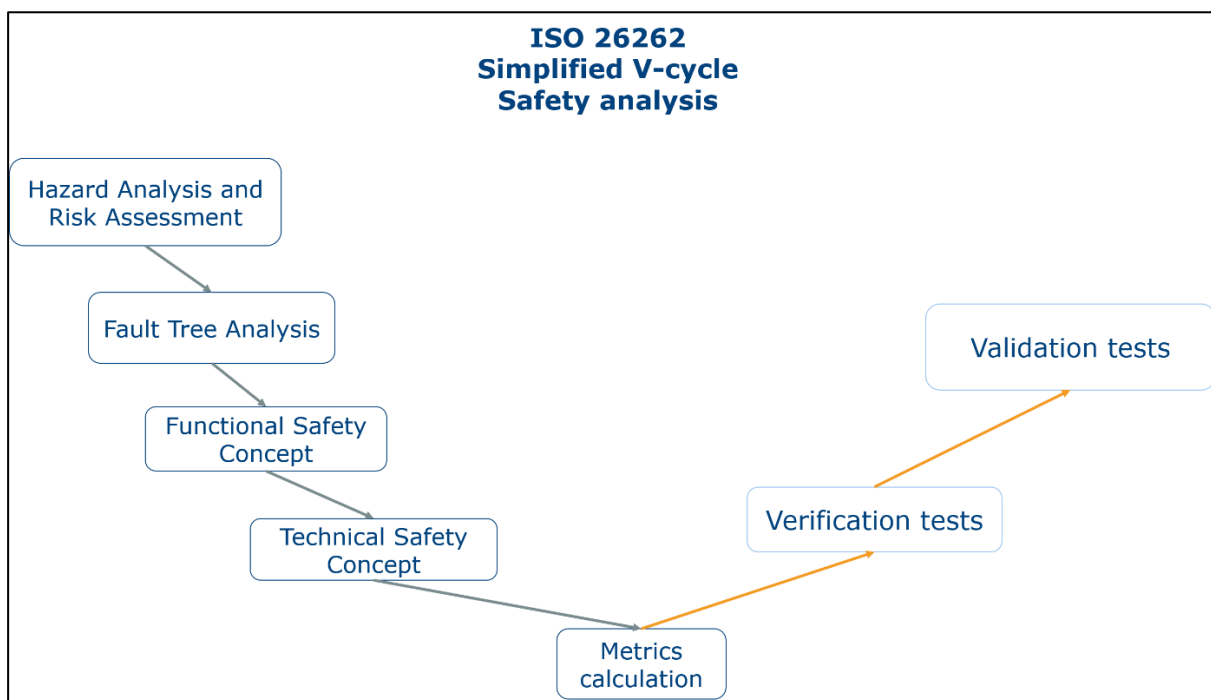


Abbildung 1 Vereinfachtes ISO 26262 V-Diagramm

4.2.1. Produktentwicklung in der Konzeptphase

Definition des ITEM

Das ITEM bezeichnet das Entwicklungsobjekt (Abbildung 2). Für das Projekt ist es das Front-Kamera-Demonstratorsystem. Die initiiierende Aufgabe des Sicherheitslebenszyklus besteht darin, eine Beschreibung des Entwicklungsobjekts hinsichtlich seiner Funktionalität, Schnittstellen, Umgebungsbedingungen, rechtlichen Anforderungen, bekannter Gefahren usw. zu entwickeln. Der Umfang des Items und seiner Schnittstellen sowie Annahmen bezüglich anderer Elemente, der Randbedingungen oder externer Maßnahmen werden festgelegt (siehe ISO 26262-3:2018, Klausel 5).

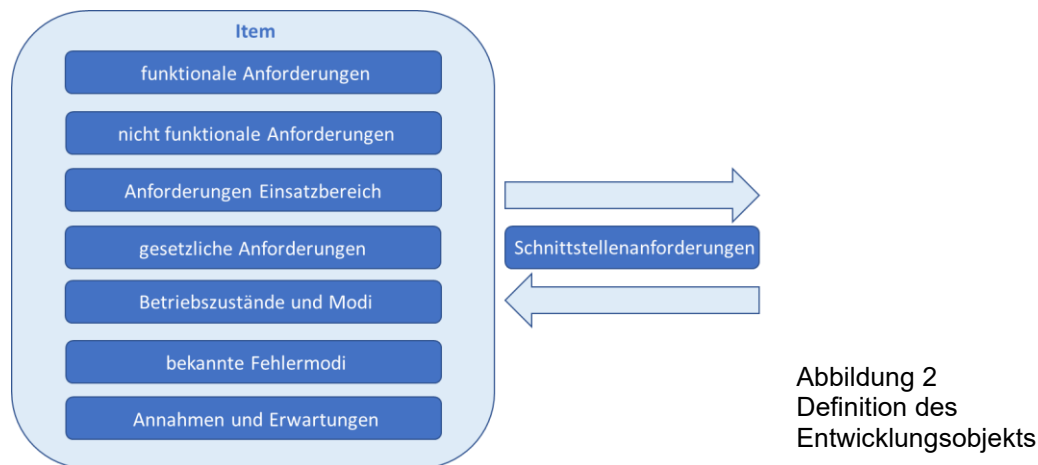


Abbildung 2
Definition des
Entwicklungsobjekts

Gefahrenanalyse und Risikobewertung

Die Gefahrenanalyse und Risikobewertung erfolgt gemäß ISO 26262-3:2018, Klausel 6. Zunächst schätzt die Gefahrenanalyse und Risikobewertung die Wahrscheinlichkeit der Exposition, die Kontrollierbarkeit und die Schwere der gefährlichen Ereignisse im Hinblick auf den Gegenstand ein. Zusammen bestimmen diese Parameter die ASILs der gefährlichen Ereignisse. Anschließend legt die Gefahrenanalyse und Risikobewertung die Sicherheitsziele für den Gegenstand fest, wobei die Sicherheitsziele die Sicherheitsanforderungen auf höchster Ebene für den Gegenstand darstellen. Die für die gefährlichen Ereignisse ermittelten ASILs werden den entsprechenden Sicherheitszielen zugeordnet. Die Annahmen bezüglich menschlichen Verhaltens, einschließlich Kontrollierbarkeit und menschlicher Reaktion, in der Gefahrenanalyse und Risikobewertung, dem funktionalen Sicherheitskonzept und dem technischen Sicherheitskonzept sowie die für die ASIL-Klassifizierung relevanten technischen Annahmen werden validiert (siehe ISO 26262-3:2018, Klausel 6, ISO 26262-3:2018, Klausel 7 und ISO 26262-4:2018, Klausel 8). Während der anschließenden Phasen und Teilphasen werden detaillierte Sicherheitsanforderungen aus den Sicherheitszielen abgeleitet. Eine Sicherheitsanforderung erbt die ASIL des entsprechenden Sicherheitsziels oder erhält die ASIL nach der Dekomposition im Fall der Anwendung von Anforderungsreduktion bezüglich ASIL-Anpassung (siehe ISO 26262-9:2018, Klausel 5) durch z.B. Redundanz.

Fehlerbaumanalyse

Die Fehlerbaumanalyse ist eine systematische, deduktive Methode, die verwendet wird, um die potenziellen Ursachen von Systemausfällen zu identifizieren.

Ein Fehlerbaum ist ein deduktives Logikmodell, das mit einem unerwünschten Hauptereignis an der Spitze erstellt wird. Von diesem aus erfolgen logische Verknüpfen bis zu den möglichen Fehlerursachen. Die FTA beantwortet die Frage "Wie kann etwas passieren?" Sie wird in Risiko-, Zuverlässigkeits- und Sicherheitsbewertungen eingesetzt. Die Methode ist gut geeignet, um Fehlermodi innerhalb komplexer E/E-Systeme zu adressieren. Die FTA kann die Bedeutung dieser Fehlermodi aus verschiedenen Perspektiven wie Kosten, Zuverlässigkeit und Sicherheit bestimmen. Eine Fehlerbaumanalyse des Demonstrators wird als Beispiel aufgeführt.

Funktionales Sicherheitskonzept

Basierend auf den Sicherheitszielen wird ein funktionales Sicherheitskonzept entwickelt (siehe ISO 26262-3:2018, Klausel 7), wobei die vorläufigen architektonischen Annahmen berücksichtigt werden. Das funktionale Sicherheitskonzept wird entwickelt, indem funktionale Sicherheitsanforderungen aus den Sicherheitszielen abgeleitet und diese funktionellen Sicherheitsanforderungen den Elementen des Gegenstands zugeordnet werden. Eine Methode zur Realisierung dieser Ableitung ist die FTA.

Die Ausgabe aus dem FSC und TSC ist eine Liste von funktionalen und technischen Sicherheitsanforderungen mit ASIL-Level und zugehörigen EMV-Tests.

4.2.2. Produktentwicklung auf Systemebene

Nachdem das funktionale Sicherheitskonzept festgelegt ist, wird der Gegenstand auf Systemebene entwickelt, wie in ISO 26262-4 angegeben. Der Systementwicklungsprozess basiert auf dem Konzept eines V-Modells mit der Spezifikation der technischen Sicherheitsanforderungen, der Systemarchitektur, dem Systemdesign und der Implementierung auf der linken Seite und der Integration, Verifikation und der Sicherheitsvalidierung auf der rechten Seite.

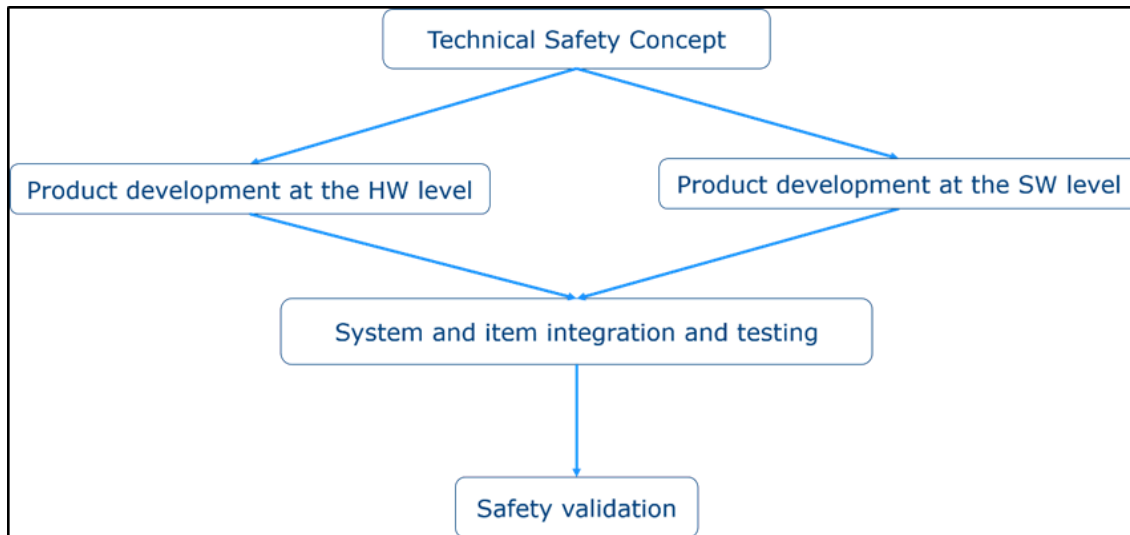


Abbildung 3 Modell der Entwicklung eines sicherheitsrelevanten Elements

Die Systementwicklung umfasst Sicherheitsvalidierungsaufgaben für Aktivitäten, die innerhalb anderer Sicherheitslebenszyklusphasen auftreten, einschließlich:

- Die technischen Annahmen, die für die ASIL-Klassifizierung relevant sind.
- Die Validierung der Annahmen über menschliches Verhalten, einschließlich Kontrollierbarkeit und menschlicher Reaktion.
- Die Validierung der Aspekte des funktionalen Sicherheitskonzepts, die von anderen Technologien implementiert werden.
- Die Validierung der Annahmen über die Wirksamkeit und die Leistung externer Maßnahmen.

Technisches Sicherheitskonzept (TSC)

Das funktionale Sicherheitskonzept und das technische Sicherheitskonzept sind ähnlich. Während das funktionale Sicherheitskonzept einen Überblick über das System und dessen Anforderungen gibt, geht das technische Sicherheitskonzept ins Detail. So könnte das funktionale Sicherheitskonzept eine allgemeine Anforderung definieren, während das technische Sicherheitskonzept erläutert, wie diese in der konkreten Implementierung umgesetzt wird.

Technische Sicherheitskonzepte werden oft in ein technisches Sicherheitskonzept auf Systemebene und ein technisches Sicherheitskonzept auf Subsystemebene unterteilt. Eine elektronische Steuereinheit könnte zum Beispiel ihr eigenes technisches Sicherheitskonzept haben.

Es folgt eine Verdeutlichung der oben genannten Konzepte: Das funktionale Sicherheitskonzept ist implementierungsunabhängig und berücksichtigt nur die funktionale Architekturebene. Die technischen Sicherheitskonzepte berücksichtigen die Implementierungsebene eines Systems.

Die Hardware-Software-Schnittstelle wird in dieser Phase spezifiziert. Die Schnittstellen zwischen Hardware und Software werden während der Hardware- und Softwareentwicklung aktualisiert.

4.2.3. Produktentwicklung auf Hardwareebene

Basierend auf der Systemspezifikation wird die Hardware entwickelt (siehe ISO 26262-5). Der Hardwareentwicklungsprozess basiert auf dem Konzept eines V-Modells mit der Spezifikation der Hardwareanforderungen und dem Hardware-Design sowie der Implementierung auf der linken Seite und der Hardwareintegration und -verifikation auf der rechten Seite.

ISO 26262-5:2018 gibt einen Überblick über die Teilphasen der Hardwareentwicklung.

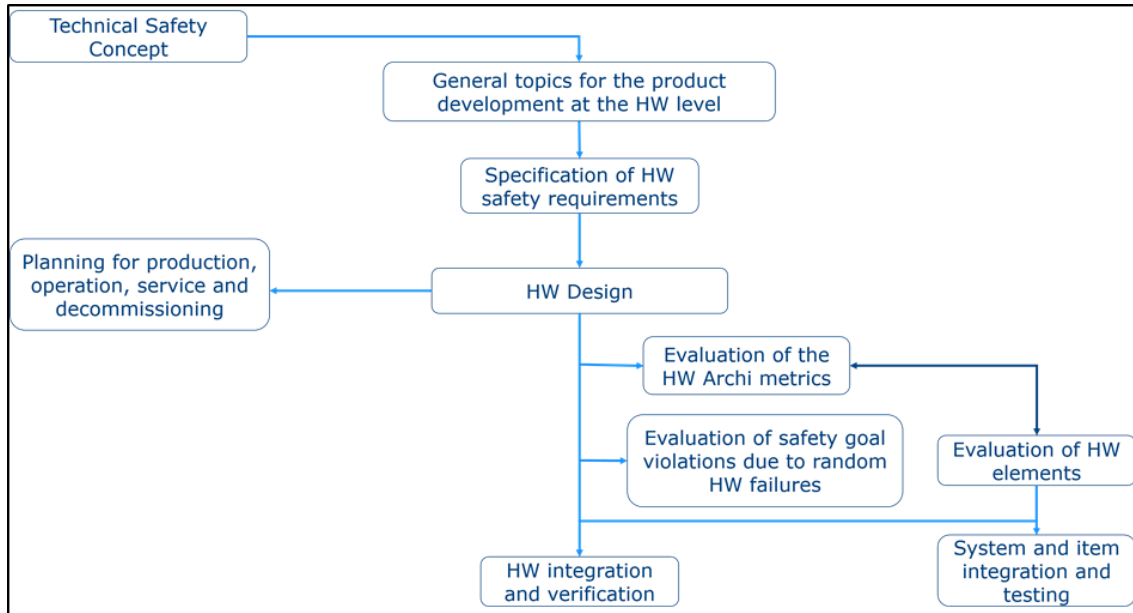


Abbildung 4 Teilphasen der Hardwareentwicklung

4.2.4. Produktentwicklung auf Softwareebene

Basierend auf der Systemspezifikation wird die Software entwickelt (siehe ISO 26262-6). Der Softwareentwicklungsprozess basiert auf dem Konzept eines V-Modells mit der Spezifikation der Softwareanforderungen und dem Softwarearchitekturentwurf sowie der Implementierung auf der linken Seite und der Softwareintegration und -verifikation auf der rechten Seite.

ISO 26262-6:2018 gibt einen Überblick über die Teilphasen der Softwareentwicklung.

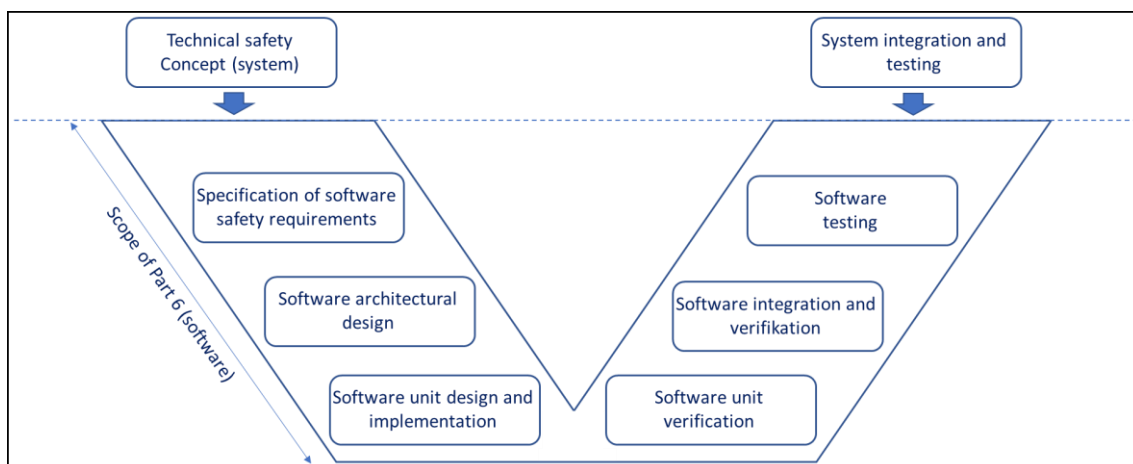


Abbildung 5 Teilphasen der Softwareentwicklung

4.2.5. Produktion, Betrieb, Service und Außerbetriebnahme

Die Planung dieser Phase (siehe ISO 26262-7:2018, Klausel 5) und die Spezifikation der zugehörigen Anforderungen beginnt während der Produktentwicklung auf Systemebene (siehe ISO 26262-4) und findet parallel zur System-, Hardware- und Softwareentwicklung statt. Eine solche Planung kann durch den Austausch von Informationen oder Anforderungen

ermöglicht werden, z. B. sicherheitsrelevante besondere Merkmale oder Anforderungen, die die Produktionsfähigkeit des Produkts verbessern.

Diese Phase behandelt die Prozesse, Mittel und Anweisungen, um die funktionale Sicherheit in Bezug auf Produktion, Betrieb, Service und Außerbetriebnahme des Gegenstands oder Elements sicherzustellen. Die sicherheitsrelevanten besonderen Merkmale sowie die Entwicklung und Verwaltung von Anweisungen für die Produktion, den Betrieb, den Service (Wartung und Reparatur) und die Außerbetriebnahme des Gegenstands oder Elements (siehe ISO 26262-7:2018, Klauseln 6 und 7) werden berücksichtigt.

4.2.6. Verifikation & Validierung und Testphase

Tests im Rahmen von ISO 26262 sind wesentlich, um sicherzustellen, dass Systeme die Sicherheitsanforderungen erfüllen. Zusammenfassend sind ISO 26262-Tests entscheidend dafür, dass Automobilsysteme strenge Sicherheitsstandards erfüllen. Sie umfassen eine Vielzahl von Testmethoden, von Modultests bis hin zu systemweiten Validierungen, die alle darauf abzielen sicherzustellen, dass die Sicherheitsanforderungen während des gesamten Lebenszyklus des Systems erfüllt werden. Dieser gründliche Testprozess trägt dazu bei, dass Automobilsysteme sicher, zuverlässig und konform mit internationalen Sicherheitsstandards sind.

Die Testumfänge sind im folgenden Abschnitt detailliert aufgeführt.

5. Funktionale Sicherheit und Prüfverfahren

5.1. Anforderungen in der ISO 26262

5.1.1. Bedeutung von Tests in ISO 26262

Tests im Rahmen von ISO 26262 sind wesentlich, um sicherzustellen, dass Systeme die Sicherheitsanforderungen erfüllen.

- Sicherstellung der Einhaltung von Sicherheitsvorschriften: Tests stellen sicher, dass die Systeme, die in ISO 26262 spezifizierten Sicherheitsanforderungen erfüllen.
- Risikominderung: Identifizierung und Minderung potenzieller Sicherheitsrisiken frühzeitig im Entwicklungsprozess.
- Verbesserung der Zuverlässigkeit: Gewährleisten, dass das System zuverlässig ist und unter allen definierten Bedingungen sicher funktioniert.
- Einhalten von Vorschriften: Erfüllung von Branchenstandards und -vorschriften, um rechtliche und finanzielle Sanktionen zu vermeiden.
- Verbesserung der Qualität: Verbesserung der Gesamtqualität der Automobilsysteme durch rigoroses Testen jeder Komponente und des Systems als Ganzes.

Nachfolgend sind die Arten von Prüfungen aufgeführt, die in der ISO 26262 enthalten sind.

1. Verifikationstests

Verifikationstests werden durchgeführt, um sicherzustellen, dass das System oder die Komponente die spezifizierten Anforderungen und Designspezifikationen erfüllt. Dazu gehören.

- Anforderungsverifikation: Sicherstellen, dass die Systemanforderungen korrekt spezifiziert sind und die beabsichtigten Sicherheitsziele erfüllen.
- Designverifikation: Überprüfen, dass das Design die spezifizierten Anforderungen korrekt umsetzt.
- Code-Verifikation: Gewährleisten, dass die Implementierung (Quellcode) den Designspezifikationen und Anforderungen korrekt entspricht.
- Integrationsverifikation: Überprüfen, ob integrierte Komponenten wie beabsichtigt zusammenarbeiten.

2. Validierungstests

Validierungstests werden durchgeführt, um sicherzustellen, dass das entwickelte System die Bedürfnisse und Erwartungen der Endbenutzer und Stakeholder erfüllt, insbesondere in Bezug auf die Sicherheit.

- Funktionale Validierung: Sicherstellen, dass das System seine beabsichtigten Funktionen in realen Szenarien ausführt.
- Sicherheitsvalidierung: Bestätigen, dass das System alle Sicherheitsanforderungen erfüllt und unter allen definierten Bedingungen sicher funktioniert.

3. Modultests

Modultests konzentrieren sich auf die kleinsten testbaren Teile des Systems, in der Regel einzelne Funktionen oder Methoden innerhalb des Codes.

- White-Box-Tests: Testen der internen Strukturen oder Arbeitsweisen einer Anwendung im Gegensatz zu ihrer Funktionalität (z. B. Codeabdeckungstests).
- Black-Box-Tests: Testen der Funktionalität, ohne die internen Arbeitsweisen der Anwendung zu kennen.

4. Integrationstests

Integrationstests überprüfen, ob mehrere Systemkomponenten oder Systeme korrekt zusammenarbeiten.

- Schnittstellentests: Sicherstellung, dass Schnittstellen zwischen Komponenten ordnungsgemäß definiert und implementiert sind.
- Systemintegrationstests: Überprüfung der Integration aller Komponenten innerhalb des Systems.

5. Systemtests

Systemtests bewerten das vollständige und integrierte System, um sicherzustellen, dass es alle spezifizierten Anforderungen erfüllt.

- Funktionale Tests: Überprüfen, ob das System sich gemäß den funktionalen Anforderungen verhält.
- Nicht-funktionale Tests: Kontrollieren von Aspekten wie Leistung, Benutzerfreundlichkeit, Zuverlässigkeit usw.

6. Fehlerinjektionstests

Fehlerinjektionstests bewerten das Verhalten des Systems unter Fehlerbedingungen, um sicherzustellen, dass es Fehler sicher behandeln kann.

- Hardware-Fehlerinjektion: Einführung von Fehlern in die Hardware, um die Reaktion des Systems zu testen.
- Software-Fehlerinjektion: Gezieltes Verursachen von Softwarefehlern, um die Robustheit und Fehlerbehandlung des Systems zu überprüfen.

5.1.2. Empfohlene Testabdeckung nach ISO 26262

Die generellen Anforderungen an die funktionale Sicherheit werden bereits in der Konzeptphase der ISO 26262 definiert. In der Produktentwicklung werden diese genauer spezifiziert und später durch Integrations-, Verifikations- und Validierungstest abgesichert. Umfangreiche Prüfungen sind auf Hardware, Software und Systemebene vorgesehen. Die nachfolgenden Tabellen sind der ISO 26262 entnommen. Diejenigen Schritte, die mit „++“ bzw. highly recommended gekennzeichnet sind, sind als verpflichtend für das entsprechende ASIL anzusehen. Die weiteren Abstufungen sind recommended (+) und neutral (o).

Methoden	ASIL			
	A	B	C	D
Requirement-based test	++	++	++	++
Fault injection test	+	+	++	++
Back-to-back test	o	+	+	++

Tabelle 1 Prüfung der korrekten Umsetzung von funktionalen Sicherheits- und technischen Sicherheitsanforderungen auf Systemebene nach ISO26262 [1]

Methoden	ASIL			
	A	B	C	D
Back-to-back test	o	+	+	++
Fault injection test	+	+	++	++
Performance test	o	+	+	++
Error guessing test	+	+	++	++
Test derived from field experience	o	+	++	++

Tabelle 2 Prüfung der korrekten funktionalen Funktionsweise, Genauigkeit und Zeitsteuerung von Sicherheitsmechanismen auf Systemebene nach ISO26262 [1]

Methoden	ASIL			
	A	B	C	D
Resource usage test	o	+	+	++
Stress test	o	+	+	++
Test for interference resistance and robustness under certain environmental conditions*	++	++	++	++

Tabelle 3 Prüfung des Robustheitsniveaus auf Systemebene nach ISO26262 [1]

Tests zur Widerstandsfähigkeit gegen Störungen und Robustheit unter bestimmten Umweltbedingungen sind spezielle Fälle von Belastungstests. Diese umfassen auch EMV- und ESD-Tests (Tabelle 3). Diese werden für alle ASIL empfohlen.

Für die Hardware ist der Prüfumfang in Teil 5 der ISO 26262 aufgeführt und mit Empfehlungen zur Anwendung für verschiedene ASIL versehen (Tabelle 4). Es werden hier 10 verschiedene Prüfmethode aufgeführt, EMV und ESD-Tests sind ein Teil davon. Die EMV ist nur einer der zahlreichen Aspekte, die bei der von der ISO 26262 geforderten effektiven Sicherheitsanalyse zu berücksichtigen sind. EMV-Untersuchungen werden für alle ASIL empfohlen. Bei der Integration und Verifizierung der Hardware wird die Haltbarkeit und Robustheit der Hardware gegenüber Umwelt- und Betriebsstressfaktoren geprüft.

Methoden	ASIL			
	A	B	C	D
Environmental testing with basic functional verification	++	++	++	++
Expanded functional test	o	+	+	++
Statistical test	o	o	+	++
Worst case test	o	o	o	+
Over limit test	+	+	+	+
Mechanical test	++	++	++	++
Accelerated life test	+	+	++	++
Mechanical Endurance test	++	++	++	++
EMC and ESD test	++	++	++	++
Chemical test	++	++	++	++

Tabelle 4 Hardware-Integrationstests zur Überprüfung von Haltbarkeit, Robustheit und Betrieb unter Beanspruchungen nach ISO26262 [1]

5.2. EMV und funktionale Sicherheit

ISO 26262 Part	Referenzierung von EMV/ESD in den einzelnen Teiler der ISO 26262
3	Impact analysis
4	Test goals and test methods
5	Specification of hardware safety requirements
5	Hardware architectural design and hardware detailed design
5	Hardware integration and testing
5	Example calculation of hardware architectural metrics
9	Analysis of dependent failures
9	Relationship between faults, errors and failures
10	Example of dependent failure analysis

Tabelle 5 Auflistung von EMV und ESD für die funktionale Sicherheit in der ISO 26262 [1]

Auf EMV oder ESD wird in 5 Teilen der ISO 26262 Bezug genommen, wie in Tabelle 5 dargestellt. Wie ersichtlich ist, wird neben den Prüfanforderungen von Teil 5 ein großer Schwerpunkt auf Fehler gelegt, die durch EMV bei der Analyse und dem Design der Hardwarekomponente verursacht werden können. Bei der Entwicklung von Serienfahrzeugen

ist das frühzeitige Erkennen und Korrigieren von Problemen entscheidend für kostengünstige und zuverlässige Produkte.

Ein weiterer wichtiger Aspekt des Sicherheitsassessments ist die in Teil 3 beschriebene Gefahrenanalyse und Risikobewertung (HARA). Die EMV wird in diesem Abschnitt nicht ausdrücklich erwähnt, da sie nur eine von vielen möglichen Ursachen für eine Gefährdung ist. Diese potenziellen Ursachen für eine Gefährdung sollten in einer Analyse ermittelt werden und EMV-Auswirkungen einschließen.

Es ist nicht möglich, einen ASIL nur einem Störfestigkeitsereignis zuzuordnen. Im Gegensatz zu vielen klassischen EMV-Anforderungen, bei denen Grenzwertlinien mit Pass/Fail-Kriterien festgelegt sind, gibt es keinen definierten Schwellenwert, der bestimmt, ob die Anforderungen nach der ISO 26262 erfüllt sind. Es ist Aufgabe der zuständigen Sicherheits-, System- und EMV-Experten, alle EMV-bedingten Gefahrenursachen in die Gefahrenanalyse und Risikobewertung einzubeziehen.

5.2.1. Qualitative und quantitative Sicherheitsanalysen in Bezug zu EMV

Im Rahmen von ISO 26262 sind zwei Ansätze für die Durchführung von Sicherheitsanalysen (FMEDA / FMEA) möglich, die quantitative und die qualitative Analyse. Die FMEA geht induktiv vor, also von der Ursache zum Fehler. Die Fragestellung bei der Durchführung lautet daher, welche sicherheitsrelevanten Folgen aus einem Fehler entstehen können.

Quantitative Sicherheitsanalyse:

- Beinhaltet die Verwendung von numerischen Daten und Metriken zur Bewertung der Sicherheit.
- Nutzt Techniken wie probabilistische Risikobewertung, Fehlerbaumanalyse (FTA), Fehlermöglichkeits- und -diagnoseanalyse (FMEDA) und quantitative Risikobewertung.
- Konzentriert sich auf die Quantifizierung der Ausfallwahrscheinlichkeit, der Schwere der Folgen und des Gesamtrisikos, das mit Systemausfällen verbunden ist.
- Bietet präzise Schätzungen von Sicherheitsmetriken wie der Ausfallwahrscheinlichkeit auf Anforderung oder dem Automobil-Sicherheitsintegritätslevel (ASIL).
- Erfordert detaillierte Informationen über Ausfallraten, Systemarchitektur und Betriebsbedingungen.

Qualitative Sicherheitsanalyse:

- Stützt sich auf beschreibende oder kategoriale Bewertungen der Sicherheit.
- Umfasst Techniken wie Gefahrenanalyse und Risikobewertung (HARA), Fehlermöglichkeits- und -effektanalyse (FMEA) und strukturiertes Brainstorming.
- Betonung des Verständnisses der Natur und der Eigenschaften potenzieller Gefahren und Ausfallmodi.
- Konzentriert sich auf die Identifizierung und Priorisierung von Sicherheitsbedenken auf der Grundlage von Expertenurteilen, historischen Daten und Systemkenntnissen.
- Bietet Einblicke in potenzielle Ausfallszenarien, ihre Ursachen und ihre Auswirkungen, ohne spezifische numerische Wahrscheinlichkeiten zuzuweisen.
- Kann in frühen Stadien des Systementwurfs durchgeführt werden, wenn detaillierte quantitative Daten möglicherweise nicht verfügbar sind.

5.2.2. Der Beta-Faktor als Sicherheitsmetrik

Im Kontext der gemeinsamen Ursachenanalysen ist eine wichtige zu berechnende Sicherheitsmetrik der Beta-Faktor. Es ist eine wichtige Kennzahl zur Anzeige der Anfälligkeit für gemeinsame Ursachen. Es wird hier das Verhältnis aus der Gesamtfehlerrate und den Fehlern, die aufgrund einer gemeinsamen Fehlerursache auftreten, gebildet. Ein

gemeinsames Ursachenversagen führt dazu, dass alle Einheiten in der Gruppe gleichzeitig versagen.

Der Beta-Faktor repräsentiert das Verhältnis von Common Cause Failures (CCF) für alle möglichen Fehler (1):

$$\beta = \frac{\lambda_c}{\lambda} \quad (1)$$

Mit

β = Maß für CCF; Anteil von Ausfällen, die eine gemeinsame Ursache haben (Beta-Faktor)

λ_c = abhängige Ausfälle

λ = abhängige Ausfälle (λ_c) + unabhängige Ausfälle

Um die Berechnung des Beta-Faktors durchzuführen, muss zunächst λ_c (abhängige Ausfälle) definiert werden. Für E/E-Komponenten wird üblicherweise die Ausfallwahrscheinlichkeit (quantitativ) für verschiedene Fehlerarten ermittelt.

Wenn es um ausfallsichere Systeme geht, sollten elektromagnetische Störungen unbedingt als potenzielle gemeinsame Ursachen von Ausfällen (CCF) berücksichtigt werden. Eine spezifische qualitative EMV-CCA (Electromagnetic Compatibility Common Cause Analysis) kann helfen, alle Szenarien und Gefährdungen durch elektromagnetische Störungen zu identifizieren, die zu einem gleichzeitigen Ausfall der Primär- und Redundanzfunktionen führen könnten. Diese Analyse führt zu einem Katalog von Fehlerszenarien, der im Systemdesign berücksichtigt werden muss.

Bei der quantitativen Analyse stoßen sowohl die Modellierung als auch das Testen auf praktische Grenzen. Die Bewertung der EMV-Ereignisse erfordert detaillierte Informationen über das spezifische Ereignis, das zur Nichtverfügbarkeit des Systems führt: Zeitpunkt, Dauer und Häufigkeit des Auftretens müssen im Voraus bekannt sein. Zusätzlich sind genaue Daten über die prognostizierten Auswirkungen des Ereignisses auf verschiedene Systeme und Elemente erforderlich. Diese Informationen sind oft nicht verfügbar, schwer zu beschaffen oder nicht präzise genug. Für den betrachteten Bereich des EMV-Verhaltens ist die quantitative Analyse aufgrund von Faktoren, wie begrenzte Datenbasis als Berechnungsgrundlage oder statistische Wahrscheinlichkeiten des Fehlerauftretens, unvollständig. Daher sind die quantitativen Analysen und deren Ergebnisse in diesem Fall nicht vertrauenswürdig. Für EMV bietet sich deshalb die qualitative Sicherheitsanalyse an [2].

5.3. Betrachtung der elektromagnetischen Phänomene

Für den Betrieb eines sicherheitskritischen Systems müssen die möglichen Störgrößen in der für den Einsatzbereich geplanten spezifischen Umgebung betrachtet werden. Dazu gehören:

- Elektromagnetische Umgebung:
 - Bewertung vorhandener Informationen
 - Ableitung von Prüfverfahren und notwendiger Prüfschärfe
 - Einbeziehung der geplanten Sicherheitslevel (ASIL)
- Entwurfs und Integrationsprozess
 - Anforderungen auf Systemebene
 - Anforderungen auf Geräteebene
- Verifikation und Validierung
 - Nachweis der geltenden Anforderungen durch Prüfungen mit geeigneten Bewertungskriterien auf Komponentenebene

- abschließende Bestätigung auf Systemebene durch Checklisten, Inspektionen, Prüfungen, ...
- Störfestigkeitsprüfungen
 - Ableitung von Prüfverfahren und -pegeln
 - Betrachtung der systematischen Eignung der Prüfungen

5.4. EMV im Automobilbereich – eine langjährige Entwicklung

Eine Maßnahme, die in Teil 5 der ISO 26262 definiert ist, um häufige Konstruktionsfehler zu vermeiden, ist die Nutzung von Erfahrungswerten. EMV-Überlegungen für die Automobilindustrie gibt es bereits seit den 1980er Jahren, als die ersten EMV-Design- und Prüfnormen für Kraftfahrzeuge entwickelt wurden. Die Fachleute für EMV in der Automobilindustrie spielen traditionell eine aktive Rolle bei der Entwicklung von Normen und in der Arbeit zahlreicher internationaler Organisationen wie der Internationalen Organisation für Normung (ISO), dem Comité International Spécial des Perturbations Radioélectriques (CISPR), dem Europäischen Komitee für elektrotechnische Normung (CENLEC), der Society of Automotive Engineers (SAE) und der International Commission on Non-Ionizing Radiation Protection (ICNIRP). Die internen Anforderungen der Fahrzeughersteller (OEM) gehen über die Zulassungsvorschriften und oft auch über die Prüfanforderungen der oben genannten Organisationen hinaus.

Die von der EMV-Gemeinschaft gesammelten Erfahrungen sind gewachsen und erstrecken sich auf das Wissen, das in über 30 Jahren Erfahrung mit Serienfahrzeugen gesammelt wurde. Im Umgang mit EMV-bedingten Fehlern im Hinblick auf die funktionale Sicherheit hat die Industrie seit ihren Anfängen in den 1980er Jahren im Laufe der Zeit wertvolle Erkenntnisse gewonnen. ADAS führen keine grundlegend neuen Komponenten in das traditionelle Fahrzeug ein, aber neue Anforderungen, da der Fahrer als Rückfallebene bei Fehlfunktionen ausfällt. Zusammenfassend lässt sich sagen, dass die in der ISO 26262 geforderten spezifischen Störfestigkeitsprüfungen in der Industrie bereits gängige Praxis sind, mit einigen kleinen Ausnahmen, die eine weitere Bewertung durch den OEM erfordern. Dies spiegelt die Bemühungen der Industrie in den letzten Jahrzehnten wider, ihre Methoden in Bezug auf EMV zu aktualisieren und zu verfeinern, um neuen Anforderungen gerecht zu werden und sichere Produkte zu entwickeln.

5.5. EMV-Störfestigkeitsprüfverfahren und die Anforderungen an die funktionale Sicherheit

Die Sicherheitsnormen beruhen stets auf der Anwendung bewährter Sicherheitstechniken, die folgende Aspekte berücksichtigen

- alle wahrscheinlichen Fehler,
- Umweltextreme und Alterung,
- vernünftigerweise vorhersehbarer Gebrauch oder Missbrauch
- über den gesamten Lebenszyklus des Geräts.

Dieser Ansatz unterscheidet sich deutlich von der normalen EMV-Störfestigkeitsprüfung, bei der zum Beispiel der Lebenszyklus der Geräte außer Acht gelassen wird. In der Normung greifen einige veröffentlichte und in Arbeit befindliche Papiere die Thematik "EMV für funktionale Sicherheit" auf, wie die IEC-Grundnorm für EMV für funktionale Sicherheit, IEC 61000-1-2 [3].

Herkömmliche EMV-Prüfmethoden sind auf Genauigkeit, Vergleichbarkeit und Wiederholbarkeit ausgelegt und simulieren nicht jede denkbare reale Exposition

elektromagnetischer Ereignisse. Es lassen sich schon aus ökonomischen Gründen nicht alle denkbaren EMV-Szenarien für alle Prüfebene abdecken.

Normale Störfestigkeitsprüfungen decken jeweils nur eine Art von Störung ab, während Geräte in der Praxis mehreren elektromagnetischen Bedrohungen gleichzeitig ausgesetzt sein können. Tests haben gezeigt [4], dass bei Einwirkung mehrerer Störungen (z. B. eines gestrahlten HF-Feldes und von schnellen Transienten) die Störfestigkeit gegenüber dem Einzelstörereignis niedriger ausfallen kann.

Einfach EMV-Störfestigkeitsprüfungen anzuwenden und mit einer Art "Sicherheitsspanne" (z. B. 6 dB) zu versehen, kann daher im Sinn der funktionalen Sicherheit unzureichend sein.

Bei Störfestigkeitsprüfungen wird beispielsweise eine Testfrequenz und Modulation eingestellt und dann mit fester Schrittweite der Prüffrequenzbereich mit einem festgelegten Störgrößenpegel durchfahren, aber in der Praxis sind mehrere, gleichzeitige Bedrohungen mit verschiedenen Frequenzen und Modulationen möglich.

Bei normalen Störfestigkeitsprüfungen werden möglicherweise Kompatibilitätsspannen verwendet, die nicht mit funktionalen Sicherheitsanforderungen vereinbar sind. Alle elektromagnetischen Störungen variieren von Ort zu Ort und von Zeit zu Zeit gemäß einer statistischen Grundlage. Bei Störfestigkeitsprüfungen werden Kompatibilitätsgrenzen festgelegt, die für die kommerzielle und industrielle Zuverlässigkeit geeignet sind, oft auf dem statistischen Zwei-Sigma-Niveau, das 95 % entspricht. Nach IEC 61000-2-2 dürfen zum Beispiel 5 % der elektromagnetischen Ereignisse die geprüften Werte überschreiten. Wo jedoch ein hohes Maß an Sicherheitsintegrität erforderlich ist, können selbst sehr unwahrscheinliche Risiken inakzeptabel sein - daher sollten EM-Bedrohungen mit geringer Wahrscheinlichkeit berücksichtigt werden.

Bei einigen sicherheitsrelevanten Systemen (ASIL D) muss gewährleistet sein, dass mindestens 99 % der EM-Störungen keine Fehler oder Ausfälle verursachen.

Mit Blick auf die funktionale Sicherheit lässt sich festhalten, dass die Prüfungen in den EMV-Normen nicht alle Phänomene einer realen EM-Umgebung abdecken, beispielsweise:

- mehrere elektromagnetische Störeinträge gleichzeitig
- Frequenzbereichsbeschränkungen in Prüfspezifikationen können zu Testlücken führen
- Beschränkung der Betriebsmodi bei den Prüfungen
- Abdeckungslücken bei der Höhe der Feldexposition insbesondere bei hohen Frequenzen
- geringe Anzahl von Prüflingen
- deterministisches Verhalten der Prüflinge bei EMV-Prüfungen
- festgelegte Prüfdauer
- keine Variation anderer Umgebungsbedingungen bei EMV-Prüfungen
- unterschiedliches Verhalten von Prüfeinrichtungen, wie Abweichungen von Pulsformen

Die elektromagnetischen Einwirkungen müssen den ganzen Lebenszyklus über ausgehalten werden, aber die Störfestigkeitsprüfungen simulieren keine möglichen Fehler, die das EMV-Verhalten des Prüflings beeinträchtigen können, zum Beispiel

- eine unterbrochene elektrische Verbindung in einem Filterkondensator oder in der Erdverbindung eines Filters, die die EM-Leistung des Filters beeinträchtigen könnte
- eine Schaltungskomponente, die versehentlich kurzgeschlossen, offen oder außerhalb der Toleranz ist, oder der falsche Typ oder Wert eingebaut wurde
- eine gebrochene Federfingerdichtung oder eine gebrochene elektrische Verbindung, die die Abschirmwirkung eines Gehäuses zerstören könnte

Bei den herkömmlichen EMV-Störfestigkeitsprüfungen werden die vorhersehbare physikalische Umgebung und die Alterung oft nicht berücksichtigt. Die physikalische Umgebung eines Betriebsmittels umfasst Belastungen durch Montage, Stöße, Vibrationen,

Kondensation, Staub, Flüssigkeiten, Alterung, ultraviolettes Licht, extreme Temperaturen und Temperaturwechsel, Korrosion, extreme Versorgungsspannungen usw. All diese Faktoren können sich negativ auf die EMV-Anfälligkeit auswirken [5], zum Beispiel durch

- Verringerung der Abschirmwirkung durch schlechten Kontakt an EMV-Dichtungen
- Verringerung der Filterung durch Alterung der Filterkondensatoren und Temperaturschwankungen, die die Werte der Filterinduktivitäten beeinflussen.

Die Filterleistung kann durch über dem Nennwert liegende Umgebungstemperaturen, Versorgungsspannungen und Lastströme stark beeinträchtigt werden, da sie die Parameter der Filterinduktoren beeinflussen können.

Die für normale Störfestigkeitsprüfungen verwendeten Leistungskriterien können für Sicherheitszwecke unangemessen sein. Eine Leistungsver schlechterung während einer Störung, die für eine einzelne Komponente als akzeptabel gilt, kann zu einem unsicheren Verhalten des Systems führen, in dem es eingesetzt wird.

So lässt die ECE R10 [6] für Tests von Komponenten mit Pulsen und Burst nach ISO 7637 für "Immunity related functions", zu denen auch sicherheitsrelevante Funktionen wie die elektrische Lenkung oder die Datenübertragung gehören, je nach Prüfsignal Funktionszustände A – C zu. Der Hersteller einer Fahrzeugkomponente kann behaupten, dass sein Gerät die Anforderungen der ECE R10 (Typzulassung) vollständig erfüllt, aber wenn es in einem ADS eingesetzt wird, kann der Funktionszustand C der Einzelkomponente während der Störbeeinflussung die Funktionalität des Gesamtsystems unzulässig herabsetzen.

Die Leistungskriterien für die einzelnen Geräte - wenn sie auf Störfestigkeit gegen EMI geprüft werden - hängen also von der jeweiligen Anwendung ab. Sie müssen die Anforderungen des endgültigen Sicherheitssystems erfüllen, wie sie durch eine Gefahrenbewertung und Risikoanalyse ermittelt wurden.

Nur eine oder wenige repräsentative Stichproben werden auf EMV geprüft. Entwickelte Geräte werden mit "Black-Box"-EMV-Prüfverfahren getestet und dann nach Bedarf geändert, bis sie die EMV-Tests bestehen. Ob die endgültige Version aufgrund eines guten Designs bestanden hat oder wie groß der Sicherheitsabstand ist, bleibt unerkannt. *Es besteht hier ein anderer Ansatz, als er für Sicherheitsnormen typisch ist.*

Die EMV-Prüfung bezieht sich im Allgemeinen nicht auf Wartung, Reparatur, Überholung und Aufrüstung (z.B. Softwareupdate). Bei einer Betrachtung des gesamten Lebenszyklus können diese Bedingungen relevant sein. Sicherheitsprüfungsnormen berücksichtigen einige dieser Aspekte im Sinne einer guten sicherheitstechnischen Praxis.

5.6. Fehler bei EMV-Prüfungen aus Sicht der funktionalen Sicherheit

Fehlerzustände, die infolge von elektromagnetischen Ereignissen auftreten, sind systematische Fehler. Diese sind nach ISO 26262 definiert als "Fehler, die auf deterministische Weise mit einer bestimmten Ursache zusammenhängen und nur durch eine Änderung der Konstruktion oder des Fertigungsprozesses, der Betriebsverfahren, der Dokumentation oder anderer relevanter Faktoren beseitigt werden können".

Damit können wir systematische Fehler als "Methoden- oder Prozessfehler" bezeichnen. Es handelt sich dabei um jeden Fehler in der Anwendung von Methoden oder Prozessen, dessen Folgefehler sich auf deterministische Weise zeigt.

Was verstehen wir unter "deterministisch"? Es bedeutet, dass, wenn derselbe Fehler n-mal unter bestimmten Bedingungen in das System eingespeist wird, jedes Mal derselbe Fehler auftreten wird. Der Fehler ist nicht wirklich an den Kontext der Sicherheit gebunden. Er kann sich auf die Sicherheit auswirken, muss es aber nicht. Mit anderen Worten, dieser Fehler kann schließlich zu

- einer Verletzung des Sicherheitsziels,

- einer falschen Erkennung einer Verletzung des Sicherheitsziels,
- der Nicht-Erkennung einer Verletzung des Sicherheitsziels oder
- einem Fehlverhalten führen, das überhaupt nicht mit der Sicherheit zusammenhängt.

Systematische Fehler können durch die konsequente Anwendung von Sicherheitsanalysemethoden gefunden und abgestellt werden.

5.7. Prüfphilosophie für sicherheitsbezogene Systeme und EUT

Das Verhalten eines sicherheitsrelevanten Systems muss unter allen festgelegten Bedingungen bekannt sein. Damit müssen auch für den Fall eines Ausfalles oder Auftreten eines Fehlers Zustände definiert sein. Ausschlaggebend ist die sicherheitskritische Funktion. Damit muss die Funktion unter allen Bedingungen immer einen vorher festgelegten Zustand einnehmen und dieser muss auch detektierbar sein. In der IEC 61000-1-2 werden hierfür folgende Zustände definiert:

A: Das Verhalten wird von dem elektromagnetischen Ereignis nicht beeinflusst. (Das ist vergleichbar zu den Funktionszustandsklassifizierungen.)

DS: Die Funktionen für Sicherheitsanwendungen des Prüflings muss unter allen Umständen (beeinflusst, nicht beeinflusst) einen (von mehreren) detektierbaren, definierten Zuständen einnehmen und diesen für eine definierte Zeit aufrechterhalten.

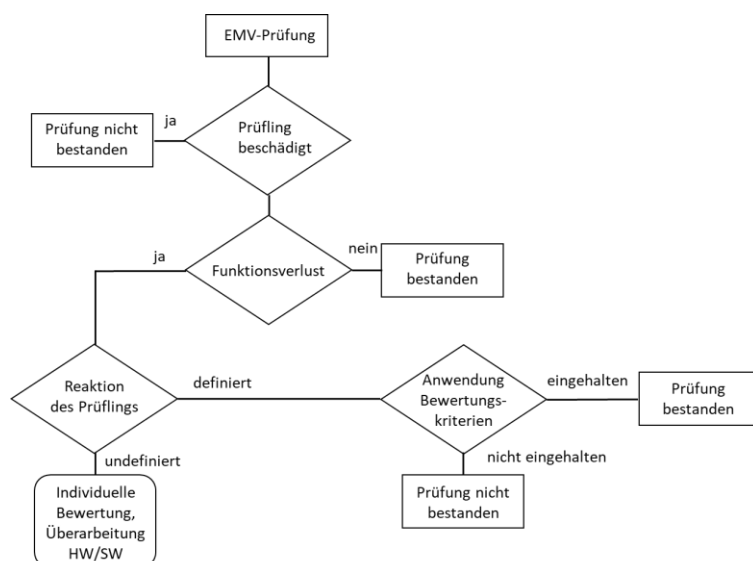


Abbildung 6 Vorgehen bei Störfestigkeitsprüfungen für nicht sicherheitsrelevante Systeme

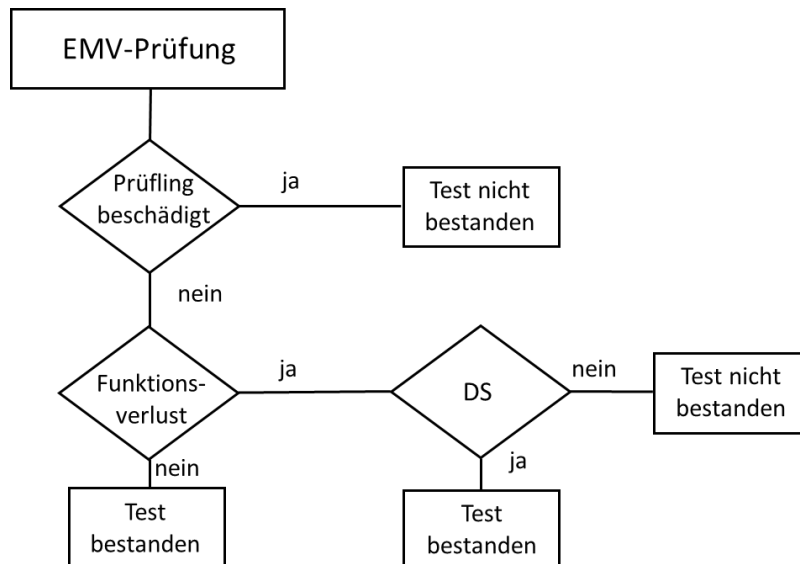


Abbildung 7 Vorgehen bei Störfestigkeitsprüfungen für sicherheitsrelevante Systeme

Damit unterscheiden sich diese Bewertungskriterien von den üblichen Funktionszustandsklassifizierungen, bei denen z.B. die Erholzeit erst bei den Messungen dokumentiert wird.

Für das Bestehen der Prüfung ist es aus Sicht der funktionellen Sicherheit rein formal nicht notwendig, ein unter Störbeeinflussung fehlerfreies sicherheitsrelevantes System zu haben, das System muss jedoch immer einen – vorher – definierten (sicheren) Zustand erreichen.

Da in der Analyse der Gefährdungen nur die Phänomene berücksichtigt werden, die aufgrund von Erfahrungen, Vorgaben oder Recherchen bekannt sind, können keine unvorhersehbaren Ereignisse Bestandteil der Sicherheitsbetrachtungen sein. Im Bereich der EMV ist davon auszugehen, dass die möglichen Beeinflussungen, wie maximal im Einsatzbereich der Fahrzeuge auftretende Feldstärken, bekannt sind und die potentiellen Gefahren ständig analysiert und bewertet werden.

5.8. Sicherstellung der EMV-Vorgaben für die funktionale Sicherheit

In der Produktentwicklung für Systeme und Komponenten, die funktionalen Sicherheitsanforderungen unterliegen, müssen die folgenden Punkte berücksichtigt werden:

- Welchen elektromagnetischen Bedrohungen könnten die Geräte vorhersehbar ausgesetzt sein?
- Was könnte als Folge der im ersten Punkt genannten EM-Bedrohungen vorhersehbar passieren?
- Welche Auswirkungen haben die obigen Punkte auf die funktionale Sicherheit?
- Welche Maßnahmen sind erforderlich, um die erforderliche Integrität der funktionalen Sicherheit zu erreichen?
- Welche Unterlagen sind erforderlich, um das Vorgehen nachzuweisen?

Diese Punkte sollen nun näher beschrieben werden.

5.9. Welchen EMV-Bedrohungen könnten die Geräte vorhersehbar ausgesetzt sein?

Zur Nachbildung der realen EMV-Bedrohungen sind EMV-Prüfungen vorgeschlagen. Diese enthalten die oben bereits aufgeführten Testeinschränkungen. In der ISO 26262-Teil 5 sind folgende EMV-Prüfungen zur Absicherung der funktionalen Sicherheit für Komponenten aufgeführt:

- ISO 11452 Straßenfahrzeuge - Elektrische Störungen durch schmalbandige gestrahlte elektromagnetische Energie; Prüfverfahren für Komponenten
- ISO 11452-1 Allgemeines und Definitionen [7]
- ISO 11452-2 Absorberraum [8]
- ISO 11452-4 Stromzange (BCI) [9]

- ISO 7637 Straßenfahrzeuge - Elektrische, leitungsgeführte und gekoppelte Störungen
- ISO 7637-1 Allgemeines und Definitionen [10]
- ISO 7637-2 Elektrische, leitungsgeführte Störungen auf Versorgungsleitungen [11]
- ISO 7637-3 Übertragung von impulsförmigen elektrischen Störgrößen durch kapazitive und induktive Kopplung auf Leitungen, die keine Versorgungsleitungen sind [12]

- ISO 10605 Straßenfahrzeuge - Prüfverfahren für elektrische Störungen durch elektrostatische Entladungen [13]

Für die Untersuchungen in dieser Arbeit am Demonstrator werden nur diese Prüfungen berücksichtigt. Unter Berücksichtigung der Fragen im vorhergehenden Abschnitt können sich weitere notwendige Testumfänge ergeben.

Diese Prüfverfahren werden im Folgenden kurz beschrieben.

5.9.1. ISO 11452-2 Gestrahlte Störfestigkeit - Antennenmessverfahren

Das Messverfahren beschreibt die Prüfungen von Komponenten gegenüber der Einstrahlung von elektromagnetischen Feldern durch externe (offboard) Störquellen in einer geschirmten Messkabine. Es erfolgt der Aufbau auf der leitfähigen Grundplatte des Messtisches. Die Versorgung wird über eine Bordnetznachbildung geführt. Es ist nach ISO im Bereich von 80 MHz – 18 GHz definiert. Abhängig vom Frequenzbereich erfolgt die Einstrahlung auf den Kabelbaum ($f \leq 1$ GHz) oder das EUT ($f > 1$ GHz) direkt. Bei den Prüfungen wird der Prüfling den festgelegten Prüfschärfegraden und Modulationen für jede Prüffrequenz für eine festgelegte Zeitspanne ausgesetzt und dann die Prüffrequenz mit den in der Norm festgelegten Schrittweiten entsprechend weitergeschoben. Die Funktionen des Prüflings werden während der Prüfung überwacht.

Es sind in der ISO 11452-1 vier mögliche Modulationen für die Tests definiert, die genutzt werden können, wenn im Lastenheft keine weiteren Festlegungen getroffen wurden.

- a) Unmodulierte Sinuswelle (CW)
- b) Sinuswelle amplitudenmoduliert (AM) mit 1 kHz Sinuswelle bei einem Modulationsgrad von 0,8
- c) Sinuswelle pulsmoduliert Typ 1 (PM, ähnlich GSM).
- d) Modulierter Sinusimpuls Typ 2 (PM, ähnlich Radar)

Weiterhin sind die Frequenzbereiche festgelegt, in denen die Modulationen standardmäßig anzuwenden sind.

- CW: 15 Hz bis 18 GHz;
- AM: 10 kHz bis 800 MHz;
- PM Typ 1: 800 MHz bis 1,2 GHz und 1,4 GHz bis 2,7 GHz;
- PM Typ 2: 1,2 GHz bis 1,4 GHz und 2,7 GHz bis 18 GHz.

Es sind in der Norm verschiedene Prüfschärfgrade definiert, deren Anwendung im Lastenheft typischerweise festgelegt ist. Die Prüfschärfgrade (Beispiele in Tabelle 6) sind für die Bewertung im Sinne der funktionellen Sicherheit mit einer Funktionszustandsklassifizierung zu verbinden. Frequenzbereiche für die Definition von Prüfschärfgrade können entsprechend des EUT in den Grenzen der Norm gewählt werden.

Frequenz (MHz)	Test Level I (V/m)	Test Level II (V/m)	Test Level III (V/m)	Test Level IV (V/m)	Test Level V (V/m)
80 - 18.000	25	50	75	100	Spezifische Werte, die zwischen den Nutzern dieses Dokuments vereinbart wurden

Tabelle 6 Prüfschärfegrade nach ISO 11452-2 für ALSE-Tests

Ergänzend sei noch erwähnt, dass in der ECE R10 für die Typzulassung das Verfahren für Komponenten abweichend im Bereich von 20 – 2.000 MHz definiert ist.

5.9.2. ISO 11452-4 Stromzange (BCI)

EMV-Störfestigkeitstestmethode, bei der nach ISO 11452-4 die Störfestigkeit elektronischer Komponenten gegenüber Störfeldern von 0,1 bis 400 MHz geprüft wird, die auf Leitungsstränge bzw. Kabelbäume, an die die betreffenden EUT angeschlossen sind, einstrahlen. Dazu werden mittels einer Stromeinspeisenzange (BCI-Probe) äquivalente HF-Ströme in die Kabelbäume eingekoppelt. Die BCI-Zange bildet hierbei die Primär- und der Kabelbaum die Sekundärwicklung. Auch beim BCI-Test erfolgt der Aufbau in einer geschirmten Kabine mit dem Testaufbau auf der leitfähigen Grundplatte des Messtisches. Die Versorgung wird über eine Bordnetznachbildung geführt.

Normativ gibt es zwei Möglichkeiten für die Regelung der Stromeinspeisung:

- die Substitutionsmethode, bei der ein vorher kalibrierter Strom entsprechend des Prüfgrades eingespeist wird,
- die Closed-Loop-Method, bei der der eingespeiste Strom mit einer weiteren Stromzange gemessen wird.

Der resultierende Störstrom ist von den Impedanzen in den Leitungen abhängig, in die eingekoppelt wird. Es sind verschiedene Einkoppelpunkte auf dem Kabelbaum mit unterschiedlichen Abständen zum Prüfling definiert.

Es sind hier fünf verschiedene Prüfschärfegrade (siehe Tabelle 7) definiert.

Frequenz-band [MHz]	Test Level I [mA]	Test Level II [mA]	Test Level III [mA]	Test Level IV [mA]	Test Level V
0,1 – 1	20	33	50	66	Spezifische Werte, die zwischen den Nutzern dieses Dokuments vereinbart wurden
1 – 3	60 x f / 3	100 x f / 3	150 x f / 3	200 x f / 3	
3 – 200	60	100	150	200	
200 – 400	60 x 200 / f	100 x 200 / f	150 x 200 / f	200 x 200 / f	
In den Formeln ist die Frequenz (f) in MHz einzusetzen					

Tabelle 7 Prüfschärfegrade nach ISO 11452-4 für BCI-Tests

Ein Prüfschärfegrad ist für die Bewertung im Sinne der funktionellen Sicherheit mit einer Funktionszustandsklassifizierung zu verbinden.

5.9.3. ISO 7637-2 Störungen auf Versorgungsleitungen

Die Norm beschreibt die Störfestigkeitsprüfungen von Komponenten gegenüber typischen Transienten, die in einem Kfz-Bordnetz auftreten können. Diese Pulse werden mit entsprechenden Impulsgeneratoren für die Prüfungen auf Tischaufbauten eingepreßt. Es werden langsame und schnelle Pulsformen als Prüfbeaufschlagung auf den

Versorgungsleitungen in der Norm beschrieben. Die Beaufschlagung erfolgt als Pulsfolge mit einer vorgegebenen Prüfdauer. Es können positive und negative Spannungsspitzen auftreten. Bei negativen Spannungen kann es zu einer Unterbrechung der Versorgung des EUT kommen.

Puls	Beschreibung	Spannungsspitze Testpuls U_s	Dauer t_d (max. Wert)
1	Impuls 1 entsteht durch die Unterbrechung der Versorgung durch induktive Lasten, die parallel zum EUT geschaltet sind. Es sind bis zu 200 ms ohne Versorgungsspannung möglich.	-75 bis -150 V	2 ms
2a	Impuls 2a tritt auf, wenn ein Lastschalter geöffnet wird, während der Zündschalter geschlossen ist. Dieser Impuls kann auch beim Auslösen oder Herausziehen von Sicherungen sowie beim Prellen von Schaltern auftreten.	-75 bis -150 V	0,05 ms
2b	Impuls 2b tritt auf, wenn ein zum EUT paralleler Motor läuft und der Zündschalter geöffnet wird. Impuls 2b umfasst eine Zeitspanne bis 1,5 ms, in der die Versorgungsspannung 0 V betragen kann.	+10 V	0,2 s bis 2 s
3a	Impuls 3 tritt als Folge von Schaltvorgängen auf. Diese umfassen auch das Durchbrennen oder Herausziehen von Sicherungen. Die Charakteristik dieses Impulses wird durch verteilte Kapazitäten und Induktivitäten des Kabelbaums beeinflusst. Impuls 3a hat eine negative U_s .	-112 bis -220 V	150 ns $\pm$ 45 ns
3b	Impuls 3 tritt als Folge von Schaltvorgängen auf. Diese schließen das Durchbrennen oder Herausziehen von Sicherungen ein. Die Charakteristik dieses Impulses wird durch verteilte Kapazitäten und Induktivitäten des Kabelbaums beeinflusst. Impuls 3b hat eine positive U_s .	+75 bis +150 V	150 ns $\pm$ 45 ns
Die Prüfschärfegrade sind vor den Prüfungen durch die beteiligten Parteien festzulegen.			

Tabelle 8 Pulsformen nach ISO 7637-2 für Versorgungsleitungen für 12V-Systeme

5.9.4. ISO 7637-3 Impulsförmige Störungen auf anderen als Versorgungsleitungen

Dieser Teil der ISO 7637 legt Prüfstandsmethoden zur Bewertung der Störfestigkeit von Prüflingen gegenüber transienten Impulsen fest, die an andere Leitungen als Versorgungsleitungen gekoppelt sind. Für die Überkopplungen werden die Pulse 2a, 2b, 3a und 3b aus dem Teil 2 verwendet. Die Überkopplung erfolgt für die langsamen Pulse (2a,2b) über eine Koppelkapazität (DCC slow) mit 100 nF, für die schnellen Pulse mittels der kapazitiven Koppelzange. Die Koppelzange ist eine 1 m lange Messvorrichtung, in die die Leitungen eingelegt werden und die zu den Leitungen eine Koppelkapazität von 100pF hat. Damit wird die Überkopplung im Kabelbaum nachgebildet.

Puls	Spannungsspitze U_s			
	Testlevel I	Testlevel II	Testlevel III	Testlevel IV
2a	-8 V	-15 V	-23 V	-30 V
2b	+8 V	+5 V	+23 V	+30 V
3a	-30 V	-60 V	-80 V	-110 V
3b	+18 V	+37 V	+60 V	+75 V
Die Prüfschärfgrade sind vor den Prüfungen durch die beteiligten Parteien festzulegen.				

Tabelle 9 Pulsformen nach ISO 7637-2 für alle Leitungen außer Versorgungsleitungen für 12V-Systeme

5.9.5. ISO 10605 Elektrostatische Entladungen (ESD)

In der Norm werden Tests gegenüber elektrostatischen Entladungen beschrieben. Der Standard umfasst Prüfungen auf Komponenten als auch auf Fahrzeugebene. Für die Komponentenebene werden Tests mit und ohne Spannungsversorgung aufgeführt. Die Prüfungen im unversorgten Zustand der Prüflinge bilden die Gefährdungen beim „Packaging and Handling“ nach. Aus Sicht der funktionalen Sicherheit sind somit auch die Bereiche Produktion und After Sale (Maintenance) abgedeckt. Der Test findet als Labortest auf einem Tisch mit leitender Oberfläche statt.

Für die Entladung mit dem ESD-Generator sind verschiedene Entladenetzwerke, auch RC-Kombinationen vorgesehen, die den menschlichen Körper nachbilden.

Für den Menschen wird als Richtwert eine Kapazität von 100-500 pF gegen Erde angegeben. Mit einem Widerstandswert im k Ω -Bereich bei Entladung der statischen Elektrizität leitet sich das sogenannte Human Body Model (HBM) ab. Die bei der Entladung auftretende Induktivität liegt im nH-Bereich und findet keine Berücksichtigung (Abbildung 8).

Im Kfz-Bereich werden nach ISO 10605 auf der Basis des HBM verschiedene Entladenetzwerke definiert. Die Werte für Widerstand und Kapazität richten sich hierbei nach den jeweils zu betrachteten Fällen. Bei einer elektrostatischen Entladung, welche durch direkten Kontakt mit der menschlichen Haut hervorgerufen wird, definiert die Norm einen Widerstandswert von 2 k Ω . Für die Berührung einer elektronischen Baugruppe mit einem metallischen Gegenstand (Werkzeug, Schlüssel, Ring) gilt ein Widerstandswert von 330 Ω . Zur Ermittlung der Kapazitätswerte wird der Standpunkt des Menschen gegenüber dem Fahrzeug betrachtet. Findet eine Berührung im Fahrzeug statt, gilt der Wert 330 pF. Befindet sich der Mensch außerhalb des Fahrzeugs und berührt die Baugruppe, definiert die Norm einen Wert von 150 pF.

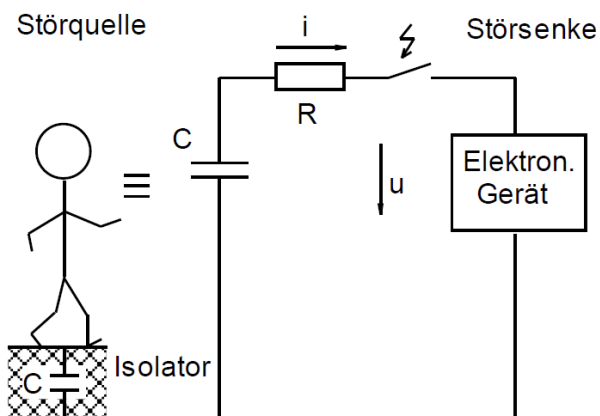


Abbildung 8
Ersatzschaltbild für die elektrostatische Entladung eines Menschen nach dem HBM

Berührungsart	Innerhalb des Fahrzeuges	Außerhalb des Fahrzeuges
Direkter Hautkontakt	2000 Ω / 330 pF	2000 Ω / 150 pF
Metallischer Gegenstand	330 Ω / 330 pF	330 Ω / 150 pF

Tabelle 10 Kombinationen der Entladenetzwerke nach ISO10605

Nach ISO 10605 existieren prinzipiell vier verschiedene Konstellationen für das Auftreten von ESD am Kfz, die mit folgenden Prüfverfahren untersucht werden:

1. Messung im Fahrzeug
2. Messung am Fahrzeug
3. Komponentenprüfung im Labor
4. Prüfung Packaging and Handling (Fertigung / Servicebereich) im Labor

Es werden Kontaktentladungen (direkt und indirekt) und Luftentladungen unterschieden.

Art der Entladung	Entladespannungen
Kontaktentladung	$\pm 2 \text{ kV} - 15 \text{ kV}$
Luftentladung	$\pm 2 \text{ kV} - 25 \text{ kV}$

Tabelle 11 Entladespannungen der Entladenetzwerke nach ISO10605

Die Norm enthält im Anhang C Vorschläge für die einzelnen Prüfungen zu Funktionszuständen und zugeordneten Prüfschärfegraden. Eine feste Einteilung der Entladespannungen für die Entladearten in Prüfschärfegrade wird nicht festgelegt.

5.10. Bewertung von Prüfungen unter Berücksichtigung der funktionalen Sicherheit

5.10.1. Messunsicherheiten von EMV-Prüfungen

Das Ziel von EMV-Messungen ist die Konformitätsaussage in Bezug zu einer Spezifikation oder einem Standard. Mit anderen Worten, es interessiert den Kunden die Bewertung der Prüfungen mit bestanden/nicht bestanden. Für die Prüfungen muss damit angegeben werden

- für welche Ergebnisse die Aussagen zur Konformität gilt;
- welche Spezifikationen, Normen oder Teile davon erfüllt oder nicht erfüllt werden;
- welche Entscheidungsregeln angewendet wurden.

Ein wichtiger Teil der Entscheidungsregeln ist die Betrachtung der Messunsicherheiten während der Prüfungen. Für die Ergebnisse aus den Prüfungen für Baugruppen, die funktionalen Sicherheitsbetrachtungen unterliegen, gelten hierfür besondere Anforderungen. Alle Messungen unterliegen Abweichungen vom exakten Wert. Diese Abweichungen resultieren aus kleinen Fehlern bei den Messungen. Je komplexer der Messaufbau, umso mehr Fehlerquellen kommen hinzu. Die Fehler akkumulieren sich zu einer Gesamtmessunsicherheit, um die der gemessene Wert von der Zielgröße abweicht (Abbildung 9). Eine Reihe von fiktiv identischen Messungen ergibt im Allgemeinen eine Streuung um einen Mittelwert. Die Messergebnisse unterliegen somit einer Wahrscheinlichkeitsverteilung. Sie beschreibt die Wahrscheinlichkeit, dass der wahre Wert bei einer bestimmten Differenz zum Messergebnis liegt. Die Verteilung ergibt sich aus systematischen Anteilen, wie Kalibrierfehlern, und zufälligen Fehlern, wie dem Rauschen einer Spannung im Verstärker. Systematische Fehler weisen immer die gleiche Abweichung vom Messwert auf, zufällige schwanken mit einer bestimmten Bandbreite um einen Mittelwert.

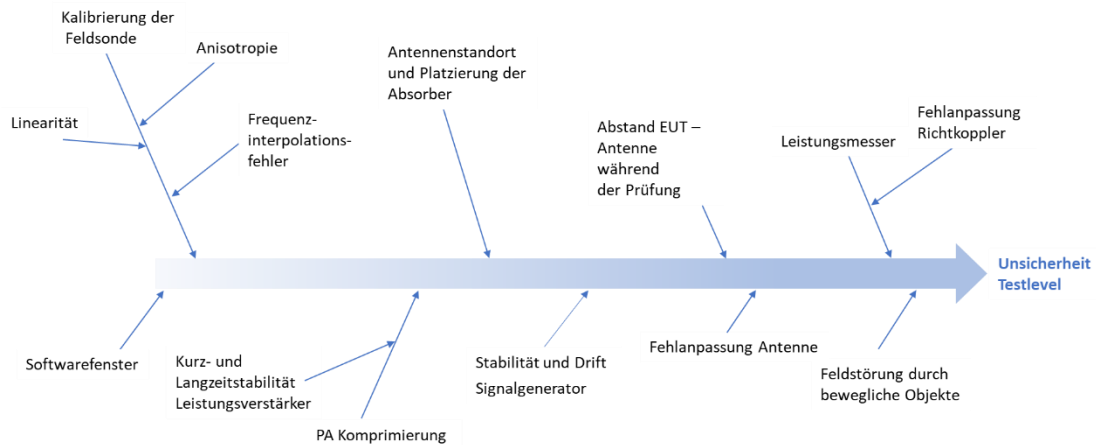


Abbildung 9 Messunsicherheitskomponenten für die Störfestigkeitsprüfung

Für EMV-Prüfungen sind die Wahrscheinlichkeitsverteilungen relevant (Abbildung 10).

- normal: Unsicherheiten, die sich aus mehreren Beiträgen ableiten, z.B. Kalibrierungsunsicherheiten mit einer Aussage zum Vertrauen
- rechteckig: gleiche Wahrscheinlichkeit, dass der wahre Wert irgendwo zwischen zwei Grenzwerten liegt, z. B. Herstellerangaben
- U-förmig: anwendbar auf Fehlanpassungsunsicherheit, bei der die Wahrscheinlichkeit, dass der wahre Wert nahe am gemessenen Wert liegt, gering ist
- dreieckig: Die Wahrscheinlichkeit, dass der wahre Wert an einem Punkt zwischen zwei Grenzwerten liegt, steigt gleichmäßig von Null an den Enden bis zum Maximum in der Mitte an; sollte zugewiesen werden, wenn die Mehrheit der Werte zwischen den Grenzwerten um den zentralen Punkt herum liegt.

Ihre tatsächliche Form wird für die einzelnen Messunsicherheitskomponenten oft unbekannt sein. Es muss aufgrund von Vorkenntnissen oder einer Theorie angenommen werden, dass sie sich einer der üblichen Formen annähert. Sie können dann die Standardunsicherheit $u(x_i)$ für die zugewiesene Form aus einfachen Ausdrücken berechnen.

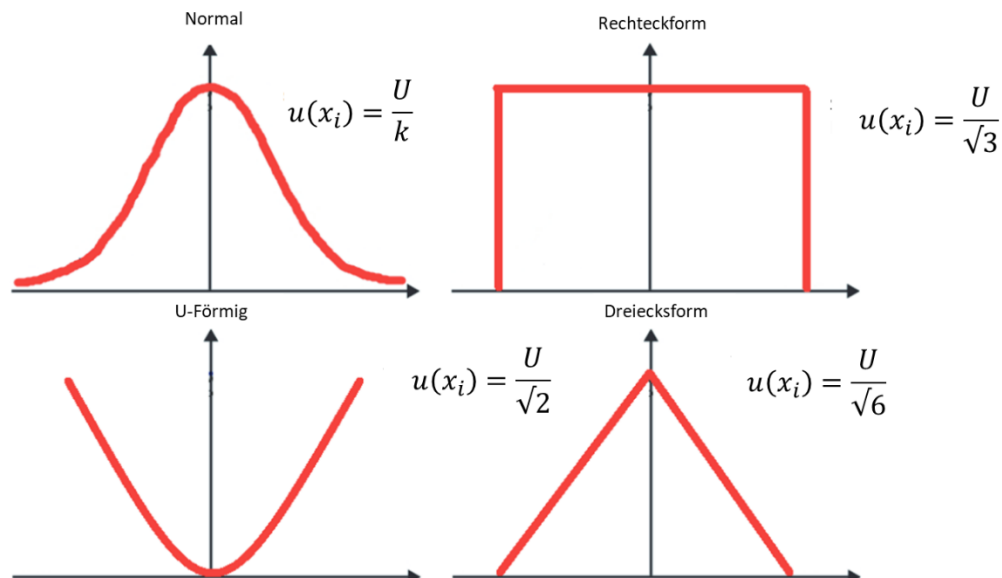


Abbildung 10 Relevante Messunsicherheitsverteilungen für EMV-Messungen

Nachdem jeder Beitrag wie oben in eine Standardunsicherheit umgewandelt wurde, erhält man die kombinierte Unsicherheit $u_c(x)$ für m Beiträge, indem man die Quadratwurzel aus der Summe der Quadrate der einzelnen Standardunsicherheiten zieht.

Daraus kann die erweiterte Unsicherheit U berechnet werden. Diese definiert ein Intervall um das Messergebnis, das den wahren Wert mit einem bestimmten Vertrauensniveau einschließt. Dieses Intervall ist größer als die Standardunsicherheit, so dass eine höhere Wahrscheinlichkeit besteht, dass es den Wert der Messgröße einschließt. Die erweiterte Unsicherheit ergibt sich durch Multiplikation der kombinierten Standardunsicherheit mit einem Erweiterungsfaktor k . Der Faktor wird nach ISO 17025 für ein Vertrauensniveau von 95% auf 2 gesetzt. Der Faktor k entspricht der Standardabweichung σ . Andere Vertrauensniveaus können mit anderen Werten von k erreicht werden, aber der Wert von 95% ist für industrielle und kommerzielle Messanwendungen üblich. Er stellt einen guten Kompromiss aus erreichbarer Testabdeckung und Wirtschaftlichkeit dar.

Wie in Abbildung 11 zu sehen, erreicht man somit aufgrund der Wahrscheinlichkeitsverteilung nur eine 50%ige Sicherheit, dass der Prüfling einer Störfestigkeitsprüfung mit einem vorgegebenen Prüflevel entsprechend der Spezifikation getestet wurde.

Eine detaillierte Erläuterung zur Messunsicherheit mit Beispielen ist in Abschnitt 10 zu finden.

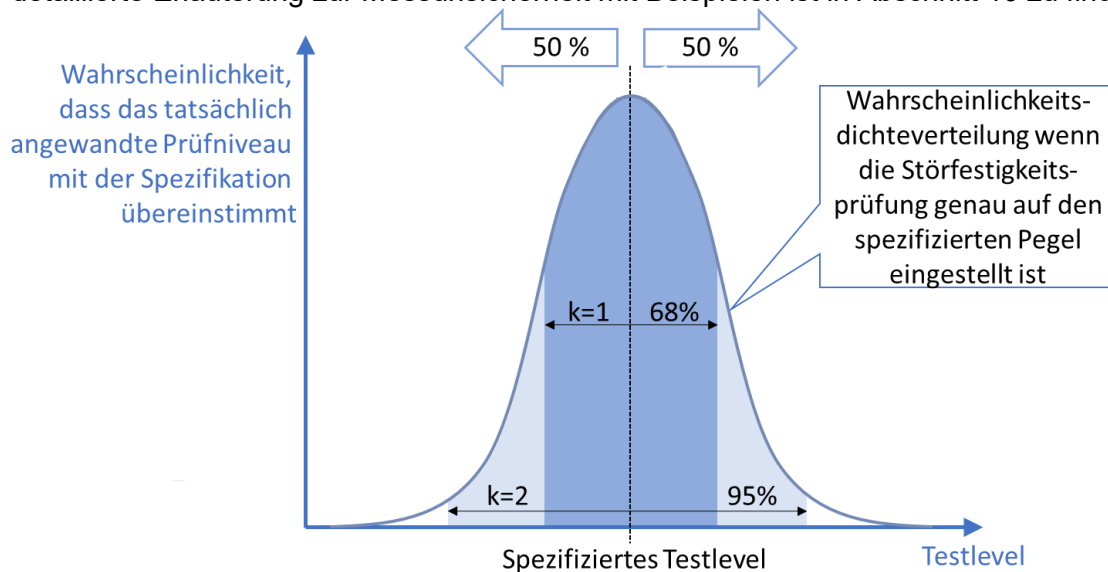


Abbildung 11 Verteilung der Messergebnisse auf Grund der Gesamtmessunsicherheit

5.10.2. Folgen der Störfestigkeits-Bedrohungen

Alle relevanten Fehler, die unter EMV-Beeinflussung auftreten könnten, werden in der Hazard Analysis and Risk Assessment (HARA) ermittelt. Aus der HARA werden dann Sicherheitsziele abgeleitet. Dabei handelt es sich um Sicherheitsanforderungen der obersten Ebene auf Fahrzeugebene. Jede identifizierte Gefährdung erhält entlang des Risiko-Klassifizierungs-Schemas eine ASIL-Sicherheitsstufe (Automotive Safety Integrity Level, kurz ASIL). Dabei wird die Schwere des möglichen Sicherheitsrisikos und das Ausmaß des Risikos berücksichtigt.

Dabei geht es um

- die Schwere der Auswirkung („Severity“ / S),
- die Häufigkeit („Exposure“ / E),
- und die Beherrschbarkeit der Fehlfunktion („Controllability“ / C)

Sind die Sicherheitsziele abgeleitet, dienen sie als Grundlage für das Konzept der funktionalen Sicherheit.

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

Tabelle 12 Ableitung der ASIL-Sicherheitsstufen

5.10.3. Auswirkungen auf die Sicherstellung der funktionalen Sicherheit

Die notwendigen Prüfungen für jedes System und seine Komponenten müssen sorgfältig anhand der zu erwartenden elektromagnetischen Umgebung gewählt werden. Die Störpegel sollten dem Maximum der wahrscheinlich auftretenden Störgrößen entsprechen.

Der Ansatz der quantifizierten Risikobewertung ist für EMV-Prüfungen nicht anwendbar, da die Exposition gegenüber elektromagnetischen Störungen und die Reaktionen der Geräte auf diese Bedrohungen statistische Wahrscheinlichkeiten haben.

Die Absicherung der Störfestigkeit erfolgt anhand von bereits definierten Verfahren und Grenzwerten aus den EMV-Normen. Die Prüfungen unterliegen auch wirtschaftlichen Gesichtspunkten und können nicht alle möglichen Einflüsse und deren Kombinationen abbilden. Weiterhin können EMV-Prüfungen Schwankungen, z. B. in Abhängigkeit vom verwendeten Prüfequipment, unterliegen oder bereits in den Anforderungen so definiert sei, dass sich Abweichungen in den Ergebnissen ergeben können [15].

Für die funktionale Sicherheit müssen dagegen den ASIL feste Ausfallraten in Abhängigkeit von der Betriebszeit zugeordnet werden (FIT-Rate). Die ASIL korrelieren daher nicht mit Prüfschärfegraden. Damit lassen sich keine einfach nachweisbaren Zusammenhänge zu den EMV-Verfahren, den zugehörigen Pegeln und den Anforderungen der funktionalen Sicherheit finden.

Sicherheitsbetrachtungen können zu dem Ergebnis kommen, dass die festgelegten Normverfahren nicht alle erwartbaren Phänomene abdecken können. Daraus folgende Abweichungen von den Normen müssen einer fundierten technischen Begründung unterliegen. Die Abweichungen müssen das Ziel haben, den Vertrauensbereich der Prüfungen zu erhöhen. Abweichungen können sein:

- Prüfpegel
- Prüfdauer
- Variation Prüfaufbau
- Anzahl Prüflinge
- Variation Prüfeinstellungen (Modulation, Phasenlage, Einstrahlrichtung des Feldes)
- Umgebungsfaktoren (Temperatur, Alterung, Feuchtigkeit, Addition von Störeinflüssen)
- Bewertungskriterien

Ein systematischer Ansatz zur Erhöhung des Vertrauensbereiches der Prüfungen muss sich auf verschiedene Schritte stützen. Nachfolgend werden beispielhaft einige aufgeführt.

1. Identifizierung der Zielsetzung:

Der Zweck der Prüfung muss definiert werden. Will man einen Entwurf validieren, ein Herstellungsverfahren verifizieren oder die Einhaltung von Sicherheitsnormen prüfen?

2. Risikobewertung:

Führen Sie eine Risikobewertung durch, um die potenziellen Fehlerarten und ihre Auswirkungen zu ermitteln. Komponenten oder Systeme mit höherem Risiko erfordern in der Regel umfangreichere Tests.

Daraus ergeben sich auch weitere Anforderungen an die Tests auf der Grundlage des Pflichtenheftes für die funktionale und die technische Sicherheit.

3. Statistische Methoden:

Die Verwendung statistischer Methoden zur Bestimmung des Stichprobenumfangs umfasst übliche Ansätze wie:

- Konfidenzniveau und Fehlermarge:
Dazu erfolgt die Bestimmung des gewünschten Konfidenzniveaus (z. B. 95 %) und der akzeptablen Fehlermarge. Dies kann mit statistischen Standardformeln berechnet werden.
- Standardabweichung und Variabilität:
Notwendig ist hier die Abschätzung oder Bestimmung der Variabilität des zu prüfenden Prozesses oder Bauteils. Eine höhere Variabilität erfordert in der Regel einen größeren Stichprobenumfang.

4. Industrienormen und Vorschriften:

Einhaltung der einschlägigen Industrienormen (z. B. ISO 26262 für die Automobilindustrie, IEC 61508 für industrielle Systeme), der Richtlinien oder Anforderungen, die z.B. den Stichprobenumfang bei Prüfungen enthalten.

5. Historische Daten:

Verwenden Sie historische Daten aus früheren Tests, um den erforderlichen Umfang abzuschätzen. Wenn ähnliche Tests bereits durchgeführt wurden, können die Daten als Grundlage für die aktuelle Teststrategie informieren.

6. Pilotversuche:

Durchführung von Pilottests, um erste Daten zu sammeln. Dies kann zur Verfeinerung der Berechnung des Prüfumfangs helfen, indem sich Erkenntnisse zur Variabilität und möglichen Problemen geben.

7. Ressourcen und Beschränkungen:

Berücksichtigung von praktischen Beschränkungen wie Zeit, Kosten und Verfügbarkeit von Proben. Abgleich des Bedarfs an statistischer Sicherheit ist mit diesen Beschränkungen abzuwägen.

8. Sicherheitsspannen:

Berücksichtigung von Sicherheitsmargen, um unerwartete Schwankungen oder Unwägbarkeiten einzugrenzen. Dies kann bedeuten, dass der Stichprobenumfang über das berechnete Minimum hinaus erweitert werden muss.

In den beiden nachfolgenden Kapiteln finden sich Ansätze für die Bewertung von den oben genannten Parameterabweichungen.

5.10.4. Methode zur Ermittlung des statistisch notwendigen Stichprobenumfanges

Generell erhöht die Anzahl der Prüflinge immer das Vertrauensniveau. Aber um diese Aussage auch zu quantifizieren, ist eine statistische Betrachtung notwendig. Grundsätzlich ergibt sich eine statistische Verteilung der Ergebnisse durch eine Erhöhung der Prüflingsanzahl.

Definition von Z-Score und Konfidenzniveau: Der Z-Score (auch bekannt als Z-Wert oder Standardwert) ist ein Maß dafür, um wie viele Standardabweichungen ein Element vom Mittelwert entfernt ist. Im Kontext der Bestimmung der Stichprobengröße wird der Z-Score verwendet, um den kritischen Wert zu finden, der dem gewünschten Konfidenzniveau in einer Standardnormalverteilung entspricht.

Beziehung zwischen Konfidenzniveau und Z-Score:

- Das Konfidenzniveau stellt den Prozentsatz aller möglichen Stichproben dar, von denen erwartet wird, dass sie den wahren Parameter der Grundgesamtheit enthalten.
- Ein Konfidenzniveau von 95 % bedeutet beispielsweise, dass wir erwarten, dass 95 % der Stichprobenmittelwerte innerhalb eines bestimmten Bereichs um den Mittelwert der Grundgesamtheit liegen.

Um den Z-Score zu finden, der einem bestimmten Konfidenzniveau entspricht, betrachtet man die kumulative Wahrscheinlichkeit für die Standardnormalverteilung.

Für gängige Konfidenzniveaus:

- 90% Konfidenzniveau: $Z \approx 1,645$
- 95% Konfidenzniveau: $Z \approx 1,96$
- 99% Konfidenzniveau: $Z \approx 2,576$

Diese Werte können in Z-Tabellen gefunden oder mit statistischer Software berechnet werden.

Standardabweichung Die Standardabweichung (σ) ist ein Maß für das Ausmaß der Variation oder Streuung in einem Datensatz. Im Kontext der Bestimmung der Stichprobengröße spiegelt die Standardabweichung die Variabilität der Daten wider.

Berechnung der Standardabweichung:

1. Für eine Grundgesamtheit (N Werte):

$$s = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - \mu)^2} \quad (2)$$

mit x_i : Wert der einzelnen Stichprobe

μ : Mittelwert der Grundgesamtheit

N : Anzahl der Stichproben/Samples in der Grundgesamtheit

2. Für eine Stichprobe (n Werte):

$$s = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2} \quad (3)$$

mit x_i : Wert der einzelnen Stichprobe

$\bar{x}$: Mittelwert der Stichproben/Samples

n : Anzahl der Stichproben/Samples

Die Stichproben-Standardabweichung (s) wird verwendet, um die Standardabweichung der Grundgesamtheit (σ) zu schätzen, wenn die gesamte Grundgesamtheit nicht gemessen werden kann.

Beispiel: Berechnung der Stichprobengröße mit Z-Score und Standardabweichung
Angenommen, man testet eine elektronische Steuereinheit (ECU) für Fahrzeuge auf Übereinstimmung mit ISO 26262. Das Konfidenzniveau von 95% und die Fehlermarge von 5% ist vorgegeben. Basierend auf früheren Tests ist die Standardabweichung der Ausfallrate bekannt.

- Konfidenzniveau: 95%
- Z-Score für 95% Konfidenzniveau (Z): 1,96
- Fehlermarge (E): 5%
- Standardabweichung (σ): 2% (angenommen aus historischen Daten)

Unter Verwendung der Formel für die Stichprobengröße (n):

$$n = \left(\frac{Z\sigma}{E} \right)^2 \quad (4)$$

ergibt sich aus den hier beispielhaft getroffenen Annahmen:

$$n = \left(\frac{1,96 \cdot 2}{0,05} \right)^2 = (78,4)^2 = 6.145,76 \quad (5)$$

Aufgerundet, um eine ganze Zahl zu erhalten, ergibt sich die notwendige Anzahl der Stichproben zu $n = 6146$.

Diese große Anzahl ist möglicherweise nicht praktikabel, daher können Anpassungen basierend auf Ressourcenbeschränkungen und zusätzlichen Risikoanalysen vorgenommen werden.

Durch die Befolgung dieses Ansatzes wird sichergestellt, dass die Anzahl der für die Tests ausgewählten Stichproben statistisch valide ist und praktische Einschränkungen berücksichtigt, was letztlich die Zuverlässigkeit und Sicherheit des Produkts erhöht. Die Tabelle 13 zeigt den Zusammenhang von ASIL-Level zur erforderlichen quantitativen Metrik.

Fazit: Die Bestimmung der Anzahl der Stichproben für Tests erfordert mehrere Überlegungen, um sicherzustellen, dass der Testprozess robust ist und zuverlässige Daten liefert. Unter Berücksichtigung der verschiedenen Einschränkungen und der Anzahl der Stichproben, die durch die statistische Methode erforderlich sind, erscheint es sinnvoll, sich auf den qualitativen Ansatz zu stützen. Dieser basiert auf Prozessen wie dem Stand der Technik, der ISO 26262-Standardtests, anforderungsbasierten Tests usw.

5.10.5. Zusammenhang von FIT und Prüfpegel

Für die ASIL müssen im Zuge der Sicherheitsanalysen für die FIT bestimmte Wahrscheinlichkeiten erreicht werden (Tabelle 13). Ziel der Hardwaresicherheitsanalysen ist es, die Hardwarearchitektur und die Bauteile noch vor der eigentlichen Hardwareentwicklung nach ISO 26262 im Hinblick auf Robustheit gegenüber Einfach- und Mehrfachfehler. Dies geschieht durch Metriken, welche auch am Ende die Grundlage zur Berechnung der Ausfallwahrscheinlichkeit bzw. die Restfehlerwahrscheinlichkeit bildet.

Für eine Baugruppe mit ASIL D sind also mindestens 99% der sicherheitsrelevanten Einfachfehler des Systems sicher zu beherrschen und mindestens 90% aller latenten Fehler, das sind Fehlfunktionen der Diagnose, zu erkennen. Die bestimmungsgemäße Funktion des Items darf nur 10 FIT Restausfallwahrscheinlichkeit haben.

Ein FIT bedeutet einen Ausfall in einer Milliarde Betriebsstunden. Die Anzahl der Betriebsstunden ergibt sich aus dem Produkt der Anzahl der Geräte und deren

Betriebsstunden. Die FIT-Rate kann also die Anzahl der Ausfälle bei 1 Million Geräten für 1000 Betriebsstunden oder 1000 Geräte für 1 Millionen Stunden erfassen.

ASIL	Fehlerrate pro Zeit	SPFM [%] ^{*)1}	LFM [%] ^{*)2}	Erhöhung Testlevel
A	<1000 FIT	nicht relevant	nicht relevant	nicht relevant
B	<100 FIT	≥90	≥60	1,28
C	<100 FIT	≥97	≥80	1,88
D	<10 FIT	≥99	≥90	2,32

^{*)1} Single-point fault metric (SPFM)

^{*)2} Latent fault metric (LFM)

Tabelle 13 Fehlermetrik für ASIL und resultierende Prüfgrößenerhöhung

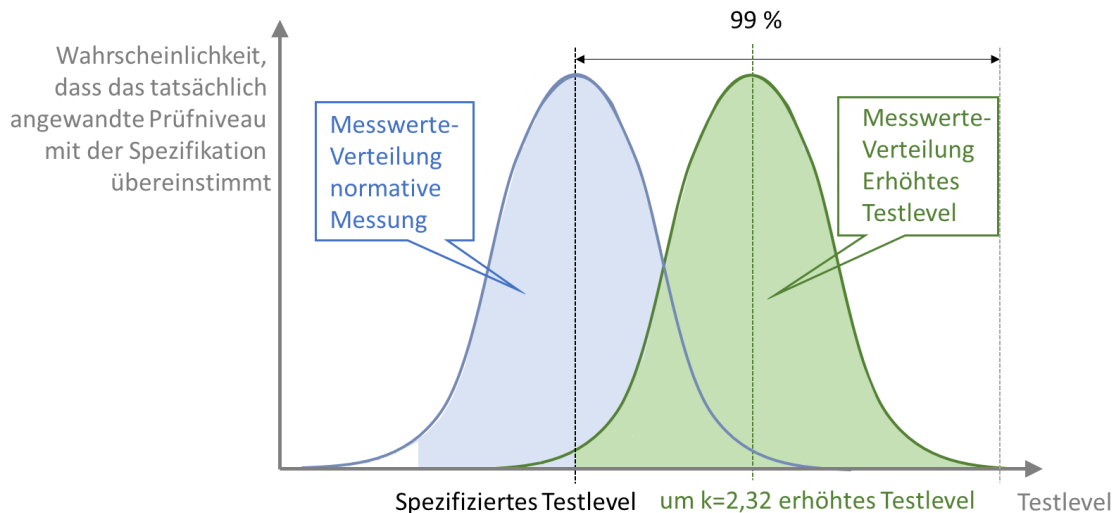


Abbildung 12 Erhöhung des Vertrauenspotentials für die Prüfungen

Wie weiter oben beschrieben (Abbildung 11) wird bei den Standard-EMV-Messungen nur eine bestimmte Abdeckung des Testniveaus erreicht. Die Abdeckung des Testniveaus mit nur 50% der Messwerte ist für sicherheitsrelevante Prüflinge nicht immer ausreichend. Um diese Abdeckung auf ein das ASIL gefordertes Level zu heben, wird die Störgröße um den Faktor k für erweiterte die Unsicherheit erhöht. Dazu muss das in Abbildung 11 eingezeichnete „Spezifizierte Testlevel“ (blau) soweit erhöht werden, dass das notwendige Vertrauensintervall der Messwerte gleich oder größer als der Wert des „Spezifizierte Testlevel“ ist (grün).

Wie aus der Tabelle 13 zu erkennen ist, muss für eine ASIL D Applikation die Hardware-Architektur sicherstellen, dass die Risiken durch Einfachfehler zu $\geq 99\%$ durch Sicherheitsmechanismen abgedeckt sind. Wenn die EMV-Messungen bei Spezifizierung auf die nominalen Prüfniveau nur ein Vertrauensniveau von 95% erreichen, ist das nicht gegeben. Eine Möglichkeit besteht darin, das Vertrauensniveau so weit zu erhöhen, dass die Vorgaben aus der Fehlermetrik nach Tabelle 13 erreicht werden. Da die Unsicherheitsbereiche eine angenommene Gauß-Verteilung haben, wird das Prüfniveau für eine Komponente soweit erhöht, bis alle Messungen im notwendigen Vertrauensintervall im Bereich oberhalb des spezifizierten Prüfniveaus liegen. Es wird sichergestellt, dass die Anzahl der Messwerte den Vorgaben der Single Point Fault Metrik entspricht. Hierbei ist zu beachten, dass die notwendige Abdeckung nur eine anteilige Verschiebung der Messwerte bedingt. Das soll kurz am Beispiel aus Abbildung 11 erläutert werden. Die hier dargestellte Abdeckung von 95% ist um den Mittelwert der Gauß-Verteilung angeordnet. Die beiden Bereiche außerhalb des Konfidenzintervalls umfassen je $2,5\%$ der Messwerte. Für eine Verschiebung sind nur die Messwerte zu betrachten, die größer oder gleich dem „Spezifizierten Testlevel“ sind. Für eine ASIL D Komponente bedeutet dies, dass 99% der Messwerte in diesem Bereich liegen müssen. Damit dürfen 1% der Messwerte niedriger als das „Spezifizierten Testlevel“ sein. Es erfolgt somit eine Verschiebung um den Faktor $2,32$ multipliziert mit der ermittelten Standardabweichung, der einem Konfidenzintervall von 98% entspricht. Damit erreicht man mathematisch eine

99prozentige Abdeckung des Testlevels (Abbildung 12) und würde damit die Vorgabe zur SPFM erfüllen. Die Erhöhung des Testlevels ist damit abhängig von den ermittelten Messunsicherheiten des Aufbaus für das jeweilige Prüfverfahren und den dafür genutzten Komponenten. Für die Sicherstellung des Vertrauenspegels ist somit die Kenntnis der Messunsicherheiten im Messlabor notwendig. Das Vorgehen ist für ASIL B und C gleich. Die entsprechenden Werte für den Faktor k lassen sich den Z-Tabellen in Literatur ablesen. Beispiele sind im Anhang aufgeführt.

Einer Erhöhung der Prüfgrößen sind Grenzen gesetzt, die sich aus praktischen Überlegungen und der Prüftechnik ergeben. Einmal sind die Limits, die die OEMs vorgeben, in der Regel signifikant höher als die gesetzlichen Vorgaben. Es sind hier bereits Sicherheitsaufschläge berücksichtigt. Weiterhin sind durch die vorhandene Prüftechnik Beschränkungen vorgegeben. Damit sind unter Umständen die ermittelten Erhöhungen gar nicht umsetzbar. Das vorgeschlagene Vorgehen ist somit unter fachlichen Gesichtspunkten für jeden Prüfling zu bewerten.

5.10.6. Erforderliche Maßnahmen für Integrität der funktionalen Sicherheit

- Schutzmaßnahmen als Sicherheitsfunktion(en) bzw. Sicherheitsziel(e) formulieren mit Merkmalen (ASIL, phy. Grenzwerte, etc.)
- Sicherheitsanforderungen ableiten
- Sicherheitskonzept entwerfen
- Systementwurf auf Eignung prüfen durch Analyse (Methodenkompetenz):
 - HW robust gegen Einfach- oder Mehrfachfehler auslegen
 - Diagnoseumfang im notwendigen Maß zur realisieren
 - Aufbau, Testumgebung und Prüfungen an die Anforderungen des EUT und die der funktionalen Sicherheit anpassen

5.10.7. Zusammenfassung von EMV-Prüfungen unter Berücksichtigung der funktionalen Sicherheit

EMV-Prüfungen im Rahmen der funktionalen Sicherheit müssen nachweisen, dass die im Rahmen der Analyse definierten Sicherheitsziele eingehalten werden. Dies gilt auch für den Fall, dass während der Prüfung Fehler auftreten.

Was die Störfestigkeitstests nicht nachweisen können, ist die Fehlerfreiheit. Welches Verhalten die Funktionen eines Prüflings über die Testschärfe hinaus haben, bleibt unbekannt. Im Rahmen des Sicherheitsassessments werden je nach ASIL auch quantitative Nachweise der Fehlerwahrscheinlichkeit und Diagnoseabdeckung (Tabelle 13) gefordert. Für die quantitative Analyse der Auswirkungen von EMV-Prüfungen sind weder Modellierung noch experimentelle Untersuchungen umsetzbar. EMV-Auswirkungen lassen sich im Sinne der Sicherheitsmetriken nur quantifizieren, wenn Zeitpunkt, Dauer, Auftretenshäufigkeit und elektromagnetische Eigenschaften der realen Umgebung bekannt sind. Zudem wären präzise Informationen über die erwarteten Auswirkungen auf Systeme und Komponenten erforderlich – diese fehlen jedoch oft oder sind nur schwer und ungenau zu ermitteln. Eine umfängliche quantitative Analyse nach den Metriken der ISO 26262 ist damit für die EMV-Prüfungen nicht möglich [2].

5.10.8. Welche Unterlagen sind erforderlich, um das Vorgehen nachzuweisen?

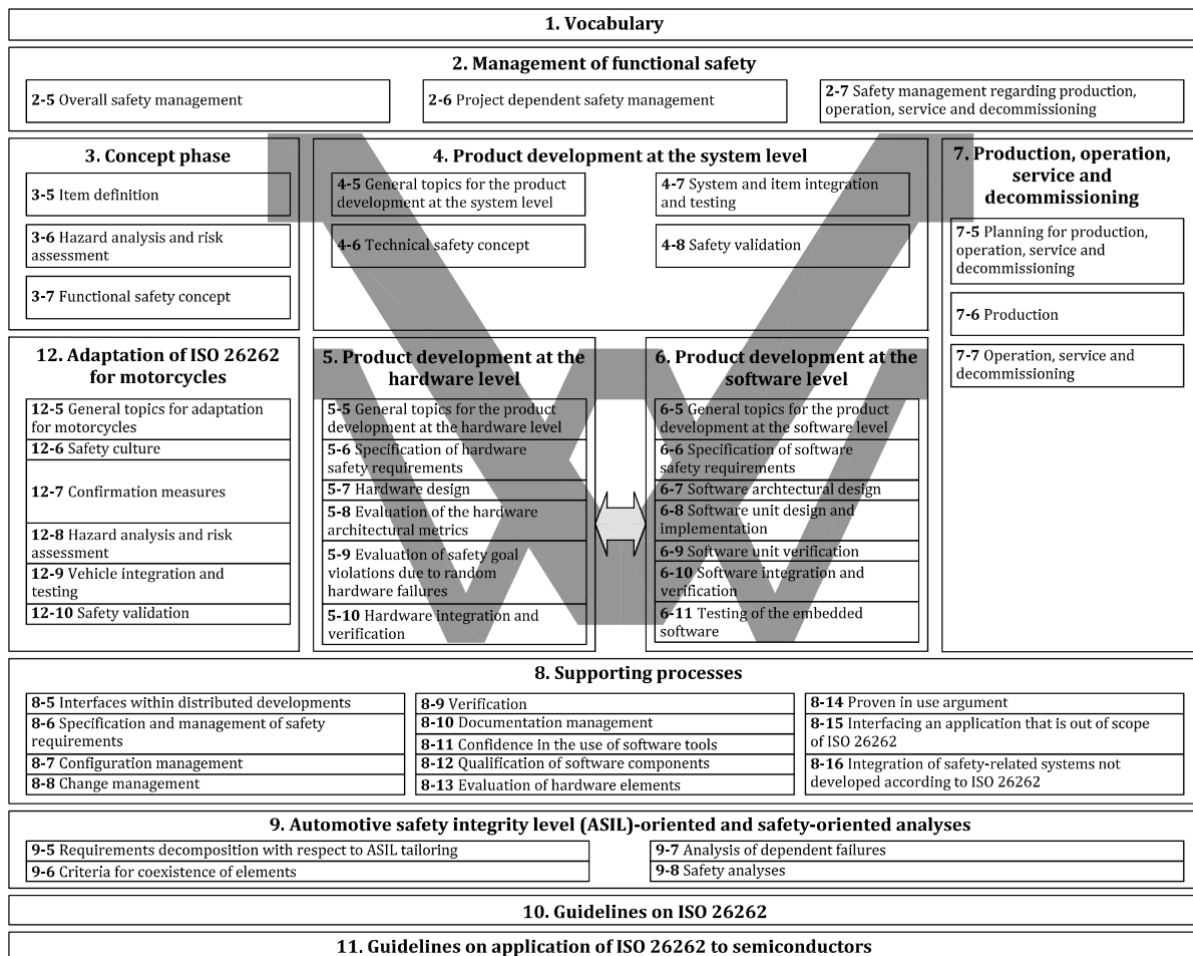


Abbildung 13 V-Diagramm des funktionalen Sicherheitsmanagements aus ISO 26262 [1]

In Bezug auf das technische Arbeitsprodukt in der Entwicklungsphase (linke Seite des V-Zyklus) besteht es aus 3 Schritten:

1. Konzeptphase
2. Produktentwicklung auf Systemebene
3. Produktentwicklung auf HW- und SW-Ebene

In der Konzeptphase besteht das Ziel darin, den untersuchten Gegenstand, seine Schnittstellen mit anderen Gegenständen, die Hauptfunktionen, die damit verbundenen gefährlichen Ereignisse und das Sicherheitskonzept einschließlich der vorläufigen Architektur zu definieren. Der EMV-Aspekt muss in diesem Schritt berücksichtigt werden, um die relevante Architektur des Elements zu wählen (d. h. die Art der Redundanz, die je nach Projektbeschränkung verwendet wird). Die wichtigsten Dokumente in diesem Schritt sind:

- Objektdefinition (Item)
- HARA
- Funktionales Sicherheitskonzept

Bei der Produktentwicklung auf Systemebene besteht das Ziel darin, das Element mit den technischen Sicherheitsanforderungen (TSC) zu analysieren und technisch zu definieren, den Sicherheitsmechanismus auf Systemebene zu definieren und den Architekturentwurf zu verfeinern. In diesem Schritt muss der EMV-Aspekt in der Sicherheitsanalyse berücksichtigt

werden, um den richtigen Sicherheitsmechanismus und die beste Architektur zu definieren, um EMV-gefährdende Ereignisse zu vermeiden. Die wichtigsten Dokumente dieses Schrittes sind:

- Technisches Sicherheitskonzept
- Fehlerbaumanalyse (einschließlich EMV-Aspekt)
- Analyse der gemeinsamen Ursache (einschließlich EMV-Aspekt)
- Architektonischer Entwurf

Bei der Produktentwicklung auf HW- und SW-Ebene besteht das Ziel darin, das Produkt genauer zu analysieren und sich einerseits auf den HW-Teil des Produkts und andererseits auf den SW-Teil des Produkts zu konzentrieren, den Sicherheitsmechanismus auf HW- und SW-Ebene zu definieren und das Sicherheitskonzept des Produkts zu bewerten. Bei der Sicherheitsanalyse in diesem Schritt liegt der Schwerpunkt auf dem EMV-Aspekt in Bezug auf die HW-Komponente und die HW-Architektur. Die wichtigsten Dokumente in diesem Schritt sind:

- HW-SW-Schnittstelle
- HW-Sicherheitskonzept
- Architektonischer Entwurf auf HW-Ebene
- Analyse der gemeinsamen Ursache auf HW-Ebene
- Analyse der Metrik der HW-Architektur
- SW-Sicherheitskonzept
- Architektonischer Entwurf auf SW-Ebene
- SW-Einheit Entwurf
- Analyse der gemeinsamen Ursache auf SW-Ebene

Auf jeder Entwicklungsebene wird in der Validierungsphase (rechte Seite des V-Zyklus) sichergestellt, dass sämtliche Anforderungen korrekt umgesetzt werden und kein unangemessenes Risiko verbleibt. EMV-Tests zeigen auf jeder Ebene, ob die Architektur ausreichend robust gegen EMV-Ereignisse ist. Wenn es sich bei einem Test um Nok (Fail) handelt, muss ein Änderungs- und Problemmanagementprozess angewandt werden. Dieser Prozess wird zur Verfeinerung/Ergänzung von Anforderungen, zur Verfeinerung/Ergänzung von Testfällen oder zur Änderung von Systemkomponenten verwendet. Die wichtigsten Dokumente in diesem Schritt sind:

- Testfälle und Testergebnisse auf HW-Ebene
- Testfälle und Testergebnisse auf SW-Ebene
- Testfälle und Testergebnisse auf Systemebene
- Testfälle und Testergebnisse auf Fahrzeugebene

5.10.9. Bewertung von Störfestigkeitsprüfungen

A) Funktionszustandsklassifizierungen in den klassischen EMV-Normen:

Definition der Funktionszustände:

- a) Zustand I**
Die Funktion verhält sich während und nach der Prüfung wie vorgesehen.
- b) Zustand II**
Die Funktion verhält sich während der Prüfung nicht wie vorgesehen, kehrt aber nach der Prüfung automatisch in den Normalbetrieb zurück.
- c) Zustand III**

Die Funktion verhält sich während der Prüfung nicht wie vorgesehen und kehrt nicht in den Normalbetrieb zurück, ohne dass der Fahrer/Beifahrer eingreift, z. B. indem er das Fahrzeug abstellt/anzulässt oder den Zündschalter betätigt, nachdem die Störung beseitigt wurde.

d) Zustand IV

Die Funktion verhält sich während und nach der Prüfung nicht wie vorgesehen und kann nicht ohne weitergehende Eingriffe, wie z. B. das Abklemmen und Wiederanschießen der Batterie oder der Stromzufuhr, in den ordnungsgemäßen Betrieb zurückgeführt werden. Die Funktion darf durch die Prüfung keinen dauerhaften Schaden erlitten haben.

Für die Prüfungen von autonomen Gesamtsystemen ohne Fahrer als Rückfallebene wäre hier als Ergebnis nur der Zustand I akzeptabel. Diese gilt dann auch für alle anzuwendenden Prüfschärfgrade.

Wie dieser Zustand I unter EMV-Einwirkung erreicht werden kann, ist im Zuge der funktionalen Sicherheitsbetrachtung zu ermitteln. Für die Bewertung der Immunität gilt hier nur das Ergebnis, auch wenn dieses über interne Sicherheitsmechanismen wie redundante Systeme erreicht wird.

Im Gegensatz zu den bisherigen Klassifizierungen I – IV muss für sicherheitsrelevante Systeme der Systemzustand immer bekannt sein (Defined State), da sie Teil der funktionalen Sicherheitsbetrachtungen sind. Nur im Rahmen der Sicherheitsbetrachtungen festgelegte Systemzustände können Ergebnisse von EMV-Prüfungen sein. Eine Bewertung mit den bisherigen Kriterien „verhält sich nicht wie vorgesehen“ ist hier nicht zulässig.

B) Definition der Funktionszustände in der ECE R10:

Die ECE R10 umfasst in der derzeit gültigen Revision 6 keine Assistenzsysteme mit autonomen Verhalten. Das wird aktuell für die zukünftige Revision 7 diskutiert.

In der typzulassungsrelevanten Norm sind für Immunitätstests verschiedene Prüfungen mit entsprechenden Funktionsstandklassifizierungen aufgeführt. Beispielhaft soll hier die Prüfkfiguration

- verbunden mit dem Niederspannungsnetz

betrachtet werden. Während der Immunitätsprüfungen erfolgt die Überwachung der festgelegten Funktionszustände. Diese müssen eingehalten werden. Damit gilt hier im Vergleich zu den oben aufgeführten Zustandsklassifikationen immer Zustand I.

Die alleinige Zulassung von Zustand I als Kriterium für eine bestandene Störfestigkeitsprüfung entspricht zwar den Anforderungen für die funktionale Sicherheit. Allerdings sind hier für die Prüfungen nur jeweils wenige zu überwachende Fehlerkriterien aufgeführt. Dieser Umfang deckt aus Sicht der funktionalen Sicherheit nur einen Teil der denkbaren Fehlerszenarien ab. So werden im Lademodus auf Fahrzeugebene nur die Funktion der Parkbremse und das Losfahren des Fahrzeuges als relevante Fehlerfälle betrachtet. Dies erfolgt nur für einen Testfall mit einem Ladestrom und einem definierten Ladungsbereich der Batterie.

Weiterhin sind in den Festlegungen der Prüfschärfen Unterschreitungen von Prüfpegeln teilweise zulässig. So muss bei der Einstrahlung mit elektromagnetischen Felder auf den Prüfling (ALSE-Verfahren) der geforderte Prüfpegel von 30 V/m nur für 90 % des Frequenzbereichs von 20 – 2.000 MHz eingehalten werden. Für den verbleibenden zehnprozentigen Bereich gelten dann minimal 25 V/m. Sollte für ein System die Fehlergrenze bei dieser Feldstärke für bestimmte Frequenzen liegen, lassen sich die Fehler unter Umständen nicht sicher nachweisen, da der Frequenzbereich der zulässigen Unterschreitung nicht genauer definiert ist.

5.11. Offene Punkte

Die Sicherstellung der Anforderungen zur funktionalen Sicherheit durch die EMV-Messungen ist derzeit in den Normen im Fahrzeug nicht immer ausreichend abgedeckt. Einmal ergeben sich durch ökonomische Zwänge Testlücken, andererseits lassen sich die FailOp3-Systeme in den Prüflaborumgebungen oft nicht in der normalen Konfiguration prüfen. Die Umgebung in

geschirmten Kabinen kann unplausible Signale hervorrufen, die eine autonome Funktionsausführung nicht ermöglichen.

Der erste Punkt wird sich nicht vollständig vermeiden lassen, da EMV-Messungen immer statistischen Schwankungen unterliegen und somit eine hundertprozentige Testabdeckung nicht gewährleistet wird. Der letzte Punkt kann mittels der Diagnosefunktionen und spezieller Prüfmodi angegangen werden.

Eine weitere Problematik der Sicherheitsbetrachtung ergibt sich aus den Lebenszyklusanforderungen. So werden z.B. Alterungseffekte nicht im normalen EMV-Prüfumfang mit abgedeckt.

Die Funktionszustandsklassifizierungen für FailOp3-Systeme müssen angepasst werden, da die Aufrechterhaltung der sicherheitsrelevanten Funktion(en) immer gewährleistet werden muss. Minimalanforderung muss je nach System der Übergang in den Fail Safe oder Fail Operational Mode sein. Ein Verlassen der spezifizierten Modi oder Funktionen kann nur ein Nichtbestehen der Prüfungen zur Folge haben.

6. Der Demonstrator

6.1. Beschreibung des Demonstrators

Da ein Großteil der EMV-Absicherung auf Steuergeräteebene erfolgt, wurde für die Analysen im Projekt eine Front-Kamera-Applikation gewählt (Abbildung 14). Diese bildet einen Teil eines Assistenzsystems, das den Bereich vor dem Fahrzeug überwacht. Für das gesamte ADAS würden zur vollständigen Absicherung noch weitere Sensortypen wie Radar oder Lidar eingebunden und deren Ergebnisse per Sensorfusion plausibilisiert. Da man sich dann aber schon auf der Systemebene befindet, da diese Einheiten oft von verschiedenen Zulieferern stammen, wurde nur ein Sensortyp für die Untersuchungen gewählt.

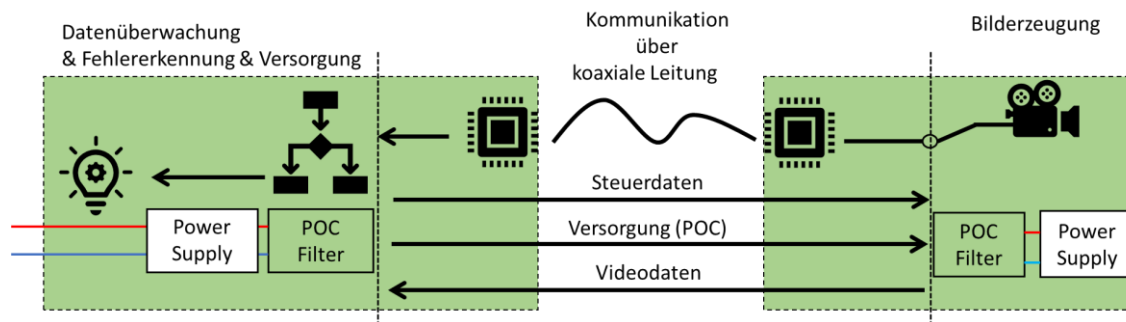


Abbildung 14 Schematische Darstellung des Demonstrators

Die Front-Kamera-Einheit besteht aus einer Hauptplatine, die die Versorgung, die (Bild)Datenverarbeitung und die Fehlererkennung gewährleistet. Hauptbestandteile sind der Deserializer-Chip zur Verarbeitung der empfangenen Videodaten und der Prozessor für die Auswertung sowie die Spannungsregelung für Haupt- und Kameraplatine. Der Verbauort ist im Fahrzeuginnenraum. Davon abgesetzt über eine koaxiale Verbindung gibt es die Kameraeinheit. Diese verfügt über den Imager-Chip und den Serializer für die Datenübertragung. Über das koaxiale Kabel erfolgt

- die Übertragung der Videodaten von der Kamera- zur Haupteinheit (Vorwärtskanal),
- die Übertragung der Systemdaten von der Kamera- zur Haupteinheit,
- die Übertragung der Steuerdaten von der Haupt- zur Kameraeinheit (Rückwärtskanal),
- sowie die Versorgung der Kameraeinheit von der Haupteinheit aus mittels Power over Coax (POC).

Funktional nimmt der Imager-Chip ein Bild auf und sendet es über eine parallele Datenverbindung an den Serializer. Dieser serialisiert die Videodaten, erzeugt Sicherheitsmerkmale wie einen CRC und fügt diese den Bilddaten hinzu. Der Deserializer empfängt den Datenstrom, plausibilisiert ihn und kann diesen an eine weiterverarbeitende Einheit weiterleiten. Es erfolgen, wenn notwendig, Fehlerkontrolle und sogar Korrektur. Fehler in der Datenübertragung werden per Diagnose überwacht.

Die maßgebliche Betrachtung der Sicherheitsaspekte für das System erfolgt anhand der Kommunikationsverbindung mittels SerDes-Anwendungen.

6.2. SerDes-Datenübertragung

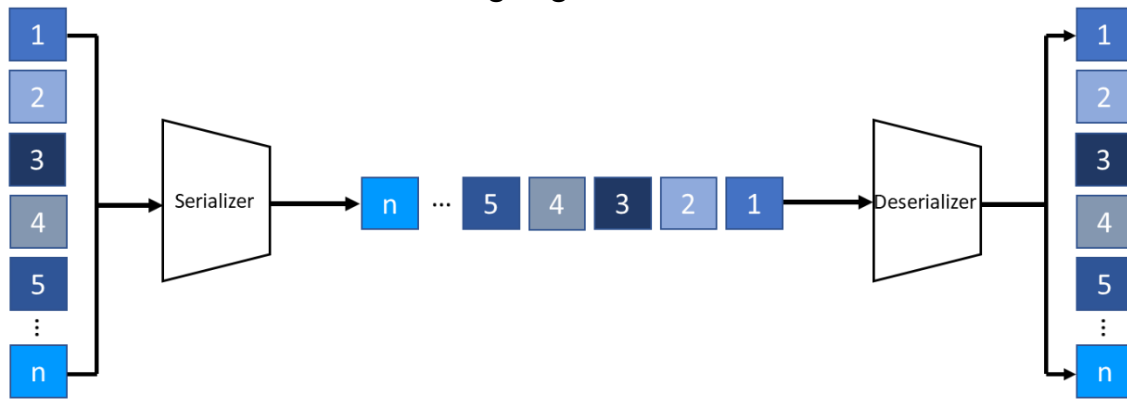


Abbildung 15 Übersicht zur SerDes-Datenübertragung

Die Bezeichnung SerDes kommt aus der Funktion der Datenübertragung. Die parallele Datenausgabe des Imagerchip wird durch den Serializer in einen sequentiellen Datenstrom umgewandelt, der zum Deserializer übertragen wird. Im Deserializer werden die Daten dann wieder für eine parallele Ausgabe, z.B. an einen Mikrocontroller, aufbereitet. Die beiden SerDes-Systeme verfügen über eine Datenrate im Gigabit-Bereich für die Videodaten. Die Videodaten werden zusammen mit Steuerdaten von der Kamera zur Hauptplatine übertragen. Von der Main-ECU können Steuerdaten im Megabit-Bereich zur Kamera übertragen werden. Die hier verwendeten Systeme umfassen einen Simplex-Videokanal auf Basis der Kodierung und Dekodierung von Datensymbolen und einen Duplex Steuerkanal auf Basis von UART oder I2C. Der Steuerkanal wird zum Lesen und Schreiben von Registern sowohl im Serializer als auch im Deserializer verwendet. Die beiden Systeme arbeiten mit NRZ-Übertragung. Damit entspricht die analoge Bandbreite der halben Übertragungsrate.

SerDes- Übertragungsraten	Datenraten Forward Channel (Videodaten)	Datenraten Reverse Channel (Steuerdaten)
Datenraten	4 bis 6 Gbit/s	50 bis 187 Mbit/s

Tabelle 14 Datenraten SerDes-Systeme

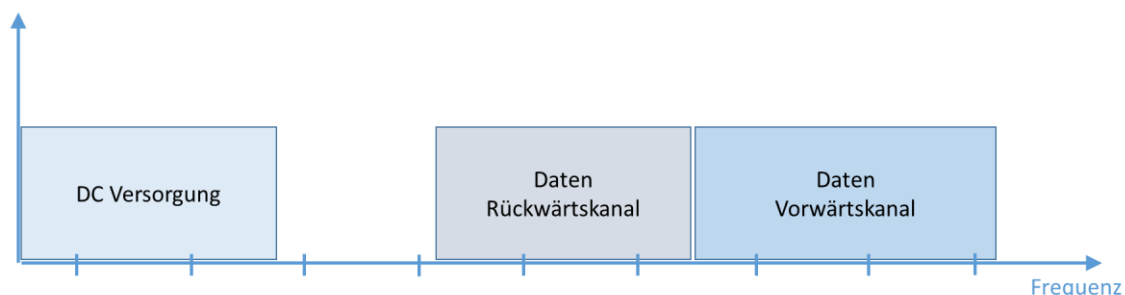


Abbildung 16 Darstellung der Trennung der Übertragungsfrequenzbereiche auf der Koax-Leitung

Die Datenraten sind einstellbar, aber nach der Systemkonfiguration fix. Die Trennung der über die gleiche Leitung übertragenen Daten und der Versorgung erfolgt im Frequenzbereich (Abbildung 16). Dazu werden die Daten in die jeweilige Richtung mit verschiedenen Datenraten übertragen und die Versorgung zusätzlich über Filter im Frequenzbereich in der Bandbreite begrenzt. Für den Hauptkanal stimmt diese Betrachtung formal nicht ganz, da sich die Frequenzbereiche für den Hin- und Rückkanal je nach gewählten Datenraten geringfügig überschneiden können.

Bei der sicheren Auslegung von Highspeed-Kommunikationssystemen sind die Parameter des Kanals ein wichtiges Kriterium. Es existieren für die Systeme Vorgaben. Diese umfassen für

die Kanaldefinitionen nach Abbildung 17 Auslegungskriterien auf Basis von Impedanz und S-Parametern. Diese umfassen folgende Größen:

- Frequenzbereiche für die Anforderungen
- Systemimpedanz mit zulässigen Abweichungen
- Einfügedämpfungen für die Signaldämpfung im Kanal
- Rückflusdämpfungen für die Signalreflexionen
- Angaben für die Verkopplungen mit breitbandigen und schmalbandigen Signalen (Crosstalk)
- Link Margin (definiert Spannungspegelreserven für eine fehlerfreie Datenübertragung)

Ein konformes SerDes-System für den Hauptkanal muss die gesamte Pin-to-Pin-Kanalspezifikation, einschließlich der S-Parameter-Kurven, Crosstalk-Spezifikation und die Link-Margin-Anforderungen, erfüllen. Diese Parameter müssen in der Konzeptphase mit definiert, in der Hardwareentwicklung sichergestellt und in der Testphase validiert werden. Die Einhaltung dieser Vorgaben bestimmt die Robustheit des Systems mit. Das umfasst das Design der Leiterplatten, die Auswahl passender Komponenten für den Kanal und die Beschaltung der Kommunikationshalbleiter.

Die verwendeten SerDes-Links sind herstellerspezifisch. Es gibt immer nur einen Anbieter für die Halbleiter, so dass sich hier keine weiteren Varianten für die Auslegung ergeben.

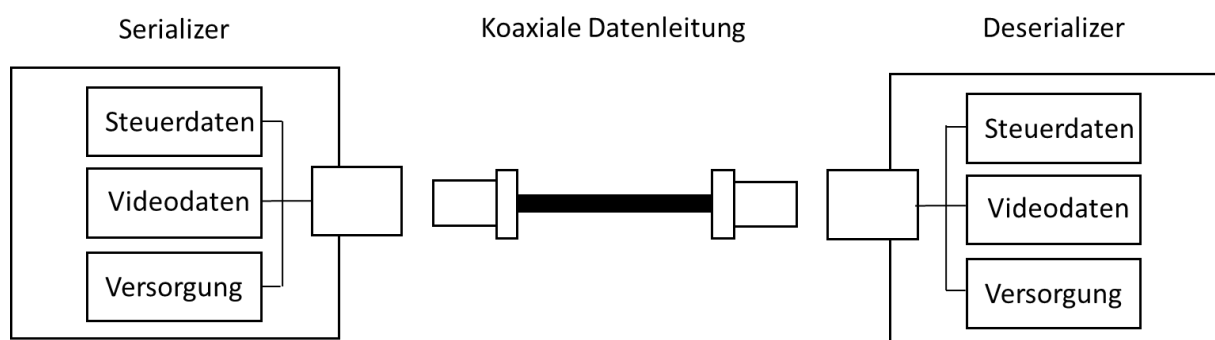


Abbildung 17 Kanal Definitionen am Beispiel Hauptkanal ohne POC und DC-Entkopplung

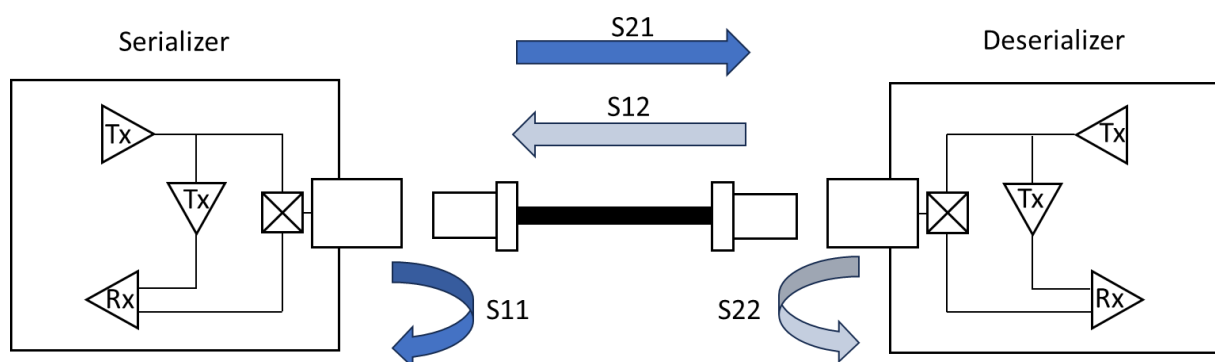


Abbildung 18 Kanal S-Parameter Definitionen

Anhand der funktionalen Sicherheitsbetrachtung ist für die Funktion des Demonstrators ein maximales ASIL D ermittelt worden. Beide Kommunikationssysteme sind vom jeweiligen Hersteller auf ein ASIL B ausgelegt. Daher erfolgt eine ASIL-Dekomposition ASIL B(D) auf Basis einer redundanten Auslegung der Kommunikation. Der Hauptkanal ist als nominaler Übertragungsweg aktiv. Sollte durch den Störeintrag die Kommunikation über ein akzeptables

Maß hinaus beeinflusst werden, übernimmt Rückfallkanal mit einer separaten Leitung die Datenübertragung. Durch die Realisierung der Redundanz mit technisch unterschiedlichen Systemen wird eine höhere Ausfallsicherheit erreicht, da davon auszugehen ist, dass die SerDes-Links auf einen Störeinfluss unterschiedlich reagieren.

7. Eingesetzte Kommunikationssysteme

Da die Kommunikation als Beispielanwendung des Demonstrators für die Untersuchungen im Rahmen des Projektes genutzt wird, soll hier eine detaillierte Betrachtung erfolgen.

7.1. SerDes Kanal A – Eigenschaften zur Einhaltung der Anforderungen der funktionalen Sicherheit

7.1.1. SerDes Kanal A – Sicherheitsmechanismen

1. Erkennung von Fehlern der Verbindung (Line-Fault Detection)

Die Erkennung von folgenden Verbindungsfehlern:

- a) Kurzschluss nach Masse
- b) Kurzschluss nach Versorgungsspannung
- c) offene Verbindung

erfolgt durch den Deserializer an der ECU durch eine spezielle Beschaltung.

Für Systeme mit POC ist es zusätzlich notwendig, die Fehler „Kurzschluss nach Masse“ und „Kurzschluss nach Versorgungsspannung“ abzusichern, um Kurzschlussströme oder Überspannungen zu vermeiden. Dazu sind spezielle Versorgungsbausteine notwendig. Diese bieten Schutz gegen die Überspannungen und -ströme und können diese Ergebnisse auch kommunizieren.

2. Bewertung der Link-Qualität

Das System verfügt über eine bidirektionale Diagnosefunktion, die es ermöglicht, die genutzten Schnittstellen und Kabel zu testen. Dies funktioniert sowohl während der Entwicklung als auch beim Einsatz im Feld und bietet eine hervorragende Felddiagnose: So bietet das Eye-Mapping-Tool im Wesentlichen eine eingebettete Sampling-Scope-Funktionalität, während das Link-Margin-Tool die minimale Sendeamplitude messen kann, die für eine fehlerfreie Verbindung in beide Richtungen erforderlich ist. Die Möglichkeiten Entzerrung (Equalization) und Preemphasis sind Werkzeuge zur Kompensation von Signalverschlechterungen. Bei der Preemphasis handelt es sich um eine Verarbeitung auf der Sendeseite und bei der Entzerrung um eine Verarbeitung auf der Empfangsseite. In beiden Fällen wird das Signal gefiltert, um die durch das Kabel verursachte Signalverschlechterung zu kompensieren und so die Bitfehlerrate zu senken.

3. Tunneling Modus in der Datenübertragung

Im Tunneling-Modus wird der gesamte Bilddateninhalt ohne Änderungen über die serielle Verbindung übertragen. Anders als im Pixel-Modus wird die empfangene CSI-2-Nutzlast nicht dekodiert. Unveränderte CSI-2-Daten werden in kleinere Datenpakete aufgeteilt, die gekapselt und mit CRCs geschützt über die Verbindung transportiert werden. Dies bietet eine durchgängige Datenintegrität, die für ADAS-Fahrzeuge entscheidend ist.

4. Erkennen von Bitfehlern in der Datenübertragung

Jedes Paket (außer Idle- und Acknowledge-Paketen) kann durch einen 16-Bit-Paket-CRC geschützt werden. Jeder Pakettyp kann individuell konfiguriert werden, um Paket-CRC zu aktivieren oder zu deaktivieren. Standardmäßig verfügen alle Kanäle mit geringer Bandbreite über Paket-CRC.

Da Acknowledge-Pakete keine Daten enthalten und der Header wiederholt wird, ist CRC unnötig. Obwohl der Videokanal in den Standardeinstellungen Paket-CRC deaktiviert, um die nutzbare Bandbreite zu maximieren, ist Videozeilen-CRC (ein 32-

Bit Code am Ende eines jeden DE- oder HS-Impulses) standardmäßig aktiviert, um die Daten zu schützen.

Das Polynom des 16-Bit-Paket-CRC-Generators lautet: $x^{16} + x^{15} + x^2 + 1$.

5. Control-Channel Retransmission im Fehlerfall

Kommunikationskanäle mit Steuerdaten (I2C/UART, GPIO, SPI) haben eine relativ geringe Bandbreite, erfordern aber den höchsten Schutz der Datenintegrität. Ein optionales automatisches Verfahren zur Wiederholung der Paketübertragung, Automatic Repeat Request (ARQ), wird hier eingesetzt. ARQ arbeitet in Verbindung mit 16-Bit-Paket-CRC, um zu erkennen, ob Pakete mit oder ohne Fehler empfangen werden.

Die Pakete werden auf der Sendeseite mit einer 2-Bit-Sequenznummer versehen, und auf der Empfängerseite wird bei erfolgreichem Empfang jedes Datenpakets eine Quittung gesendet. Die Pakete werden auf der Sendeseite gespeichert, bis sie bestätigt werden. Wenn die Bestätigung nicht in einem vorbestimmten Intervall eintrifft oder die Sequenznummer der Bestätigung nicht mit dem erwarteten Wert übereinstimmt, wird das an der Spitze der Warteschlange wartende Paket automatisch erneut übertragen.

6. Forward Error Correction

Das Protokoll enthält eine optionale Vorwärtsfehlerkorrektur (FEC). Diese verwendet eine Reed-Solomon-Kodierung und fügt ein 6-Bit-Korrekturwort zu allen 121 Datenbits hinzu. Die FEC benötigt einen zusätzlichen festen Bandbreiten-Overhead von 6,7% bei einer Reduzierung der Bit-Fehlerrate (BER) von $1e^{-15}$ auf $1e^{-55}$. Die FEC muss im Serializer und im Deserializer unterstützt werden. Es kann pro Datenpaket ein Fehlerbit korrigiert werden.

7. Error Generator

Alle Geräte verfügen über einen Fehlergenerator (ERRG), der sich hinter dem Paket-Scheduler befindet und die Auswirkungen von Bitfehlern auf die Verbindung simuliert. Dieser wird in erster Linie verwendet, um Reaktionen auf Systemebene auf Bitfehler in der seriellen Verbindung zu testen, einschließlich der ASIL-Fehlerbehandlung in sicherheitsrelevanten Systemen. Der ERRG kann auch zur Validierung interner Selbsttests (z. B. PRBS-Test) verwendet werden.

Der Fehlergenerator befindet sich in jedem PHY nach dem Scheduler und dem Packetizer. Wenn er im Serializer aktiviert ist, werden Bitfehler zum Vorwärtskanal hinzugefügt; wenn er im Deserializer aktiviert ist, werden Bitfehler dem Rückwärtskanal hinzugefügt. Bitfehler werden durch das Vertauschen von Bits im Bitstrom nach der Paketbildung und Kodierung erzeugt. Es gibt also keine Kontrolle darüber, welche Kanäle (z. B. Video, RMII) betroffen sind.

7.1.2. Anwendung der Diagnosefunktionen für die Systemauslegung

Je nach Grad der Beeinflussung treten bei Kommunikationssystemen zuerst einzelne Bitfehler auf, die sich mit zunehmenden Störeinfluss häufen und letztendlich bricht der Link ab.

Für die Systemauslegung sind die oben genannten Anforderungen an die Übertragungsstrecke einzuhalten. Die Link Margin ist wichtige Messgröße bei der Systementwicklung und ein wichtiger Bestandteil der Verbindungsvalidierungstests. Wenn die Verbindung aufgebaut ist, wird die Sendeamplitude in kleinen Schritten reduziert, bis im Empfänger Bitfehler erkannt werden. Die Differenz zwischen der nominalen Sendeamplitude

und der kleinsten Amplitude, die fehlerfrei funktioniert, wird als Link Margin bezeichnet. Die Link Margin bietet somit eine Vorgabe für die Grenzen der Systemauslegung.

Während des Betriebs und für Tests können die horizontalen und vertikalen Öffnungen der Augendiagramme mit einem eingebauten horizontalen und vertikalen Augenöffnungsmonitor (Eye-Opening Monitor – EOM) überwacht werden. Der EOM gibt Zahlen aus, die die Breite und Höhe des Datenauges darstellen. Er kann so programmiert werden, dass er regelmäßig im Hintergrund läuft und eine Unterbrechung auslöst, wenn die Augenöffnung einen vorprogrammierten Wert unterschreitet. Dieser Wert kann in der Systemauslegung festgelegt werden. Für die Prüfungen kann er bereits vor dem Auftreten von Fehlern als Threshold-Marker genutzt werden.

Bei einigen PHY's, die die Vorwärtsfehlerkorrektur unterstützen, kann die Vor-FEC-Bitfehlerrate (BER) überwacht werden. Dies ist ein nützlicher Frühindikator für eine elektrische Verschlechterung der Verbindung. Bitfehler, die der FEC nicht korrigieren konnte, werden ebenfalls erkannt.

Diese drei Möglichkeiten können genutzt werden, um eine Verbindung zu überwachen. Bereits vor dem Auftreten von Fehlern können per Diagnose Maßnahmen getroffen werden, um die Datenübertragung zu schützen.

Die Erkennung von Fehlern bei der Datenübertragung ist - unabhängig vom Fehler - immer vergleichbar aufgebaut (Abbildung 19). Nahezu alle möglichen Fehler können auf einem Interrupt gelegt werden und der Fehler wird in einem Register gespeichert. Einige Fehler lassen sich über Fehlerzähler konfigurieren, d.h. erst ab einem bestimmten Zählerwert erfolgt eine Signalisierung.

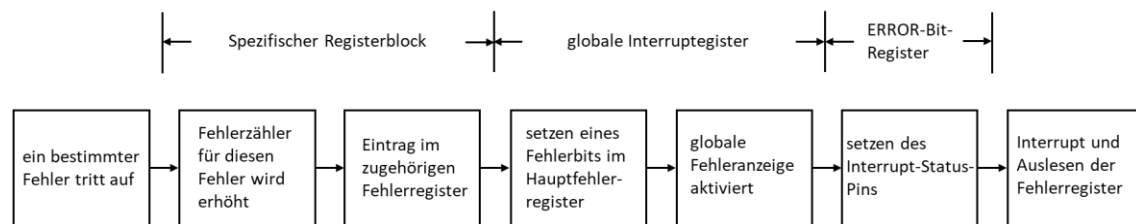


Abbildung 19 Fehlerdiagnose für das SerDes-Interface des Hauptkanals

7.1.3. Zusammenfassung ASIL-Konformität:

Das System für den Hauptkanal ist ASIL-B-konform durch folgende Eigenschaften:

- Ende-zu-Ende-Datenintegrität durch CRC im Tunneling-Modus
- FEC zum Schutz von Forward Video und Steuerkanaldaten
- CRC-Schutz von Seitenkanal- und Videodaten
- Punkt-zu-Punkt-Verbindung

Höhere Anforderungen an die funktionale Sicherheit können mit zusätzlichen Maßnahmen wie Timeout-Monitoring und Frame-Countern erreicht werden.

7.2. SerDes Kanal B – Eigenschaften zur Einhaltung der Anforderungen der funktionalen Sicherheit

7.2.1. SerDes Kanal B – Sicherheitsmechanismen

1. Erkennung von Fehlern der Verbindung (Line-Fault Detection)

Die Erkennung von folgenden Verbindungsfehlern:

- d) Kurzschluss nach Masse
- e) Kurzschluss nach Versorgungsspannung
- f) offene Verbindung

erfolgt durch den Deserializer an der ECU durch eine spezielle Beschaltung.

2. Bewertung der Link-Qualität

LOCK-Signal zeigt an, dass die Verbindung vom Serializer zum Deserializer aufgebaut ist und der Deserializer sich auf den Datenstrom synchronisiert hat. Diese Funktion überwacht auch die Clock Recovery aus dem Datenstrom und kann vom Prozessor in der ECU überwacht werden. Die Funktion Adaptive EQ Level misst die Qualität der Verbindung und kann diese über die I2C-Schnittstelle ausgeben. Im Debug Mode können über das Pinpaar CMLOUT die Augendiagramme ausgegeben werden.

3. Monitoring Interrupts

Zahlreiche Statusregister lassen sich auf externe GPIO oder Interrupt-Pins legen. Neben den Daten lassen sich hier für einige Devices auch die Spannungsebenen und die Temperatur überwachen. Über die I2C-Schnittstellen an DES und SER lassen sich Register auslesen und beschreiben.

4. Erkennen von Bitfehlern in der Datenübertragung

Sowohl der Forward als auch der Backward Channel haben eine CRC-Kontrolle, die Fehler erkennt und anzeigt. Werden Bitfehler in der Datenübertragung erkannt, werden die Register schreibgeschützt, um fehlerhafte Einträge zu vermeiden.

5. Forward Error Correction

Camera Serial Interface Error Correction Code (CSI-ECC) Fehler beziehen sich auf fehlerhafte CSI-Datenpakete, die um 1 oder 2 Bit von ihrem korrekten Wert abweichen. Fehler, die um 1 Bit abweichen, werden automatisch korrigiert. Fehler, die 2 Bit Abweichung aufweisen, werden erkannt, aber nicht korrigiert.

6. Pattern Generator

Einfacher Ansatz für die Fehlersuche, Videodaten zu erzeugen, ohne eine externe Quelle nutzen zu müssen. Die so erzeugten Daten lassen sich auf die Zielapplikation (Frame Rate, Auflösung, Datentyp, ...) anpassen.

7. Error Generator (BIST)

Überprüft die Datenintegrität zwischen SER und DES in beide Richtungen. Weiterhin können auch am Deserializer Testpattern erzeugt werden, um ohne Link die Verbindung zur Anzeige zu prüfen. Der BIST erzeugt Pseudorandomdaten und ermöglicht so die Ermittlung von Bitfehlerraten.

7.2.2. Umsetzung von Sicherheitsmechanismen

Bei der Spezifikation von Sicherheitsanforderungen ist die Rückverfolgbarkeit (Traceability) ein wichtiges Merkmal. Aus dem TSC werden die Anforderungen dafür abgeleitet. Die Sicherheitsanforderungsspezifikation sollte folgende Aspekte berücksichtigen:

- die Spezifikation mit dem Management von Sicherheitsanforderungen nach ISO 26262 Teil 8-6
- die Spezifikation der System- und Hardwareebene
- Hardware Software Interface
- ggf. spezielle Hardwaredesignspezifikationen
- Zeitvorgaben der Systemebene (Ausführungszeit und Reaktionszeit)
- Schnittstellen zu externen Systemen
- alle Betriebszustände (inkl. Ausfall)

Für die Sicherheitsintegrität sind Mechanismen umzusetzen, die die folgenden Punkte betreffen:

- Umsetzung des sicheren Zustands inklusive des Erreichens, Erhaltens und Verlassens
- Fehlerdetektion und -handling
- Selbsttests
- notwendige Funktionen für die Prüfungen in der Verifikationsphase
- mögliche Modifikationen nach der Produktentwicklung (Lebenszyklus)

7.3. Diagnosefunktionen und Fehlererkennung

Für die Sicherheitsbetrachtungen ist eine wesentliche Voraussetzung, dass Zustände der Kommunikationsverbindungen und mögliche Fehler sicher erkannt werden. Diese Informationen müssen gesammelt und den Sicherheitsmechanismen zur Verfügung stehen. Die entsprechenden Wirkketten im Fehlerfall müssen nach der Erkennung von Beeinflussungen anspringen und dafür sorgen, dass der Systemzustand definiert bleibt.

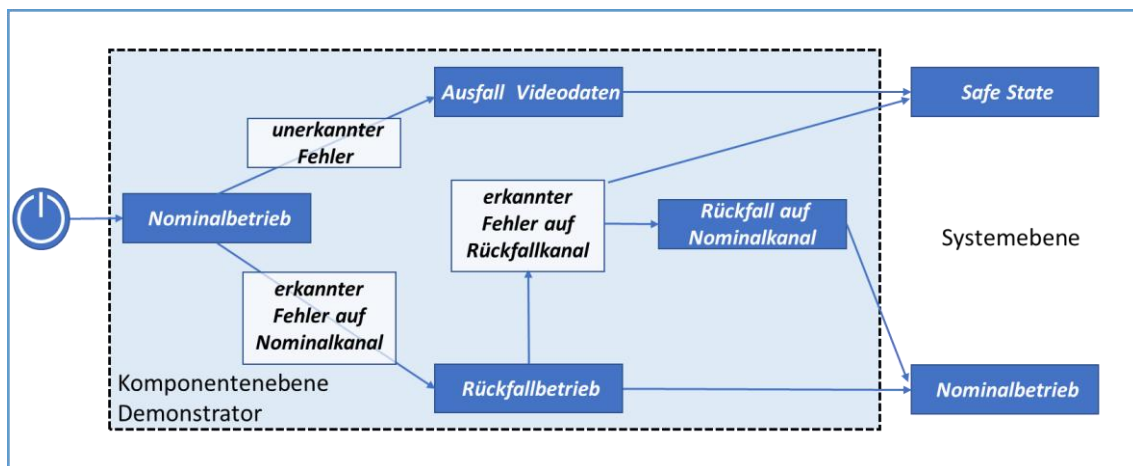


Abbildung 20 Schematische Darstellung des Verhaltens der Datenübertragung im Fehlerfall

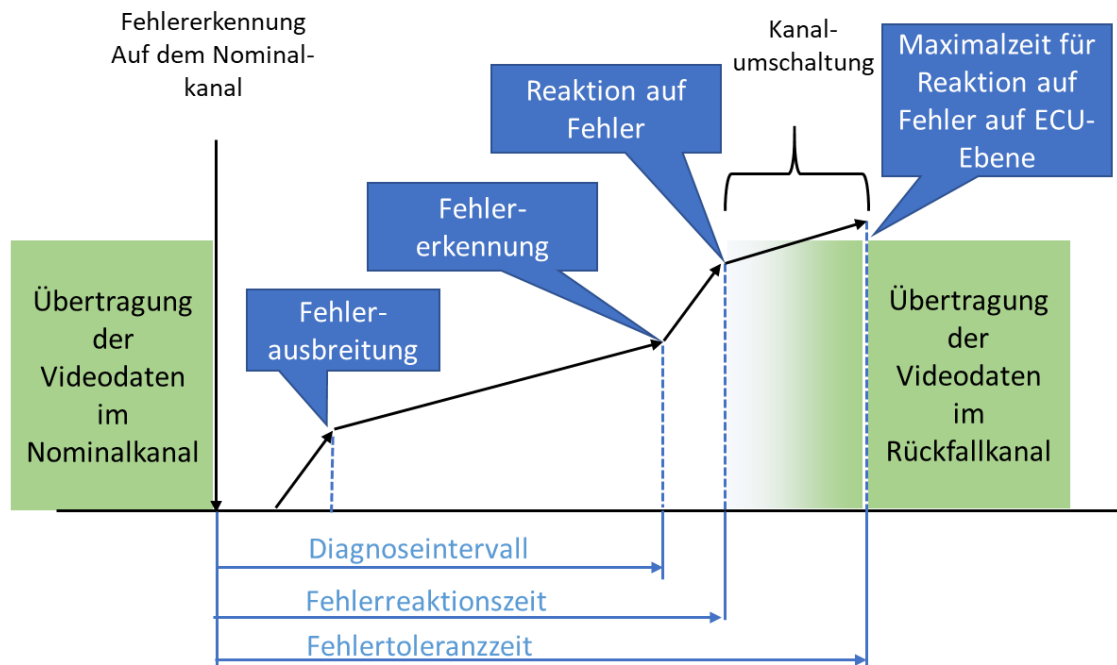


Abbildung 21 Fehler und Zeitvorgaben der Diagnose und Sicherheitsmechanismen auf ECU-Level

Ein Beispiel hierfür ist die Umschaltung vom Nominalkanal auf den redundanten Zweig, nachdem die Datenübertragung auf der primären Übertragungsstrecke durch EMV-Einfluss gestört wurde. Im Konzeptions- und Entwurfsprozess wurde hierfür eine Metrik entwickelt, die die möglichen Zustände und deren Übergänge definiert. Eine schematische Darstellung dafür ist in Abbildung 20 zu finden. Eine mögliche Fehlerkette entsteht durch eine Beeinflussung der Kommunikation auf der physikalischen Ebene, z.B. das „Umkippen“ eines Bits. Ob sich aus diesem Ereignis, dem *Fault* ein *Error* auf Steuergeräteebene ergibt oder nicht, hängt von der Art und der Häufigkeit der Beeinflussung ab. Kritisch für die Funktionsausübung wird der Fall, wenn sich aus *Fault* und *Error* auf der ECU ein *Failure* im System ergibt, auf den reagiert werden muss.

Weiterhin müssen für die Fehlererkennung und -behandlung Zeiten definiert sein. Diese Zeiten leiten sich aus den Anforderungen des Gesamtsystems ab. Beim Test auf Komponentenebene können aber nur die Reaktionszeiten des Steuergerätes erfasst werden. Der Zusammenhang hierzu ist in Abbildung 21 dargestellt. Im Beispielfall kann die Zeitdauer des Umschaltens während der Messungen überwacht werden. Die Zeitangaben auf ECU-Ebene sind in die des Systems eingebettet. Und diese des Systems sind in die des Fahrzeugs eingebettet. Für das Projekt müssen Annahmen für die Timings getroffen werden. Die Fehlertoleranzzeit ist durch die Systemspezifikation gegeben. Das übergeordnete System muss feststellen, ob ein sicherer Zustand erreicht wurde oder nicht.

Die Diagnoseabdeckung muss für Funktionen mit ASIL bestimmten normativen Vorgaben entsprechen (Tabelle 13). Daher sollte der Diagnoseumfang bereits in einem früheren Stadium der Entwicklung definiert werden.

Auf Steuergeräteebene lässt sich die Diagnose leicht umsetzen und überwachen. Bei Betrachtung des Gesamtfahrzeuges ist dieser Schritt nur noch schwer umzusetzen. Dies ergibt sich aus den Anforderungen der Cybersecurity. Sicherheitsrelevante Funktionen dürfen sich von außen nicht beeinflussen lassen. Daher ist davon auszugehen, dass diese auf der Fahrzeugebene keine Schnittstellen zur Verfügung stellen. Die Verarbeitung der Daten kann zentralisiert erfolgen. Das einzelne Steuergerät hat unter Umständen nicht genug Informationen zur Beurteilung des übergeordneten Systemzustandes.

7.3.1. Failure Injection Tests

Durch physikalisches Testen allein kann nicht sichergestellt werden, dass alle möglichen Fehler auftreten. Es können nicht alle ermittelten Umgebungsbedingungen nachgestellt werden. Die Prüfungen können nur einen bestimmten Umfang abdecken und somit nur die Fehlerwahrscheinlichkeiten reduzieren.

Die Prüfverfahren und deren Bewertung im Bereich der EMV werden unter typischen Bedingungen durchgeführt und unterliegen den Kriterien der Reproduzierbarkeit und der Wirtschaftlichkeit.

Die funktionelle Sicherheit berücksichtigt möglichst alle Risiken unter allen Umweltbedingungen während des gesamten Lebenszyklus. Weiterhin muss das Systemverhalten immer bekannt sein.

Um diese Anforderungen zu berücksichtigen, kann der Testumfang produktspezifisch erweitert werden. Damit können aber nur als besonders kritisch ermittelte Bedingungen der Anwendung betrachtet werden.

Mögliche Maßnahmen zur Erhöhung des Prüfumfanges sind beispielsweise:

- Erhöhung des Prüfniveaus: bekanntes Verhalten des Prüflings über die Grenzwerte hinaus (defined state)
- Testdauer erhöhen für statistisch gesicherte Aussage über das Ausfallverhalten
- Anzahl der Tests erhöhen: unterschiedliche Testaufbauten, Anzahl der Prüflinge, Kombinationen aus beidem, ...

- Variation der Prüfeinstellungen erweitern: Prüfpegel, Modulationen, Einstrahlungswinkel, Feldstärke, ...
- Umweltfaktoren variieren: Feuchtigkeit, Temperatur, Alterung, ...
- erweiterte Diagnosefunktionen implementieren: nicht alles kann unter EMV getestet werden., weil z.B. Fehler nicht eindeutig einer Teilkomponente zuzuordnen sind

Ein generalisierter Ansatz, der das physikalische Testen ergänzen sollte, sind Failure Injection Tests. Fehlerinjektionstests sind die absichtliche Einführung von Fehlern und Störungen in ein System, um dessen Stabilität und Zuverlässigkeit zu überprüfen und zu festigen. Ziel ist die Verbesserung der Systemauslegung im Hinblick auf die Widerstandsfähigkeit unter verschiedenen Fehlerbedingungen. Fehlerinjektionstests werden zwar nur für ASIL-D-Systeme dringend empfohlen, sind aber eine zuverlässige Methode zur Überprüfung der Robustheit und Fehlertoleranz eines Systems unabhängig von seiner Klassifizierung.

Die Hauptziele der meisten Fehlerinjektionstests sind:

- Überprüfung,
- Kalibrierung,
- Validierung.

Mit Hilfe der Fehlereinspeisung ist überprüfbar, ob die Fehlerbehandlungsmechanismen wie angegeben funktionieren. Es kann eine Kalibrierung der Schwellenwerte erfolgen, so dass die Mechanismen immer einen erkannten Fehler melden, wenn ein Fehler aufgetreten ist, aber niemals fälschlicherweise einen erkannten Fehler während des fehlerfreien Betriebs melden. Weiterhin kann eine Validierung der Effizienz der spezifizierten Fehlerbehandlungsmechanismen vorgenommen werden, z.B.:

- Erfassungsbereich,
- Erkennungslatenz (die Zeitspanne zwischen dem Auftreten eines Fehlers und seiner Erkennung),
- Rekonfigurationslatenz (die Zeitspanne zwischen der Erkennung eines Fehlers und der daraus resultierenden Rekonfiguration des Systems).

7.4. Fehler in Kommunikationssystemen

EMV-Einwirkung auf leitungsgebundene Kommunikation führt zu einer Beeinflussung der physikalischen Ebene der Datenübertragung. Die hier genutzten SerDes-Kanäle übertragen die Daten „single ended“ über Coax (50 Ω) und die Qualität der Übertragung lässt sich anhand von Augendiagrammen bewerten (Abbildung 22).

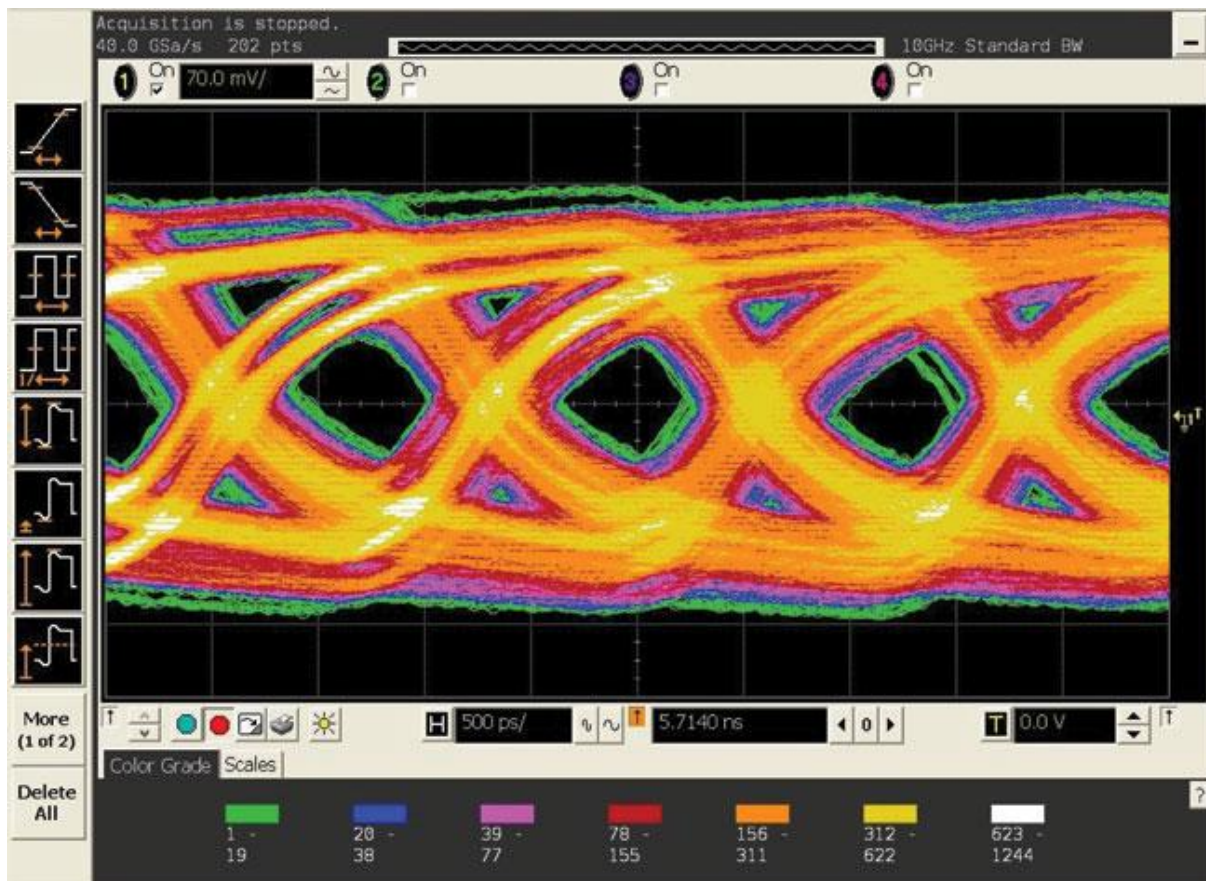


Abbildung 22 Beispiel SerDes Augendiagramm [20]

Unterschreitet die Augenöffnung vorgegebene Schwellen, wird das übertragene Bit nicht richtig vom Empfänger erkannt. Es kann sowohl zu horizontalen Beeinflussungen kommen, dem Jitter, oder zu vertikalen in der Amplitude.

Werden die Daten durch die EMV gestört, kommt es in der Regel zuerst zu Bitfehlern. Diese können sich häufen, bis die Clock and Data Recovery nicht mehr möglich ist. Dann kommt es zu einem Linkabbruch. Während einzelne Bitfehler noch erkannt und teilweise korrigiert werden können, erfolgt beim Linkabbruch erst wieder eine Datenübertragung, nachdem ein neuer Linkaufbau erfolgt ist.

Da die hier verwendeten Kommunikationssysteme die Signale mittels Adaptive Equalization (AEQ) aufbereiten und dieser Prozess dynamisch erfolgt, ergeben sich keine trivialen Zusammenhänge zwischen Signalamplituden und Störeinflüssen. Mittels AEQ werden die Signale an die vom PHY ermittelten Kanaleigenschaften angepasst. Dieser Vorgang erfolgt dynamisch, also mit einer Periodizität von ca. 1 Hz und ist nicht linear.

Bei der Nutzung von POC kann es weiterhin zu einer Beeinflussung der Versorgung kommen. Hier hat das SerDes-System Überwachungsregister implementiert, die kritische Spannungsabweichungen erkennen und speichern.

7.5. Umsetzung im Projekt

Für das Projekt werden hierbei Fehler in die Kommunikationsstrecke eingespeist. Diese Fehlererzeugung erfolgt intern durch einen Fehlergenerator in den SerDes-PHYs. Die beiden Übertragungssysteme verfügen aufgrund ihrer ASIL-Klassifikation über konfigurierbare Fehlergeneratoren.

Für das SerDes-System des Hauptkanals befindet sich der Fehlergenerator im PHY und fügt Bitfehler in den Datenstrom nach der Paketierung und Codierung ein. Der Fehlergenerator im

Serializier beeinflusst damit die Videodaten, der Fehlergenerator im Deserializier die Steuerdaten im Rückkanal.

Der Fehlergenerator kann wie folgt konfiguriert werden:

- Pseudozufälliges oder periodisches Verhalten
- Unterschiedliche Anzahl von Bitfehlern von 1 bis 20
- Rate der Fehlerereigniserzeugung
- Anzahl der Fehlerereignisse pro Aktivierung

Es können somit verschiedene Szenarien simuliert werden, um Diagnose und Systemverhalten zu testen. Nachfolgend sind zwei Beispiele aufgeführt.

1. Pseudozufällige Einzelbit-Flip-Fehler im Videostrom:

- Emulation der Auswirkungen von Transienten, die in die Koaxialleitung des Nominalkanals einkoppeln:
- Erwartetes Verhalten:
Fehler sollten durch den FEC korrigiert werden, der Videostrom sollte auf dem nominalen Kanal laufen, die Diagnose erkennt die Fehler
- Testabdeckung:
Kontrolle der FEC-Fähigkeit, Verifizierung der Diagnose der Fehlerzählregister

2. Kontinuierliche Mehrfach-Bitflip-Fehler im Videostrom:

- Emulation der Auswirkungen der EMI-Kopplung in der Koaxialleitung des Nominalkanals:
- Erwartetes Verhalten:
Fehler sollen erkannt werden, der Videostrom soll auf den Rückfallkanal umschalten, die Diagnose erkennt die Fehler und die Kanalumschaltung, das Steuergerät informiert das System
- Testumfang:
Kontrolle der Kanalumschaltung, Verifizierung der Diagnose der Fehlerregister und der Kanalnutzung, Verifizierung der Rekonfigurationszeit der Kommunikationssysteme auf Steuergeräteebene

8. Funktionale Sicherheitsanalyse des Demonstrators

8.1. Definition des ITEM

Funktionale Anforderungen

Funktionale Anforderungen sind Anforderungen mit Bezug zur Zweckbestimmung des Produkts. Die funktionalen Anforderungen an die hier zu betrachtende Kameraapplikation ist die Aufnahme von Videodaten mit der Kamera ECU und die Übertragung dieser zur Main ECU. Die Kamera soll mit einer Bordnetzspannung betrieben werden und Fehler in der Datenübertragung erkennen und auf diese mit einer Fehleranzeige reagieren. Der Datenkanal soll fehlerabhängig umschaltbar sein und ist daher redundant. Die Definition des ITEM dient als Input für die Sicherheitsanalyse.

Nicht funktionale Anforderungen

Nicht-funktionale Anforderungen umfassen Regelungen beispielsweise zur Zuverlässigkeit und dem Zeitverhalten. Sie sind meist unspezifisch für das Produkt. Eine Unterscheidung ist zwischen funktional und nicht-funktional oft schwierig. Nicht funktionale Anforderungen sind z. B.:

- Einhalten der Zeitvorgaben für die Fahrerwarnung und die Datenkanalumschaltung
- Robustheit

Anforderungen Einsatzbereich

Die Anforderungen aus dem Einsatzbereich ergeben sich aus der Nutzung im Fahrzeug. Im Projekt werden nur die EMV-Anforderungen aus den in der ISO 26262 definierten Prüfverfahren betrachtet.

Gesetzliche Anforderungen

Werden im Projekt nicht betrachtet.

Betriebszustände und Modi

Im Projekt werden nur die Betriebszustände mit Bildübertragung und daraus abgeleitete Fehlerzustände betrachtet.

Bekannte Fehlermodi

Die betrachteten Fehlermodi und Diagnosefunktionen umfassen:

- Übertragungsfehler Videodaten bei Systemstart: no filmed scene
- Übertragungsfehler Videodaten bei Systemausführung:
 1. Loss of filmed Scene
 2. Freezed Scene
 3. Very Bad Quality of Video stream (keine Auswertung möglich)
- Übertragungsfehler Videodaten bei Systemausführung: Bad Quality of Videostream (Auswertung noch möglich)
- Diagnosefähigkeit und Fehlererkennung eingeschränkt

Das ITEM ist ein Frontkamerasystem für eine Level-3-Fahrfunktion (Abbildung 14). Die Kamera überwacht die Fahrzeugumgebung in Fahrrichtung und liefert den Videostream an eine Auswerteinheit. Diese Analyseeinheit bewertet die Bilder für die automatisierten Fahrfunktionen. Die Kameraeinheit muss immer ein aktuelles, auswertbares Bild liefern oder das übergeordnete System über einen Ausfall innerhalb einer vorgegebenen Zeitspanne informieren, damit die Funktionalität von anderen Sensoren mit abgedeckt werden kann, bis der Fahrer nach einer definierten Zeitspanne übernimmt.

8.2. Gefahrenanalyse und Risikobewertung (HARA)

Function	MF Description	Failure modes	P	R	RH	AS	Effect on sys	Scenarios	Effect at the vehicle level	Feared event	S	E	C	ASIL
M.F_01	Film a scene in front of the vehicle	No function	X				No scene filmed	While parking, the filming function is OFF	No video stream for the vehicle	Hit a road user (vehicle/pedestrian)	2	4	3	C
		-		X			No scene filmed	While rolling, the filming function is OFF	No video stream for the vehicle	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-			X		No scene filmed	While rolling in highway, the filming function is OFF	No video stream for the vehicle	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-				X	No scene filmed	In after sales, the filming function is OFF	No video stream for the vehicle	-	1	1	1	QM
		Loss of function	X				Loss of the filmed scene	While parking, the filming function is lost	No video stream for the vehicle	Hit a road user (vehicle/pedestrian)	2	4	3	C
		-		X			Loss of the filmed scene	While rolling, the filming function is lost	No video stream for the vehicle	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-			X		Loss of the filmed scene	While rolling in highway, the filming function is lost	No video stream for the vehicle	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-				X	Loss of the filmed scene	In after sales, the filming function is lost	No video stream for the vehicle	-	1	1	1	QM
		Freezed function	X				Freezed scene	While parking, the filming function is freezed	Video stream freezed	Hit a road user (vehicle/pedestrian)	2	4	3	C
		-		X			Freezed scene	While rolling, the filming function is freezed	Video stream freezed	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-			X		Freezed scene	While rolling in highway, the filming function is freezed	Video stream freezed	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-				X	Freezed scene	In after sales, the filming function is freezed	Video stream freezed	-	1	1	1	QM
		Unusable degraded function	X				Very bad quality of filmed scene	While parking, the filming function is degraded and unusable	Unusable video stream for the vehicle	Hit a road user (vehicle/pedestrian)	2	4	3	C
		-		X			Very bad quality of filmed scene	While rolling, the filming function is degraded and unusable	Unusable video stream for the vehicle	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-			X		Very bad quality of filmed scene	In after sales, the filming function is degraded and unusable	Unusable video stream for the vehicle	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-				X	Very bad quality of filmed scene	In after sales, the filming function is degraded and unusable	Unusable video stream for the vehicle	-	1	1	1	QM
		Unusable degraded function	X				Bad quality of the filmed scene	While parking, the filming function is degraded but usable	No effect	Bad quality of image	0	4	0	QM
		-		X			Bad quality of the filmed scene	While rolling, the filming function is degraded but usable	No effect	Bad quality of image	0	4	0	QM
		-			X		Bad quality of the filmed scene	While rolling in highway, the filming function is degraded but usable	No effect	Bad quality of image	0	4	0	QM
		-				X	Bad quality of the filmed scene	In after sales, the filming function is degraded but usable	No effect	Bad quality of image	0	4	0	QM
		No function	X				Absence of a displayed scene	While parking, the display function is OFF	No video stream displayed	Hit a road user (vehicle/pedestrian)	2	4	3	C
		-		X			Absence of a displayed scene	While rolling, the display function is OFF	No video stream displayed	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-			X		Absence of a displayed scene	While rolling in highway, the display function is OFF	No video stream displayed	Hit a road user (vehicle/pedestrian)	3	4	3	D
		-				X	Absence of a displayed scene	In after sales, the display function is OFF	No video stream displayed	-	1	1	1	QM



Safety Goals

P - Parking, R – Rolling, RH – Rolling Highway, AS – After Sales
S – Severity, E – Exposure, C – Controllability

Abbildung 23 Demonstrator– Auszug Gefahrenanalyse und Risikobewertung (HARA)

Wie bereits in 4.2.1 beschrieben, schätzt die Gefahrenanalyse und Risikobewertung die Wahrscheinlichkeit der Exposition, die Kontrollierbarkeit und die Schwere der gefährlichen Ereignisse im Hinblick auf das Item ein. Diese Parameter werden anhand der ITEM-Funktionen definiert. In Abbildung 23 ist das Vorgehen zu erkennen. Die einzelnen Funktionen werden für verschiedene Einsatzbereiche und Anwendungsszenarios mit Fehlermodi und deren Auswirkung verknüpft. Die Spalten für die Schwere der Auswirkung („Severity“ / S), die Häufigkeit („Exposure“ / E) und die Beherrschbarkeit der Fehlfunktion („Controllability“ / C) enthalten Werte, die von den Fach- und Sicherheitsexperten festgelegt werden. Die Aufsummierung dieser Werte ergibt das ASIL für die Funktion.

Die Ausgabe aus der HARA ist eine Liste von Sicherheitszielen mit zugehörigem ASIL-Level (Tabelle 15). Die Ziele ergeben sich aus den von der Hauptfunktion abgeleiteten Fehlermodi der Risikoanalyse. In Abbildung 23 ist die Hauptfunktion (MF – Main Function), die Aufnahme und Übertragung eines Videostreams an der Fahrzeugfront. Die Sicherheitsziele dienen der Vermeidung der Fehlermodi in der späteren Analyse.

Functions	Description of Function
M.F_01	Film a scene in front of the vehicle
M.F_02	Display the video stream of the infront area of the vehicle
M.F_03	Transmit a video stream from the camera to the vehicle ADAS
C.F_01	Detect failures on image coming from the camera



SG_ID	Failure modes	ASIL
SG_01	No scene filmed	D
SG_02	Loss of the filmed scene	D
SG_03	Freezed scene	D
SG_04	Very bad quality of filmed scene	D
SG_05	Bad quality of the filmed scene	QM

Tabelle 15 Liste von Sicherheitszielen (SG) und deren ASIL

Die HARA ergibt ein maximales ASIL D. Wenn die technische Umsetzung oder andere Gründe dies nicht erlauben, muss auf die Technik der ASIL-Dekomposition (Tabelle 16) zurückgegriffen werden.

Damit wird die Aufteilung redundanter Sicherheitsanforderungen auf Elemente mit ausreichender Unabhängigkeit bezeichnet, die zum gleichen Sicherheitsziel führen. Das Ziel der Dekomposition ist, den ASIL der redundanten Sicherheitsanforderungen zu reduzieren, die den entsprechenden Elementen zugeordnet sind, um einen höheren ASIL der Funktion damit zu erfüllen. Ein Beispiel ist eine Aufteilung einer Teilfunktion mit Anforderung ASIL D in zwei redundante Teilfunktionen mit ASIL B, die als ASIL B(D) bezeichnet werden.

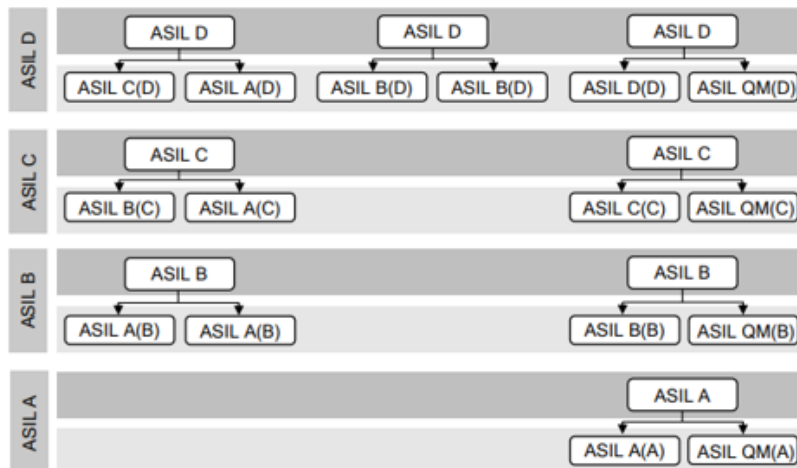


Tabelle 16 Übersicht ASIL-Dekomposition

Für das hier gewählte Beispiel des Frontkamarasystems ist die Dekomposition notwendig, da die für die Videodatenübertragung in Frage kommenden SerDes-Systeme und die Kameras nur bis ASIL B ausgelegt werden können. Dies ergibt sich aus den maximal erreichbaren FIT-Raten, vergleichbar zu Tabelle 13. Für den ASIL-konformen Einsatz der Technologie existieren entsprechende Anleitungen der Halbleiterhersteller, die bei sicherheitsrelevanten Systemen zu beachten sind. Für den Anwendungsfall ergeben sich damit zwei redundante Pfade für die Übertragungsstrecken mit Kamera mit ASIL B(D) wie in Abbildung 24a/b zu sehen. Die Auswertung und das Monitoring ist mit einem ASIL-D-fähigen Rechenkern gelöst. Das System wird als Ergebnis der Analyse aus drei Komponenten bestehen. Einer Haupteinheit, die die Bilddaten deserialisiert und aufbereitet, die Fehleranalyse und Kanalschaltung durchführt sowie zwei über Coax angebundene Kamera-Datenserialisierer-Einheiten mit unterschiedlicher Übertragungstechnologie, welche die Videodaten bereitstellen.

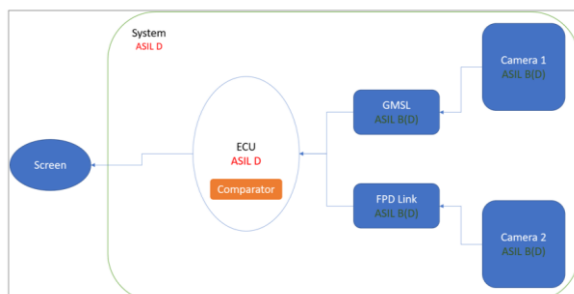


Abbildung 24a Schematische Darstellung ASIL-Dekomposition am Beispiel Frontkamarasystem

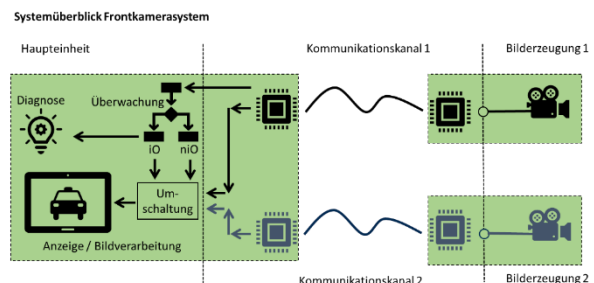


Abbildung 24b Schematische Darstellung mit redundanter Auslegung von Kamera mit Übertragungsstrecke

Die in der HARA identifizierten EMV-bezogenen Gefahren, z. B. Fehler in der Bildübertragung durch Störeinkopplungen, führen später im Prozess zur Berücksichtigung der EMV bei der Definition der Sicherheitszielen und technischen Sicherheitsanforderungen (z. B. Abschirmung der Datenleitungen).

8.3. Fehlerbaumanalyse (FTA)

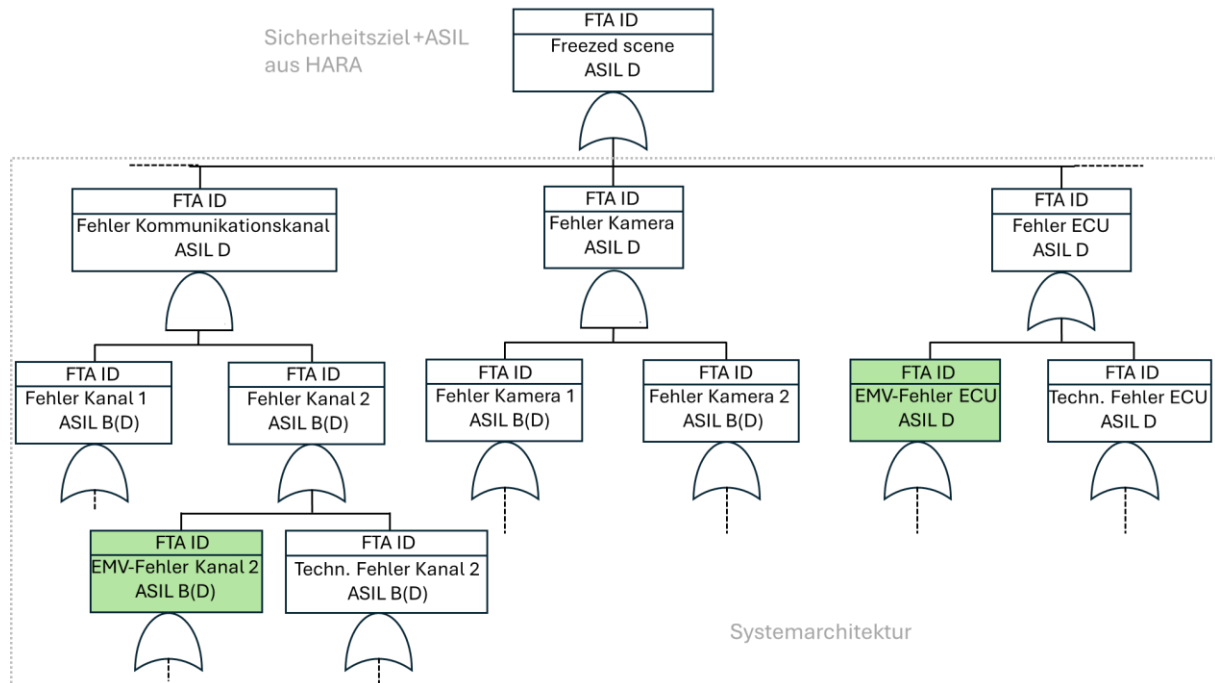


Abbildung 25 Demonstrator - Prinzipdarstellung Fehlerbaumanalyse (FTA)

Die FTA ist eine Top-Down-Methode zur Ermittlung der Ursachen eines definierten Fehlers oder Ereignisses. Sie verbindet die Sicherheitsziele mit der Systemarchitektur. Als Ergebnis erhält man die graphische Repräsentation der Fehlerpfade basierend auf der Systemarchitektur, von der auch Empfehlungen für Sicherheitsoptimierungen abgeleitet werden können. Der Fehlerbaum besteht aus den folgenden Komponenten:

Hauptereignis

Dies ist das unerwünschte Ereignis oder der Systemausfall, den die Analyse zu verhindern versucht. Es ist der Ausgangspunkt des Fehlerbaums.

Zwischenereignisse

Dies sind Ereignisse, die aufgrund eines oder mehrerer vorhergehender Ereignisse auftreten und zum Spitzenereignis führen. Sie stellen die Wege dar, auf denen das Spitzenereignis eintreten kann.

Basisereignisse

Dies sind die grundlegenden Ursachen der Zwischenereignisse. Sie sind in der Regel Komponentenausfälle oder menschliche Fehler und werden als Blätter des Fehlerbaums dargestellt.

Logikverknüpfungen

Diese Symbole repräsentieren die Beziehungen zwischen den Ereignissen. Die beiden Hauptarten von Logikgattern sind:

- "UND"-Gatter: Zeigt an, dass alle Eingangsereignisse eintreten müssen, damit das Ausgangsereignis eintritt.
- "ODER"-Gatter: Zeigt an, dass eines der Eingangsereignisse das Ausgangsereignis verursachen kann.

Abbildung 25 zeigt einen Auszug aus der FTA für den Demonstrator. Ausgehend vom unerwünschten Ereignis werden anhand der Systemarchitektur Fehlerursachen ermittelt. Hierbei werden auch EMV-bedingte Ereignisse berücksichtigt (grün). Man erkennt, dass die Fehlerursachenermittlung sukzessive immer detaillierter die Systemarchitektur berücksichtigt. Im Fall der EMV-bedingten Fehlerpfade sind mithilfe der EMV-Experten Lösungsvorschläge zu erarbeiten. Beispiele hierfür sind die Schirmungsauslegung der Übertragungskanäle oder die Filteroptimierung für die Power-Over-Coax Versorgung der Kameramodule.

8.4. Demonstrator (System) – FSC Funktionales Sicherheitskonzept

	Id	Description	ASIL	Allocation	Test ID	Test
FTA ID	SG_02	loss of filmed scene	ASIL D			
E078	SG_02_FSR_01	EMC issues on camera line shall not lead to a loss of filmed scene	ASIL D	camera	SG_02_TTR_05 SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E080	SG_02_FSR_02	No technical failure on camera shall lead to a loss of filmed scene	ASIL D	camera		
E073	SG_02_FSR_03	EMC failure on ECU side shall not lead to a loss of filmed scene	ASIL D	ECU	SG_02_TTR_05 SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E112	SG_02_FSR_04	No technical failure on ECU shall lead to a loss of filmed scene	ASIL D	ECU		
E072	SG_02_FSR_05	EMC failure at coax cable of main link shall not lead to a loss of filmed scene	ASIL B(D)	main channel	SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E109	SG_02_FSR_06	Rupture of the coax cable (main link) shall not lead to a loss of filmed scene	ASIL B(D)	main channel		
E084	SG_02_FSR_07	EMC failures at serializer (main link) shall not lead to a loss of filmed scene	ASIL B(D)	serializer	SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E110	SG_02_FSR_08	No technical failure of serializer (main link) shall lead to a loss of filmed scene	ASIL B(D)	serializer		
E083	SG_02_FSR_09	EMC failures at deserializer (main link) shall not lead to a loss of filmed scene	ASIL B(D)	deserializer	SG_02_TTR_05 SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605

Tabelle 17 Demonstrator – Auszug funktionales Sicherheitskonzept (FSC)

Die FSC leitet aus der Systemarchitektur funktionale Sicherheitsanforderungen ab. Die Ausgabe aus dem FSC und TSC ist eine Liste von funktionalen und technischen Sicherheitsanforderungen mit ASIL-Level und zugehörigen EMV-Tests.

8.5. Demonstrator (System) – TSC Technisches Sicherheitskonzept

Das technische Sicherheitskonzept (TSC) ist die Zuordnung der technischen Sicherheitsanforderungen (TSRs) zu den Systemelementen (HW, SW). Dabei handelt es sich um technische Anforderungen auf Systemebene, die für die Umsetzung der funktionalen Sicherheitsanforderungen erforderlich sind. Funktionale Sicherheitsanforderungen beschreiben lediglich, was erreicht werden muss, um die Sicherheitsziele zu erreichen, während TSRs die detaillierten technischen Spezifikationen dazu liefern, wie diese Sicherheitsziele erreicht werden können.

FTA ID	SG 02	Loss of filmed scene	ASIL	Functional Safety Requirement		ASIL	Allocation
E109	SG_02_FSR_06	Rupture of the coax cable (main link) shall not lead to a freezed or unusable scene	D	FSR 06a	check connection at start up	B	Main Unit
				FSR 06b	Permanent LOCK PIN (connection) check after start up	B	Main Unit
				FSR 06c	Permanent communication quality monitoring	B	Main Unit
				FSR 06d	Inform upper system level of connection status	B	Main Unit

Tabelle 18a Demonstrator – Auszug Ableitung von funktionellen Sicherheitsanforderungen

Functional Safety Requirement	Description	ASIL	Technical Safety Requirement		Derived from	Allocation
SG_02_FSR_06a	check communication channel connection at start up	B	TSR 1	Connected LOCK PIN	FSR 06a	Main Unit Hardware
			TSR 2	Software monitoring for LOCK PIN	FSR 06a	Main Unit Software
			TSR 3	Check Error Register	FSR 06a	Main Unit Software
			TSR 4	Check communication link quality (pre indicator)	FSR 06a	Main Unit Software

Tabelle 18b Demonstrator – Auszug Ableitung von technischen Sicherheitsanforderungen

8.6. Demonstrator (System) – FMEA Fehlermöglichkeits- und -Einflussanalyse

Block	Function	Failure Mode	Effect	Detectable?	Diagnostic Mechanism	Fault Category	Notes
Camera	Image capture	No output	Loss of object detection	Yes	Health monitoring, heartbeat	Single Point	Use redundancy with 2nd camera
Camera	Image capture	Corrupted image	Incorrect perception	Yes	CRC + plausibility check	Residual	Can lead to wrong ADAS reaction
Camera	Sensor internal fault	Silent failure	Loss of input	Yes	BIST / internal diag	Single Point	BIST available in imagers
Camera	Sensor supply	Over/under voltage	Loss of object detection	Yes	over/under voltage detection	Single Point	voltage monitoring
Camera	Bit error	Corrupted image	wrong input	Yes	CSI packet ECC/CRC (1 bit correctable)	Single Point	data chck implemented
Comm Link	Data transmission	Line fault / short	Loss of video stream	Yes	Line monitoring / CRC	Single Point	Often hardware-supported diag
Comm Link	Data transmission	EMI / corruption	Wrong data interpreted	Yes	CRC, link-layer checks	Residual	May affect object classification
Comm Link	Desync / clock drift	Invalid data	Delays or loss of sync	Partial	Frame ID / sequence check	Residual	Common in high-speed serial communication
Comm Link	Video data transmission	Invalid data due to noise coupling	wrong data	yes	CRC, FEC, adaptive equalization,	Single Point	safty measures integrated
Comm Link	control data transmission	Invalid data due to noise coupling	wrong data	yes	CRC, retransmission	Single Point	safty measures integrated
Comm Link	POC voltage	under/over voltage	loss of of control data stream	yes	over/under voltage detection	Single Point	voltage monitoring implemented
Comm Link	POC voltage	under/over voltage	loss of of video stream	yes	over/under voltage detection	Single Point	voltage monitoring implemented
Comm Link	Video data transmission	loss of video link lock due to noise coupling	link loss	yes	LOCK pin and register	Residual	Use redundancy with 2nd camera
ECU	Image processing	Software crash	System hang	Yes	Watchdog timer	Single Point	Reset possible
ECU	CPU core failure	Silent data corruption	Wrong decisions	Partial	Lockstep, ECC, monitoring	Residual	ISO 26262 HW mechanism implemented
ECU	Memory corruption	Wrong object position	Incorrect control	Partial	ECC RAM, parity check	Residual	RAM errors are safety check implemented
ECU	Power supply fail	Blackout	System stops	Yes	Voltage monitoring	Single Point	Can trigger safe state
Screen	Display alert	No display	Driver not alerted	Yes	Self-test / watchdog	Single Point	Safety-critical for warnings
Screen	Wrong display	Misleading info	Incorrect driver action	Partial	Software check / redundancy	Residual	HMI testing required

Tabelle 19 Auszug FMEA für Demonstrator

Die FMEA berücksichtigt die Sicherheitsziele, die Systemarchitektur, die Fehlermöglichkeiten sowie die Diagnosemöglichkeiten und erzeugt Empfehlungen zur Risikominderung, wie z.B. Designänderungen oder Sicherheitsmaßnahmen, sowie Abschätzungen zur Diagnoseabdeckung auf Basis von vorherigen Projekten oder Erfahrungen. Eine FMEA stellt eine System- und Risikoanalyse mit dem Ziel einer Optimierung durch Fehlervermeidung dar. Ein weiterer Vorteil ist die Möglichkeit, einen Wissensspeicher für Fehlertypen und Schutzmaßnahmen aufzubauen. Auch bei diesem Schritt werden die durch EMV hervorgerufenen Fehlermöglichkeiten berücksichtigt. Damit sollten auch hier EMV-Fachleute mit einbezogen werden.

8.7. Demonstrator (System) – FMEDA Fehlermöglichkeits-, Diagnose- und Einflussanalyse

Block	Function	Failure Mode	Effect	Failure Rate (FIT)	Detectable?	Diagnostic Mechanism	DC%	Fault Category	Notes
Camera	Image capture	No output	Loss of object detection	100	Yes	Health monitoring, heartbeat	90	Single Point	Use redundancy with 2nd camera
Camera	Image capture	Corrupted image	Incorrect perception	50	Yes	CRC + plausibility check	95	Residual	Can lead to wrong ADAS reaction
Camera	Sensor internal fault	Silent failure	Loss of input	20	Yes	BIST / internal diag.	80	Single Point	BIST often available in imagers
Camera	Sensor supply	Over/under voltage	Loss of object detection	TBC	Yes	over/under voltage detection	TBC	TBC	
Camera	Bit error	Corrupted image	wrong input	TBC	Yes	CSI packet ECC/CRC (1 bit correctable)	TBC	TBC	
Comm Link	Data transmission	Line fault / short	Loss of video stream	30	Yes	Line monitoring / CRC	95	Single Point	Often hardware-supported diag
Comm Link	Data transmission	EMI / corruption	Wrong data interpreted	20	Yes	CRC, link-layer checks	90	Residual	May affect object classification
Comm Link	Desync / dock drift	Invalid data	Delays or loss of sync	10	Partial	Frame ID / sequence check	70	Residual	Common in high-speed serial comm
Comm Link	Video data transmission	Invalid data due to noise coupling	wrong data	TBC	yes	CRC, FEC, adaptive equalization,	TBC	TBC	
Comm Link	control data transmission	Invalid data due to noise coupling	wrong data	TBC	yes	CRC, retransmission	TBC	TBC	
Comm Link	POC voltage	under/over voltage	loss of control data stream	TBC	TBC	over/under voltage detection	TBC	TBC	
Comm Link	POC voltage	under/over voltage	loss of video stream	TBC	TBC	over/under voltage detection	TBC	TBC	
Comm Link	Video data transmission	loss of video link lock due to noise coupling	link loss	TBC	TBC	LOCK pin and register	TBC	TBC	
ECU	Image processing	Software crash	System hang	80	Yes	Watchdog timer	95	Single Point	Reset possible
ECU	CPU core failure	Silent data corruption	Wrong decisions	30	Partial	Lockstep, ECC, monitoring	80	Residual	ISO 26262 HW mechanism needed
ECU	Memory corruption	Wrong object position	Incorrect control	20	Partial	ECC RAM, parity check	90	Residual	RAM errors are safety-relevant
ECU	Power supply fail	Blackout	System stops	10	Yes	Voltage monitoring	95	Single Point	Can trigger safe state
Screen	Display alert	No display	Driver not alerted	15	Yes	Self-test / watchdog	90	Single Point	Safety-critical for warnings not in Focus
Screen	Wrong display	Misleading info	Incorrect driver action	10	Partial	Software check / redundancy	70	Residual	HMI testing required

Tabelle 20 Auszug FMEDA für Demonstrator

Die FMEDA ist eine quantitative Erweiterung der klassischen FMEA, die speziell zur Berechnung von Ausfallraten, Diagnoseabdeckungsgraden (DC) und funktionaler Sicherheit eingesetzt wird. Während die FMEA qualitative Risiken bewertet, liefert die FMEDA quantitative Sicherheitsdaten. Wie schon beschrieben, reichen bei der Anforderung ASIL B (D) für die Betrachtung von Kamera, Kommunikation und Versorgung einfache Abschätzungen für die FIT und die Diagnoseabdeckung, die z.B. auf Erfahrungswerten basieren (Tabelle 20).

8.8. Demonstrator (System) – TTR Technische Testanforderungen

Die ISO 26262 ist zielorientiert und nicht präskriptiv. Sie verlangt entsprechend dem ASIL den Nachweis, dass sich das System bei Fehlern und Störungen sicher verhält. Dafür erfolgen keine generellen Vorgaben zu Prüfumfang oder Grenzwerten. Diese Festlegungen sind damit Teil der Sicherheitsanalyse.

Die projektbezogene Definition der Testumfänge leitet sich aus den funktionalen und technischen Sicherheitsanforderungen und der Systemarchitektur ab. An dem Prozessschritt sind EMV-Experten mit beteiligt. Als Ergebnis werden die Prüfumfänge und die Grenzwerte definiert.

Die Prüfumfänge lassen sich einzelnen Sicherheitszielen zuordnen (Tabelle 21).

	Id	Description	ASIL	Allocation	Test
FTA ID	SG_02	loss of filmed scene	ASIL D		
E078	SG_02_FSR_01	EMC issues on camera line shall not lead to a loss of filmed scene	ASIL B(D)	camera	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E080	SG_02_FSR_02	No technical failure on camera shall lead to a loss of filmed scene	ASIL B(D)	camera	
E073	SG_02_FSR_03	EMC failure on ECU side shall not lead to a loss of filmed scene	ASIL D	ECU	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E112	SG_02_FSR_04	No technical failure on ECU shall lead to a loss of filmed scene	ASIL D	ECU	
E072	SG_02_FSR_05	EMC failure at coax cable of main link shall not lead to a loss of filmed scene	ASIL B(D)	main channel	ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E109	SG_02_FSR_06	Rupture of the coax cable (main link) shall not lead to a loss of filmed scene	ASIL B(D)	main channel	
E084	SG_02_FSR_07	EMC failures at serializer (main link) shall not lead to a loss of filmed scene	ASIL B(D)	serializer	ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E110	SG_02_FSR_08	No technical failure of serializer (main link) shall lead to a loss of filmed scene	ASIL B(D)	serializer	
E083	SG_02_FSR_09	EMC failures at deserializer (main link) shall not lead to a loss of filmed scene	ASIL B(D)	deserializer	ISO 7637-3 ISO 11452-4 ISO 11452-2
E111	SG_02_FSR_10	No technical failure of deserializer (main link) shall lead to a loss of filmed scene	ASIL B(D)	deserializer	

Tabelle 21 Beispiel für Zuordnung EMV-Testanforderungen zu Sicherheitszielen

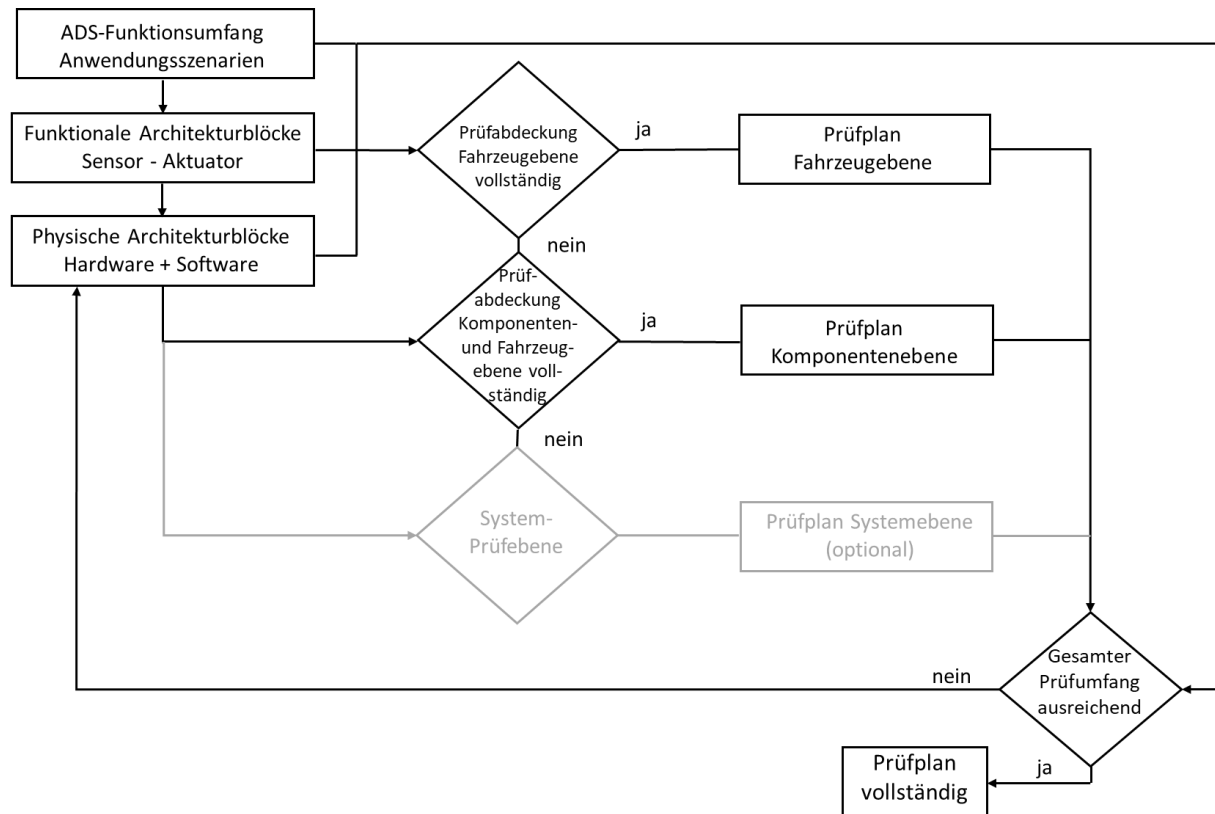
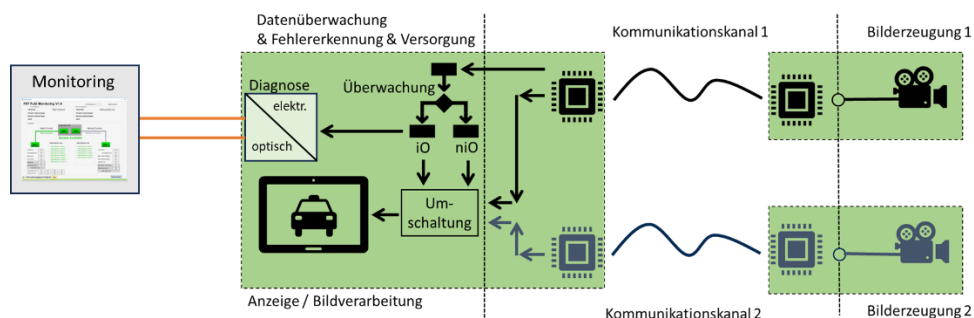


Abbildung 26 EMV- Prüfebenen und Ableitung der Prüfumfänge

Die Testanforderungen umfassen auch den Prüfumfang, der sich aus der Funktionalität auf Fahrzeugebene ableitet (Abbildung 26). Ausgehend vom dem gesamten System muss überprüft werden, welcher Umfang auf welcher Prüfebene abgedeckt werden kann. Auf Fahrzeugebene kann beispielsweise durch Einschränkungen der Prüfumgebung wie feststehende Wände der EMV-Halle nicht alle Szenarien geprüft werden. Auf der Komponentenebene kann es durch die Aufteilung der Funktionseinheiten zu Einschränkungen bei übergreifender Funktionalität wie Sensorfusion kommen. Ein großer Vorteil der Komponentenebene ist die Möglichkeit der umfangreichen Diagnose. Im Fall des Demonstrators wird der Fehlerzustand des Teilsystems detektiert und ausgegeben. Neben der reinen Funktionalität der Bilddatenerfassung und Übertragung sind somit die Information des übergeordneten Gesamtsystems über die Verfügbarkeit und die Fehleranzeige vor Ausfall wichtige Funktionsmerkmale. Diese werden bei den Messungen mit überwacht, besitzen eigene ID's für die Sicherheitsmaßnahmen und den Safe State (Tabelle 22).



8.9. Demonstrator (System) – Rückverfolgbarkeit der Elemente der Sicherheitsanalyse

FTA ID	Id	Description	ASIL	Allocation	Test ID	Safety Measure	Safe State	Test
	SG_02	loss of filmed scene	ASIL D					
E078	SG_02_FSR_01	EMC issues on camera line shall not lead to a loss of film	ASIL D	camera	SG_02_TTR_05 SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	SM0010 SM0020 ...	SS01	ISO 7637-2 ISO 7637-3 ISO 11452-2 ISO 11452-4 ISO 10605
E080	SG_02_FSR_02	No technical failure on camera shall lead to a loss of	ASIL D	camera				
E073	SG_02_FSR_03	EMC failure on ECU side shall not lead to a loss of filmed scene	ASIL D	ECU	SG_02_TTR_05 SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	SM001 SM002 ...	SS01	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E112	SG_02_FSR_04	No technical failure on ECU shall lead to a loss of filmed	ASIL D	ECU				
E072	SG_02_FSR_05	EMC failure at coax cable of main link shall not lead to a loss of filmed scene	ASIL B(D)	main channel	SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	SM001 SM002 ...	SS01	ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E109	SG_02_FSR_06	Rupture of the coax cable (main link) shall not lead to a loss of filmed scene	ASIL B(D)	main channel				
E084	SG_02_FSR_07	EMC failures at serializer (main link) shall not lead to a loss of filmed scene	ASIL B(D)	serializer	SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	SM001 SM002 ...	SS01	ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605
E110	SG_02_FSR_08	No technical failure of serializer (main link) shall lead	ASIL B(D)	serializer				
E083	SG_02_FSR_09	EMC failures at deserializer (main link) shall not lead to a loss of filmed scene	ASIL B(D)	deserializer	SG_02_TTR_05 SG_02_TTR_06 SG_02_TTR_03 SG_02_TTR_04 SG_02_TTR_09	SM001 SM002 ...	SS01	ISO 7637-2 ISO 7637-3 ISO 11452-4 ISO 11452-2 ISO 10605

Tabelle 22 Beispiel für den aus dem funktionalen Sicherheitskonzept (FSC) abgeleiteten Testplan mit Nachverfolgbarkeits-IDs und Zuordnung zu den Elementen der Sicherheitsanalyse

Id	Description	ASIL	Allocation	Impact
Safety Measure	loss of filmed scene	ASIL D		
SM001	CRC for Video Channel	ASIL B(D)	channel	EMC
SM002	PLL LOCK Video Channel	ASIL B(D)		
SM003	Forward Error Correction	ASIL B(D)		
SM004	Parity	ASIL B(D)		

Tabelle 23 Beispiel für implementierten Sicherheitsmaßnahmen mit Nachverfolgbarkeits-IDs und Zuordnung zu den Elementen der Sicherheitsanalyse

Id	Description	ASIL	Allocation
Safe State	loss of filmed scene	ASIL D	
SS01	detect: errors in both channels react: inform upper system, restart transmission, send status (heartbeat)	ASIL (D)	System

Tabelle 24 Beispiel für implementierten sicheren Zustände des EUT mit Nachverfolgbarkeits-IDs

Die in der ISO 26262 geforderte Rückverfolgbarkeit (Traceability) ist essenziell für die funktionale Sicherheit. Sie erfordert eine durchgängige, bidirektionale Verknüpfung von Sicherheitsanforderungen über Systemdesign, Implementierung bis hin zu Tests (Verifizierung/Validierung). Dies stellt sicher, dass alle Anforderungen erfüllt werden und die Risiken minimiert sind. Dieser Nachweis kann entweder auf Basis von Softwareapplikationen oder per Identifiersystem erfolgen. Jedes Arbeitselement (z.B. Sicherheitsziel, Anforderung, EMV-Prüfung) muss rückwärts zum Ursprung und vorwärts zum Testergebnis verfolgbar sein (V-Modell).

8.10. Demonstrator (System) – Qualitative Analyse

Die ISO 26262 verlangt quantitative Architekturmetriken (SPFM, LFM, PMHF) nur für ASIL C- und D-Hardware. Daher ist eine qualitative Analyse für geringere Risikoklassen akzeptabel, wenn sie durch ein überzeugendes Sicherheitsargument gestützt wird. Dieses Argument sind Anforderungen an die Rückverfolgbarkeit (Traceability) der Sicherheitselemente über den gesamten Prozess hinweg. Hier geht es darum, die durch FMEA oder FTA identifizierten

Gefahren und Fehlfunktionen lückenlos mit den Sicherheitszielen, Sicherheitsanforderungen und dem Systemdesign zu verknüpfen. Damit wird sichergestellt, dass alle potenziellen Fehlerquellen adressiert und die Sicherheitsanforderungen erfüllt werden. Dies wird durch spezielle Tools oder eindeutige hierarchische Identifier dokumentiert und nachgewiesen.

Aus Sicht der EMV ist eine Dekomposition von Anforderungen für ASIL C und D sinnvoll, da die nicht mögliche Berechnung der Metriken wegfällt und eine rein qualitative Analyse durchführbar wird.

Durch eine qualitative Analyse kann unter bestimmten Voraussetzungen auf eine Quantifizierung der Ausfallwahrscheinlichkeiten verzichtet werden. Der qualitative Prozess

- stützt sich auf beschreibende oder kategoriale Bewertungen der Sicherheit,
- umfasst Techniken wie Gefahrenanalyse und Risikobewertung (HARA), Fehlermöglichkeits- und -effektanalyse (FMEA) und strukturiertes Brainstorming,
- basiert auf dem Verständnis der Natur und der Eigenschaften potenzieller Gefahren und Ausfallmodi,
- konzentriert sich auf die Identifizierung und Priorisierung von Sicherheitsbedenken auf der Grundlage von Expertenurteilen, historischen Daten und Systemkenntnissen und
- bietet Einblicke in potenzielle Ausfallszenarien, ihre Ursachen und ihre Auswirkungen, ohne spezifische numerische Wahrscheinlichkeiten zuzuweisen.

Die Grundlagen für die Bewertung sind die technische Expertise des Ingenieurteams und der aktuelle Stand der Technik.

Ein wichtiger Vorteil, der sich aus der qualitativen Analyse ergibt, ist der mögliche Verzicht auf die Metriken für die EMV-Messungen.

Obligatorisch ist es jedoch nachzuweisen, dass EMV-Störungen nicht zu einer Verletzung der Sicherheitsziele führen. Die ISO 26262 ist zielorientiert und nicht präskriptiv. Sie verlangt entsprechend dem ASIL den Nachweis, dass sich das System bei Fehlern und Störungen sicher verhält. Dafür erfolgen keine generellen Vorgaben zu Prüfumfang oder Grenzwerten. Für einen qualitativen Sicherheitsansatz ist damit die Erhöhung der EMV-Prüfschärfegraden optional und nicht obligatorisch.

Sollten in der Sicherheitsbetrachtung höhere Prüfpegel für die Absicherungsstrategie als wünschenswert angesehen werden, können diese - in sinnvollen Grenzen - schrittweise erhöht werden. Abschließend wird festgehalten, bis zu welcher Stufe (für jeden Parameter) das zu prüfende System korrekt funktioniert. Ein weiterer Ansatz ist die Berücksichtigung von Messunsicherheiten zur Festlegung von Prüfpegeln entsprechend der ASIL [3].

Für die abgeleiteten ASIL X(Y) gelten etwas strengere Anforderungen als für reine ASIL X, da sie ein übergeordnetes Sicherheitsziel mit höherem ASIL haben. Für ASIL B(D) beispielsweise gelten nach ISO 26262 bestimmte Pflichtaktivitäten. Dazu gehören eine qualitative FMEA (Bottom-Up-Methode) für alle Fehlermodi sowie eine partielle FMEDA, bei der – sofern verfügbar – diagnostische Abdeckungswerte angenommen werden können, z.B. von Vorgängerprojekten. Darüber hinaus sind eine begründete Darstellung der Unabhängigkeit und des verbleibenden Restrisikos sowie vollständige Anforderungs- und Nachweisverfolgbarkeit, die in den Sicherheitsnachweis einfließt, erforderlich. Die FTA (Top-Down-Ansatz) wird ebenfalls für die ASIL-B-Entwicklung empfohlen. Weiterhin müssen bestimmte Anforderungen an die Dokumentation eingehalten werden. Damit sind für diesen Fall keine quantitativen Analysen zwingend notwendig.

8.11. Demonstrator (System) – Zusammenfassung Sicherheitsanalyse

Die Einbindung von EMV in den Sicherheitsprozess nach ISO 26262 erfordert keine komplette Neubewertung der EMV, aber eine strukturierte frühzeitige Einbindung der EMV-Maßnahmen in den Prozess. Der Nachweis über die Einhaltung der definierten Sicherheitsziele ist hier die Bewertungsmaßgabe für die Prüfungen.

Die für die EMV wichtigen Punkte im Assessment sind:

- Einbeziehung von EMV-Experten schon so früh wie möglich im Prozess,
- Berücksichtigung von EMV-bedingten Fehlermöglichkeiten und daraus abgeleiteten Sicherheitsanforderungen,
- Ableitung von EMV-Maßnahmen auf Basis der Fehleranalyse,
- Festlegung von Prüfumfängen und den Grenzwertvorgaben auf Basis der Analyse.

9. EMV-Prüfungen am Demonstrator

9.1. Allgemeine Betrachtungen

Für das hier genutzte Beispiel Frontkamera ist ein wichtiges Sicherheitsziel die Aufrechterhaltung der Videoüberwachung an der Fahrzeugfront. Ein typischer Wert für die Abtastrate solcher Systeme liegt im Millisekundenbereich. Damit muss bei redundanter Auslegung die Diagnose und im Fehlerfall die Kanalschaltung zwischen den Übertragungstrecken in einer Zeit unter dieser Vorgabe realisiert werden. Diese Anforderung muss bei der Systementwicklung bei den Functional Safety Requirements beachtet und durch die Technical Safety Requirements auf der Komponentenebene abgebildet werden. Die Umsetzung erfolgt bei der Hardware- und Softwareentwicklung. Der Nachweis der Anforderungen erfolgt in der Verifikations- und Validierungsphase. Für das hier verwendete System liegt die Kanalschaltungs- und Fehlersignalisierungszeit bei 10 ms.

Die erste Überprüfung kann durch die Failure Injection Tests erfolgen. Die verwendeten Kommunikationsbausteine, die nach ASIL-B-Vorgaben qualifiziert sind, weisen dafür die notwendigen Funktionsumfänge auf. Dazu zählen z.B. Fehlergeneratoren, die sich per Software parametrisieren lassen. Durch die so eingepprägten Fehler lassen sich Diagnose und Abfangroutinen prüfen und optimieren. Diese Fehlerinjektion wurde im Projekt genutzt, um die Diagnose zu prüfen.

Die EMV-Prüfungen fallen in die Verifikationsphase auf Systemebene. EMV-Prüfungen im Rahmen der funktionalen Sicherheit müssen die Einhaltung der Sicherheitsziele nachweisen. Für den gesamten Prozess ist eine Planung notwendig, die frühzeitig eine Einbeziehung von EMV-Fachleuten erfordert. Bereits für die Fehlerbaumanalyse (FTA) ist die Identifizierung möglicher EMV-bedingter Einflüsse auf die Sicherheitsziele notwendig. Diese muss später im funktionalen (FSC) und technischen Sicherheitskonzept (TSC) vertieft werden. Mögliche Abhilfemaßnahmen müssen definiert werden. Diese werden dann in der FMEA zusammengeführt. Die dort ebenfalls aufgeführten Diagnosemechanismen müssen auf ihre Verwendbarkeit für EMV-Tests geprüft werden. Der Prüfumfang wird in den technischen Prüfanforderungen (TTR) von den Verantwortlichen festgelegt und kann über die in der ISO 26262 aufgeführten Prüfverfahren (Tabelle 26) hinausgehen.

Der EMV-Prüfumfang ist Teil des Verifikationsplans. Dieser definiert den Umfang, die Methoden, den Zeitplan, die Verantwortlichkeiten und die erforderlichen Ressourcen für alle Verifizierungsaktivitäten.

Für die EMV-Prüfungen ergeben sich auf Basis der TTR bei dem Prüfling in Abbildung 2 folgende zu prüfende Konfigurationen, um alle Betriebsmodi abzudecken:

- Hauptplatine + Übertragungskanal 1 + Kamera 1
- Hauptplatine + Übertragungskanal 2 + Kamera 2
- Hauptplatine + Übertragungskanal 1 + Kamera 1 +
Übertragungskanal 2 + Kamera 2

Bei den Prüfungen können neben Fehlern auch Common Cause Failures (Fehlerverkettungen) auftreten, so dass beide Videokanäle aufgrund der Störeinkopplung ausfallen. Hier muss die Diagnose mindestens an das übergeordnete System eine entsprechende Information senden, um diesen Fall auf übergeordneter Ebene abzufangen. Dies ist in der Monitoring Software, Abbildung 26, umgesetzt.

Der Vorteil von Prüfungen auf Komponentenebene liegt in der möglichen Diagnose. Bei Messungen auf Fahrzeugebene ist das Einsetzen von nicht serienkonformer Software nicht für alle Prüfungen zulässig. Damit ist bei den komplexen Systemen hier eine Fehlersuche oft sehr aufwändig, da die Diagnoseschnittstellen fehlen.

9.2. Softwareumsetzung der Kanalauswahl

Das System besteht aus drei Komponenten, der Haupteinheit und zwei über Coax-Leitungen abgesetzten Kameraeinheiten. Sind beide Kameramodule angesteckt, sind beide aktiv.

Es erfolgen pro Kanal zwei im Frequenzbereich getrennte Datenübertragungen (Abbildung 16). Der Videostream wird im oberen Frequenzbereich mit hohen Datenraten von der Kamera zur Hauptplatine übertragen. In der Gegenrichtung erfolgt mit niedrigerer Datenrate der Transport von Konfigurations- und Steuerdaten.

Die Datenübertragung erfolgt bei fehlerfreiem Betrieb über Hauptkanal (Main Link). Treten hier kritische Beeinflussungen auf, erfolgt die Umschaltung auf den Backup Link. Zeigt der Backup-Link Fehler, erfolgt die Umschaltung auf den Hauptlink. Die Fehlerregisterwerte der Kameramodule werden mit über den Rückkanal des Coax-Links übertragen und zusammen mit den Fehlerregistern der Hauptplatine kontinuierlich ausgewertet. Diese Informationen werden an die übergeordnete Ebene weitergegeben und für die Kanalschaltung genutzt (Abbildung 27).

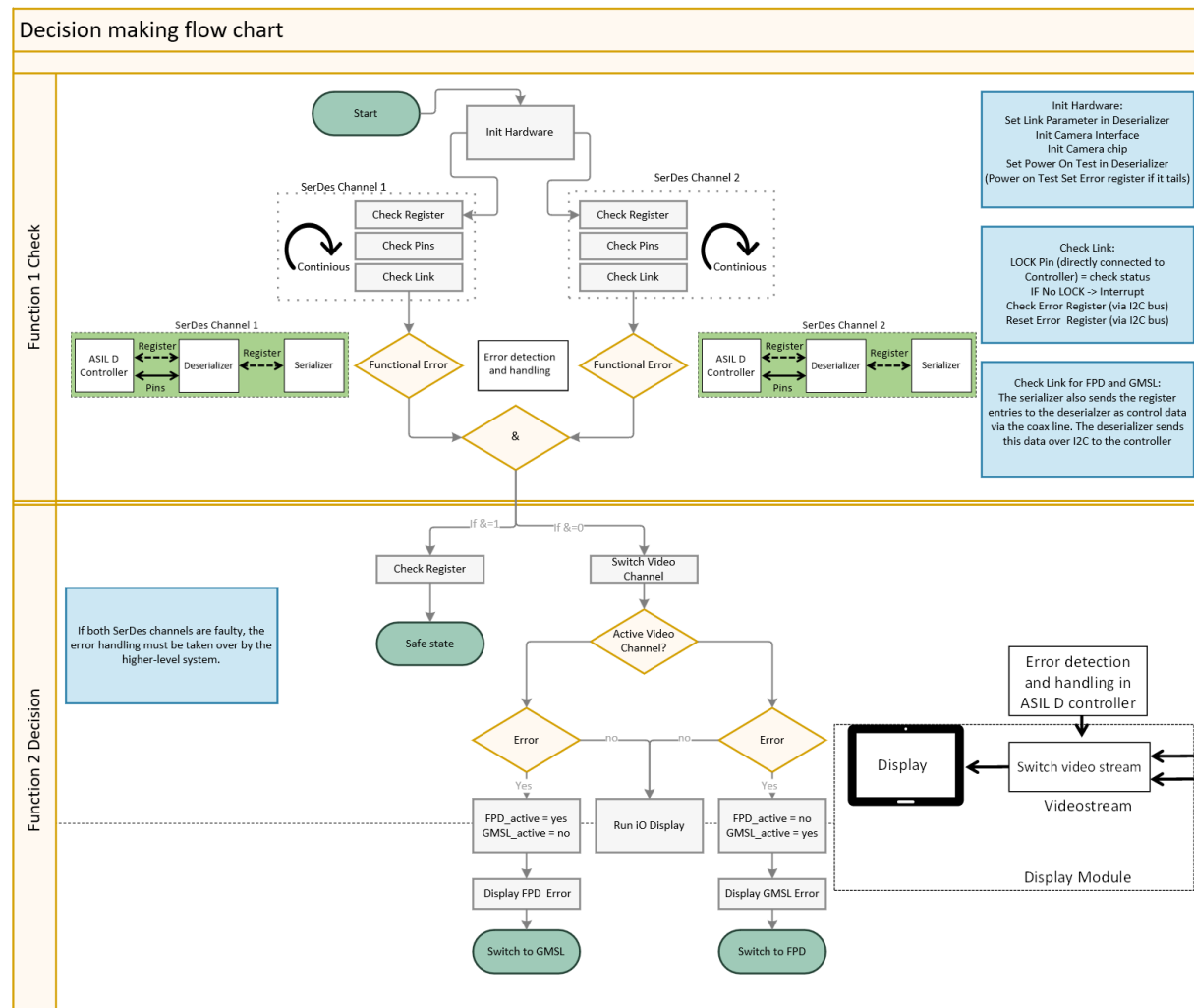


Abbildung 27 Demonstrator - Flowchart Software

9.3. Prüfkriterien

Das Flowchart für die Messungen ist in Abbildung 28 zu sehen. Es gibt hier zwei Kriterien für eine Beeinträchtigung durch die Prüfungen:

- Prüfling beschädigt (EUT damaged)
- Funktionsbeeinträchtigung (loss of function)

Es wurde festgelegt, dass eine Beschädigung immer als ‚nicht bestanden‘ zu werten ist. Ein ‚bestanden‘ (pass) wird erreicht, wenn die Systemfunktion ‚Videodatenübertragung‘ ohne Verletzung der Sicherheitsziele aufrechterhalten wird oder das System bei Funktionsverlust in einen sicheren Zustand (defined state) übergeht.

Als sicherer Zustand gilt, wenn bei Ausfall beider Kanäle das übergeordnete System über einen Ausfall der Frontkamerafunktion informiert wird.

Der Funktionserhalt kann während der Prüfungen sowohl auf Systemebene als auch auf Ebene der ausgewählten Übertragungstechnologie erfolgen.

Auf Systemebene wird überwacht und angezeigt, wenn

- bei Störungen auf dem Hauptkanal eine Umschaltung auf den Rückfallkanal erfolgt oder
- bei Störungen auf dem Rückfallkanal eine Umschaltung auf den Hauptkanal ausgeführt wird.

Auf Ebene der SerDes-Technologie ist die Überwachung der Fehlerregister möglich. Hier werden auch Fehler angezeigt, die das System auf Basis von Sicherheitsmaßnahmen wie FEC selber korrigieren kann (Corrected Error in Abbildung 29). Dies ist für die Funktionsbewertung unerheblich, aber ein guter Vorindikator für die Beeinflussungsschwelle der Kanäle während der EMV-Prüfungen.

Für die Prüfungen wurde die Information an das übergeordnete System per Monitoring (Abbildung 29) ausgegeben. Hier erkennt man den aktuell aktiven Kanal, den Fehlerzustand beider Bildübertragungsstrecken.

Beim Starten der Applikation auf den Steuergeräten werden zahlreiche Sicherheitsmaßnahmen geprüft. Die Ergebnisse hierzu werden ebenfalls im Monitoring angezeigt. Nicht alle angezeigten Fehler führen zu einer sicherheitsrelevanten Beeinflussung der Datenübertragung, da einzelne Fehler durch die jeweilige SerDes-Technologie ausgeglichen werden können.

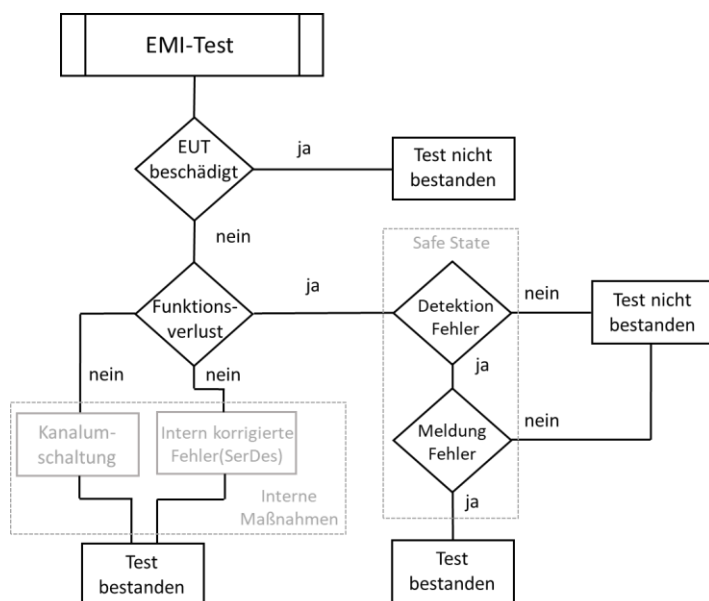


Abbildung 28 Flowchart EMV-Prüfungen

Die hier ausgewählten Verfahren zur Analyse der Störfestigkeit des Systems entsprechen denen in der ISO 26262 vorgeschlagenen Verfahren (Tabelle 26). Der Umfang kann aber projektspezifisch technisch bedingt erweitert werden.

Aus den Messverfahren wurden für das Projekt nur solche ausgewählt, die bei den Messungen einen aktiven Prüfling erfordern, um hier die im Fehlerfall notwendige Umschaltung zwischen den Kanälen und inklusive der zugehörigen Diagnose in der Überwachungssoftware darzustellen. So wurden die ESD-Prüfungen mit nicht bestromtem System (unpowered), die Prüfungen nach ISO 7637-2 sowie die Einkopplung der langsamen Pulse nach ISO 7637-3 im Rahmen dieser Untersuchungen nicht durchgeführt.

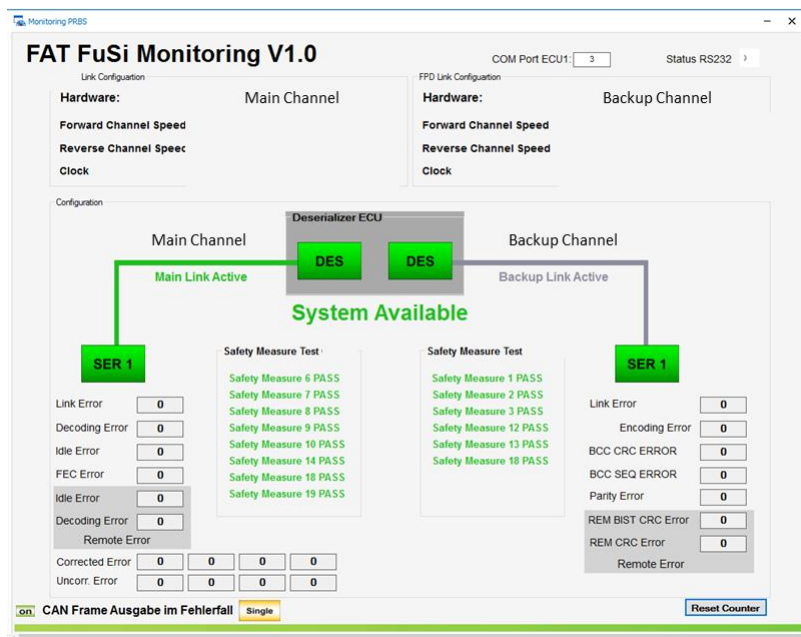


Abbildung 29 Monitoring Software für die Fehlererkennung mit Prüfung der Fehlerbehandlungsrouinen

Beschreibung	Bewertungskriterium
Prüfling beschädigt	Nicht bestanden
Safe State (Defined state) nicht erreicht / eingehalten Keine Videodatenübertragung / keine Diagnoseausgabe Information des übergeordneten Systems	Nicht bestanden
Funktion Videoübertragung nicht aufrecht erhalten mit Kanalschaltung aber übergeordnetes System informiert über Ausfall der Videodatenübertragung (Safe State / (Defined state))	Bestanden mit Einschränkungen
Funktion Videoübertragung aufrecht erhalten ohne Kanalschaltung, übergeordnetes System informiert über Funktionszustand	Bestanden
Funktion Videoübertragung aufrecht erhalten ohne Kanalschaltung aber internen Fehlern, übergeordnetes System informiert über Funktionszustand	Bestanden
Funktion Videoübertragung aufrecht erhalten mit Kanalschaltung, übergeordnetes System informiert über Funktionszustand	Bestanden

Tabelle 25: Bewertungskriterien für die EMV-Prüfungen

9.4. Prüfverfahren

Norm	Beschreibung
ISO 11452-2	Straßenfahrzeuge - Elektrische Störungen durch schmalbandige gestrahlte elektromagnetische Energie; Prüfverfahren für Komponenten - Absorberraum (ALSE)
ISO 11452-4	Straßenfahrzeuge - Elektrische Störungen durch schmalbandige gestrahlte elektromagnetische Energie; Prüfverfahren für Komponenten - Stromzange (BCI)
ISO 7637-2	Straßenfahrzeuge - Elektrische, leitungsgeführte und gekoppelte Störungen - Elektrische, leitungsgeführte Störungen auf Versorgungsleitungen
ISO 7637-3	Straßenfahrzeuge - Elektrische, leitungsgeführte und gekoppelte Störungen - Übertragung von impulsförmigen elektrischen Störgrößen durch kapazitive und induktive Kopplung auf Leitungen, die keine Versorgungsleitungen sind
ISO 10605	Straßenfahrzeuge - Prüfverfahren für elektrische Störungen durch elektrostatische Entladungen

Tabelle 26: Vorschläge für EMV-Prüfverfahren nach ISO 26262

Die Prüfungen umfassen die in Tabelle 26 aufgeführten Verfahren unter Verwendung der in Kapitel 9.7 angeführten Aufbauten und Randbedingungen.

9.5. Testlevel für Prüfverfahren

Für das Projekt wurde im Zuge der Definition des Prüfumfanges festgelegt, neben den Störpegeln aus der normativen Vorgabe auch die beschriebenen Pegelerhöhungen unter Berücksichtigung der Messunsicherheiten zu prüfen. Damit soll das Vorgehen gezeigt und eventuelle Auswirkungen auf das Prüflingsverhalten dargestellt werden. Dieses Vorgehen ist projektspezifisch und nicht generell in der ISO 26262 vorgeschrieben.

Hier wurde für die Verfahren ISO 11452-2 (ALSE), ISO 11452-4 (BCI) und die ISO 7637-3 (Impulsförmige Störgrößen) als Prüfkriterium das in den Normen vorgeschlagene Test Level IV ausgewählt. Die Prüfschärfegrade können als für solche Anwendungen als üblich angesehen werden. Für die Erhöhung nach Berücksichtigung der Messunsicherheiten wurde jeweils der höchste Wert für ASIL D projektspezifisch ausgewählt.

Die Messunsicherheiten wurden bei der ALSE- und der BCI-Methode sowie für die impulsförmigen Störgrößen berücksichtigt. Für die ESD-Prüfungen erfolgt die Erhöhung der Prüfschärfe bis zur Beeinflussung des Systems. Für ESD wurde dieses Vorgehen gewählt, da sich aus den Unsicherheitsbetrachtungen eine geringe Unsicherheit ergibt, die in der praktischen Anwendung zu keinen signifikanten Pegeländerungen ($< 1\text{kV}$) führt und um das Vorgehen exemplarisch anzuwenden.

9.6. Demonstratorsystem als Prüfling

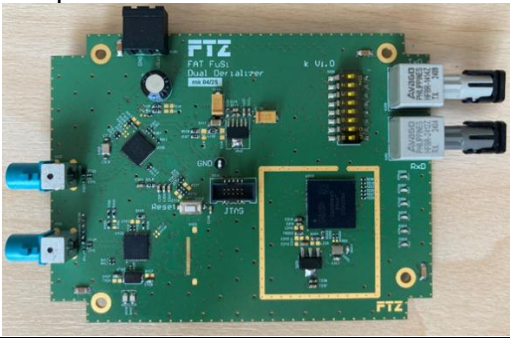
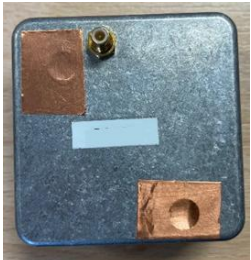
EUT ohne Gehäuse	EUT mit Gehäuse
Haupteinheit 	Haupteinheit 
Kameraeinheit 1 	Kameraeinheit 1 
Kameraeinheit 2 	Kameraeinheit 2 

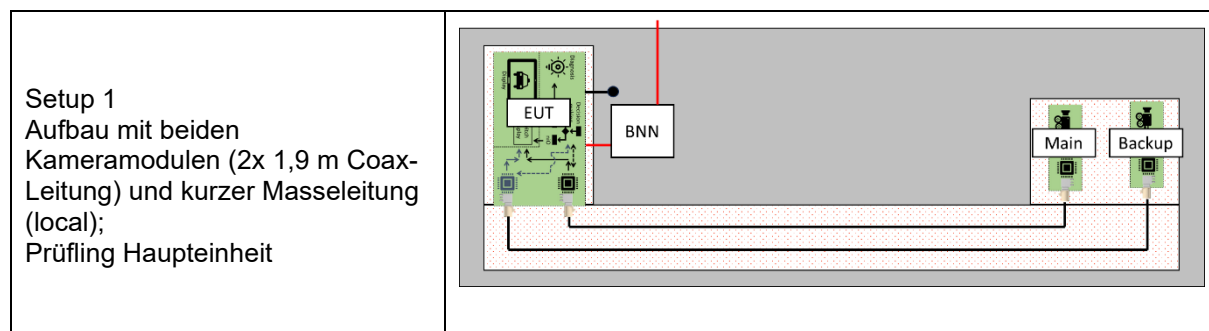
Tabelle 27 Komponenten des Demonstratorsystems

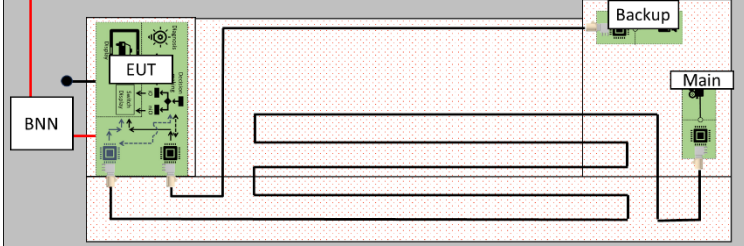
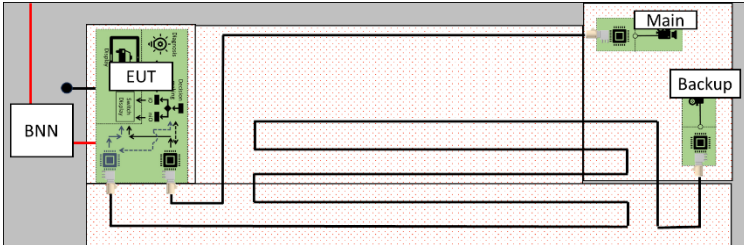
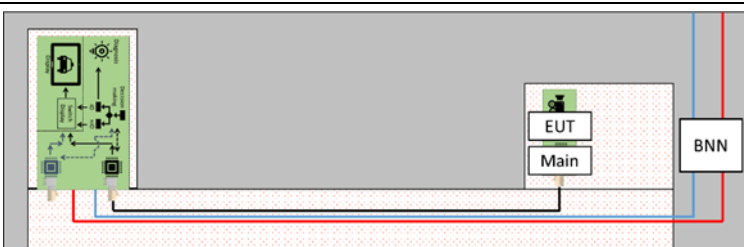
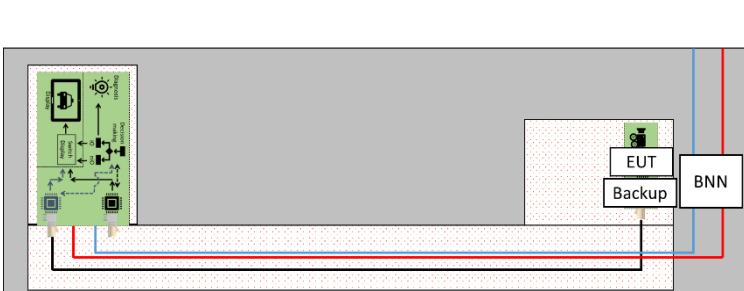
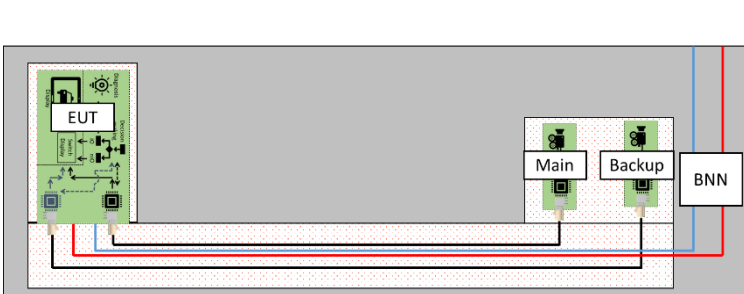
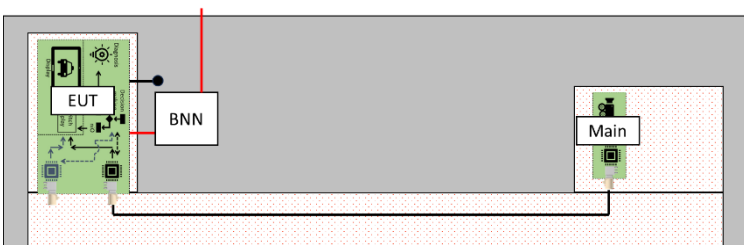
Die Komponenten des Systems sind mit Coax-Leitungen verbunden, die über Fakra-Stecker angeschlossen werden. Über diese Coax-Leitungen erfolgt auch die Spannungsversorgung der Kameraeinheiten 1 und 2. Für die Prüfungen wurden unterschiedliche Leitungslängen genutzt. Die Spannungsversorgung der Haupteinheit erfolgt über ungeschirmte Leitungen. Das Monitoring erfolgt für die EMV-Prüfungen über optische Leitungen.

9.7. EMV-Prüfungen

9.7.1. ISO 11452-2 Antennenmethode – Prüfaufbauten

Die Messungen haben die Prüfnummer TTR_04 mit der Zuordnung zu den jeweiligen Sicherheitszielen.



Setup 2 Aufbau mit beiden Kameramodulen (1,9 und 14 m) und langer Coax-Leitung; Main Channel 14 m; Masseleitung (local); Prüfling Haupteinheit	
Setup 3 Aufbau mit beiden Kameramodulen (1,9 und 14 m) und langer Coax-Leitung; Backup Channel 14 m; Masseleitung (local); Prüfling Haupteinheit	
Setup 4 Aufbau mit Kameramodul 1 (1,9 m Coax-Leitung) und langer Masseleitung (remote); Prüfling Haupteinheit	
Setup 5 Aufbau mit Kameramodul 2 (1,9 m Coax-Leitung) und langer Masseleitung (remote); Prüfling Haupteinheit	
Setup 6 Aufbau mit beiden Kameramodulen (2x 1,9 m Coax-Leitung) und langer Masseleitung (remote); Prüfling Haupteinheit	
Setup 7 Aufbau mit Einstrahlung auf Kameramodul 1 (2x 1,9 m Coax-Leitung) und kurzer Masseleitung; Prüfling Kameraeinheit Hauptkanal	

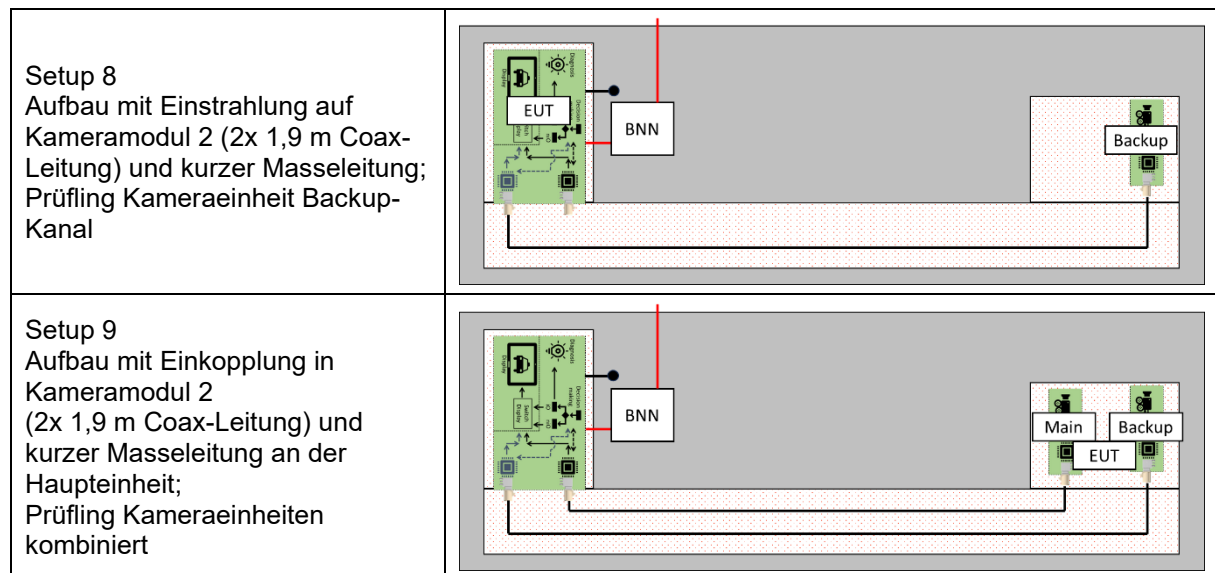


Tabelle 28 Schematische Darstellung der Messaufbauten für das Antennenprüfverfahren

Wie weiter oben beschrieben, werden sowohl die Haupteinheit als auch die Kameraeinheiten als EUT betrachtet. Damit ergeben sich die obigen Messkonfigurationen inklusive der Variation der Versorgungsleitungen. Zusätzliche Messungen sind ab 1 GHz notwendig, da hier die verwendete Hornantenne jeweils auf das EUT ausgerichtet wird. Für Messungen unterhalb von 1 GHz erfolgt die Ausrichtung der dort verwendeten logarithmisch-periodischen Antenne auf die Mitte des Kabelbaumes (Abbildung 31). Für beide Antennen sind jeweils für alle Positionen noch die Ausrichtungen vertikal und horizontal gefordert.

Die Signalleitungen haben dabei immer eine normgerechte Länge von 1,9 m, außer für die Setups 3 und 4. Diese Konfigurationen nutzen einen von der Normvorgabe abgeänderten Aufbau mit langer Coax-Leitung. Hintergrund hierfür ist, dass die Dämpfung der Signale – insbesondere für höhere Frequenzen – hier deutlich höher liegt. Durch die gleichbleibende Störeinkopplung sinkt der Signal-Rausch-Abstand. Das System wird empfindlicher gegenüber äußeren Einflüssen. Für den erwarteten Verbau im Fahrzeug ist von einer Leitungslänge größer 2 m auszugehen.

Für die nach der Sicherheitsanalyse geforderten Aufbauten mit nur einer Kameraeinheit, Setup 7 und 8, kann keine Kanalschaltung erfolgen, hier kann nur die Funktion anhand Diagnoseausgabe der Haupteinheit bewertet werden. Die Prüfaufbauten mit nur einem Datenkanal dienen der Kontrolle des Systemverhaltens unter Störeinfluss, wenn nur ein Kanal verfügbar ist.

Eine weitere Änderung kann sich aus dem geplanten Massekonzept im Fahrzeug ergeben. Die meisten Konfigurationen wurden mit einer kurzen Masseanbindung geprüft, da diese der im Projekt erwarteten Konfiguration im Fahrzeug entspricht.

Wie bereits dargelegt, ist die ISO 26262 lösungsorientiert. Das von der Normvorgabe abweichende Vorgehen kann, abhängig von der Leitungslänge der geplanten Applikation, eine Ergänzung zu den Prüfungen mit normgerechtem Leitungssatz darstellen, die auf der Expertise der EMV-Ingenieure oder Erfahrungen aus vorherigen Projekten beruht.



Abbildung 30
Beispiel ALSE-Prüfaufbau mit 1,9 m und 14 m
Leitung und LogPer-Antenne



Abbildung 31
Beispiel ALSE-Prüfaufbau mit 2x1,9 m
Leitungslänge mit Hornantenne

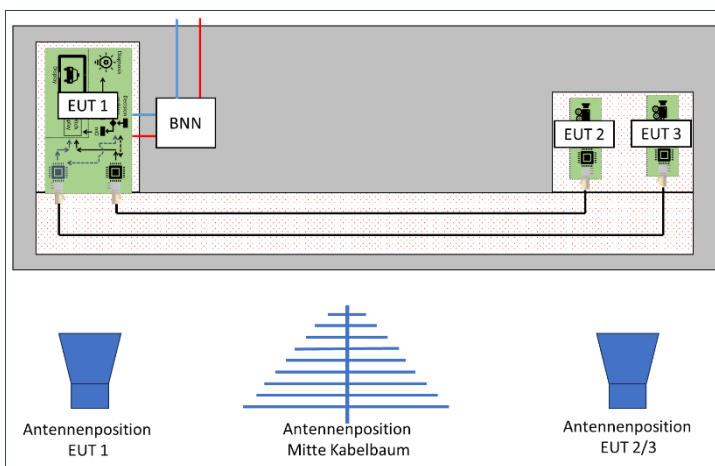


Abbildung 32
Notwendige Antennenpositionen
für die Prüfungen

Set-up	EUT	Einkopplung	Antenne	Prüfpegel	Modulation	Kanal-länge	Masse Haupteinheit
1	Haupteinheit	Main and Backup Channel	1, 2	Prüfpegel Level II und IV nach ISO 11452-2 + Erhöhung nach 5.10.5 mit Berücksichtigung der Messunsicherheit	CW, AM, PM	2x 1.9 m	local, kurz auf Masse
2	Haupteinheit	Main Channel				1x 14 m, 1x 1.9 m	local, kurz auf Masse
3	Haupteinheit	Backup Channel				1x 14 m, 1x 1.9 m	remote, über BNN
4	Haupteinheit	Main Channel				1x 1.9 m	remote, über BNN
5	Haupteinheit	Backup Channel				1x 1.9 m	local, kurz auf Masse
6	Haupteinheit	Main, Backup Channel, Versorgung				2x 1.9 m	remote, über BNN
7	Kameraeinheit 1	Main Channel				1x 1.9 m	kurz auf Masse an Haupteinheit
8	Kameraeinheit 2	Backup Channel				1x 1.9 m	kurz auf Masse an Haupteinheit
9	Kameraeinheit 1 + 2	Main, Backup Channel,				2x 1.9 m	kurz auf Masse an Haupteinheit

Antenne 1: logarithmisch-periodisch; Antenne 2: Hornantenne

Tabelle 29 Prüfmatrix Antennenprüfverfahren

9.7.2. ISO 11452-2 Antennenmethode – Ergebnisse

Die Prüfungen wurden nach dem Flowchart von Abbildung 28 mit der Monitoring-Software (Abbildung 29) durchgeführt. Damit waren durchgängig alle definierten Fehlerzustände und die Kanalschaltung detektierbar. Die Abregelung der Prüfgröße erfolgte automatisch, wenn beide Kanäle gleichzeitig Fehler aufweisen, die zu einer Verletzung der Sicherheitszeile (z.B. Aufrechterhaltung der Videoübertragung) führen. Fehler auf einem Kanal, die zu einer Umschaltung auf den redundanten Pfad führen, werden für die Abregelung nicht berücksichtigt.

Die Ergebnisse werden hier für den Prüfpegel von ASIL D mit dem Wert für Level IV aus der Norm verglichen.

Für die Prüfungen ergibt sich

Prüfpegel 100 V/m, ISO 11452-2 Level IV:

- kein Funktionsverlust für alle Prüfungen
- keine internen Fehler, auch keine Corrected Errors im Monitoring

Prüfpegel 126 V/m, erhöht um Messunsicherheit:

- reduzierte Störfestigkeit für die Setups 2, 3, 4, 5, 6 mit Haupteinheit als EUT bei Frequenzen ab 1000 MHz mit ohne Modulation (CW) durch Fehler Videoübertragung beider Kanäle
- Bemerkungen:
 - Setup 4, 5 haben nur 1 Kanal daher kann keine Umschaltung erfolgen
 - Setup 2, 3 haben jeweils 14-m-Kanal mit schlechterem Signal-Rausch-Verhältnis

Das Sicherheitsziel, einen sicheren Zustand einzuhalten, wurde eingehalten. Die Sicherheitsziele die Videoübertragung während allen Prüfungen aufrechtzuhalten, wurde nicht für alle Prüfungen erreicht. Die interne Diagnose der Übertragungstechnologien zeigt bereits Fehler, bevor es zu einem Funktionsverlust kommt.

Die zusätzlichen Prüfungen mit längeren Datenleitungen und die angepassten

Prüfschärfegraden haben eine kritische Beeinflussungsschwelle aufgezeigt, die bei Nominalpegel nach Level IV nicht gefunden wurde.

Funktional ergeben sich durch den zeitweiligen Ausfall beider Videokanäle Abstriche. Die Abregelungen erfolgen bis unter die Schwelle von 100 V/m. Wie diese zu bewerten sind, kann sich projektbezogen unterscheiden. Die Folgemaßnahmen sollten auf eine Erhöhung der Störfestigkeit abzielen.

Die Ausfälle mit der verlängerten Leitung ergeben sich aus der deutlich höheren Dämpfung der Signale. Der Signal-Rausch-Abstand sinkt frequenzabhängig um bis 20 dB. Abhilfe kann hier eine Kanalauslegung mit geringerer Dämpfung durch Reduzierung der Leitungslänge oder Verwendung einer Leitung mit geringerer Dämpfung schaffen.

ASIL	Nominale Prüfschärfe [V/m]	Unsicherheit [dB]	Unsicherheit [%]	Erhöhte Prüfschärfe [V/m]
D	100	2	125,9	126

Tabelle 30 Verwendete Prüfpegel

EMV-Test-ID	Ergebnis	Ereignisse	Bemerkung
SG02_TTR04	bestanden mit Einschränkungen	Fehler Datenübertragung beide Kanäle: Sicherheitsmaßnahmen: Detektion: SM001 SM002 SM003 SM004 Reaktion: Safe state SS01	CRC- Error LOCK-Error FEC-Error Parity-Error inform upper system, restart transmission, send status (heartbeat)

Tabelle 31 Ergebnisse Prüfungen Antennenmethode

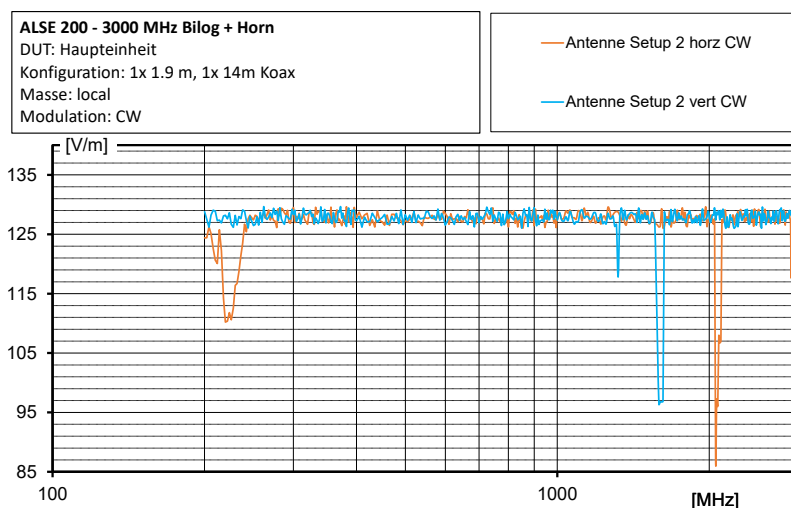


Abbildung 33

Zusammengefasste Prüfpegel für Antenne 1 und 2 für 126 V/m für Setup 2

Die Feldstärke von 126 V/m wird für die horizontale Polarisation zwischen 200 und 300 MHz nicht erreicht

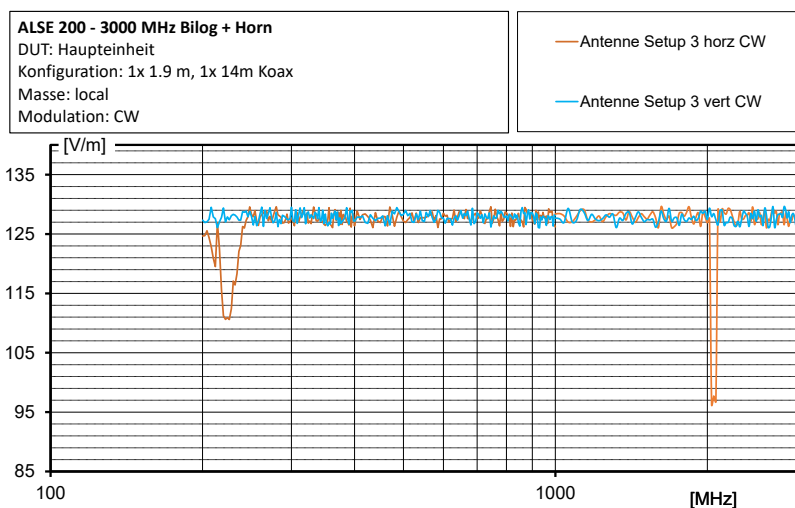


Abbildung 34

Zusammengefasste Prüfpegel für Antenne 1 und 2 für 126 V/m für Setup 3

Die Feldstärke von 126 V/m wird für die horizontale Polarisation zwischen 200 und 300 MHz nicht erreicht

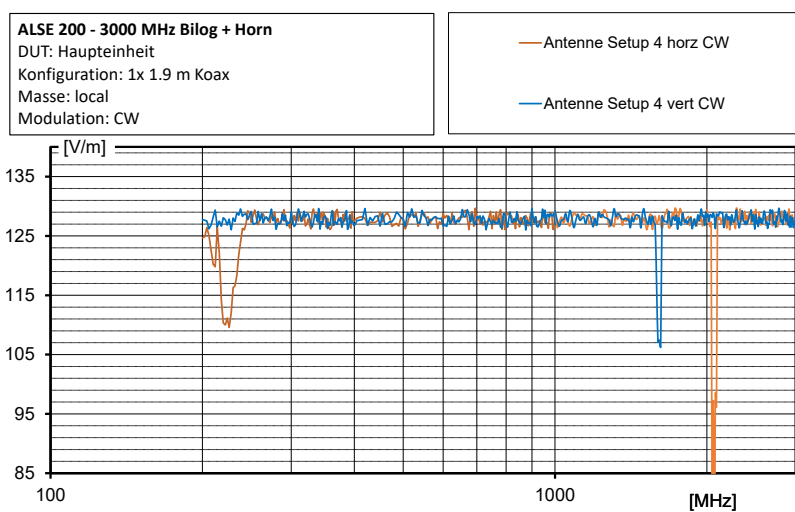


Abbildung 35

Zusammengefasste Prüfpegel für Antenne 1 und 2 für 126 V/m für Setup 4

Die Feldstärke von 126 V/m wird für die horizontale Polarisation zwischen 200 und 300 MHz nicht erreicht

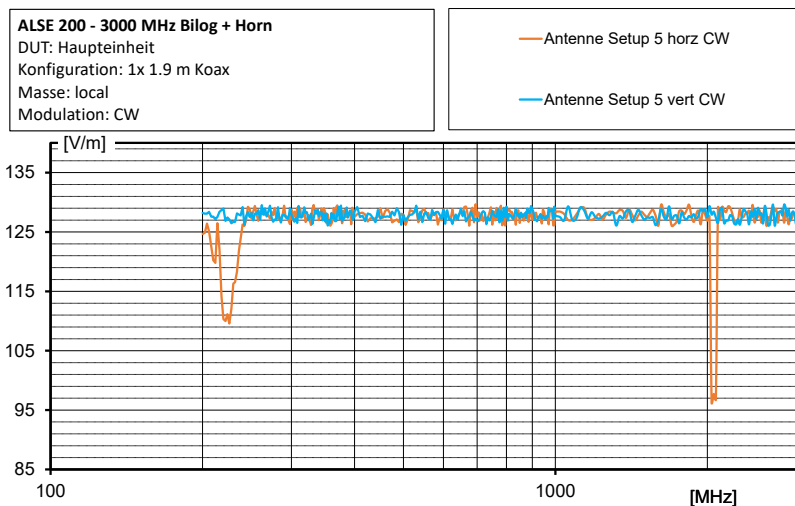


Abbildung 36

Zusammengefasste Prüfpegel für Antenne 1 und 2 für 126 V/m für Setup 5

Die Feldstärke von 126 V/m wird für die horizontale Polarisation zwischen 200 und 300 MHz nicht erreicht

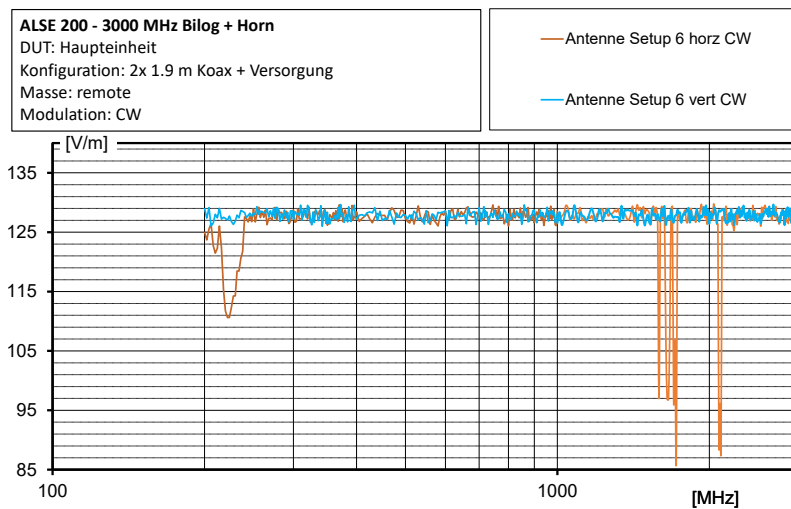


Abbildung 37

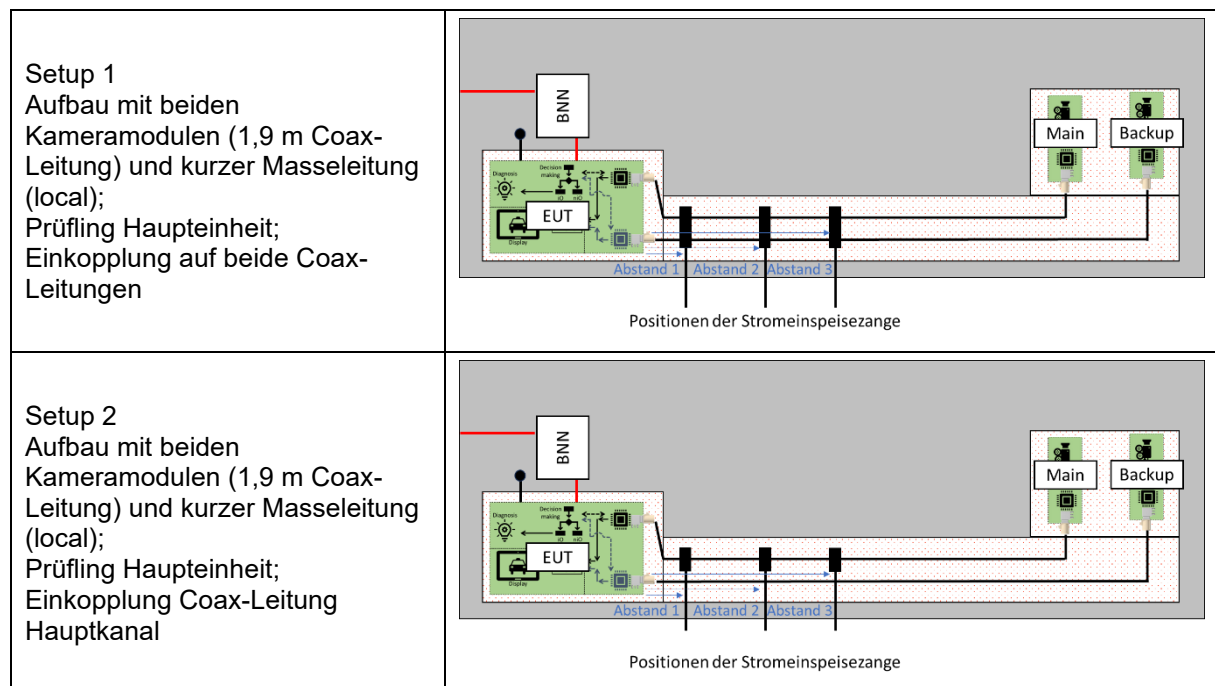
Zusammengefasste
Prüfpegel für Antenne 1
und 2 für 126 V/m für
Setup 6

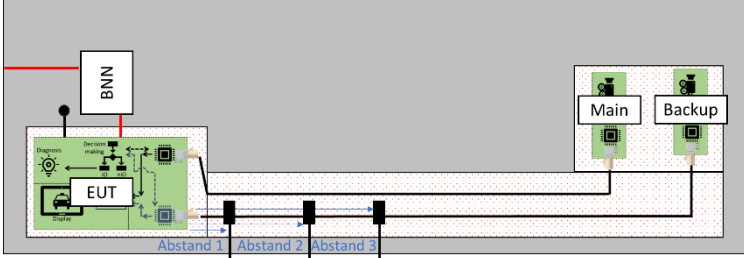
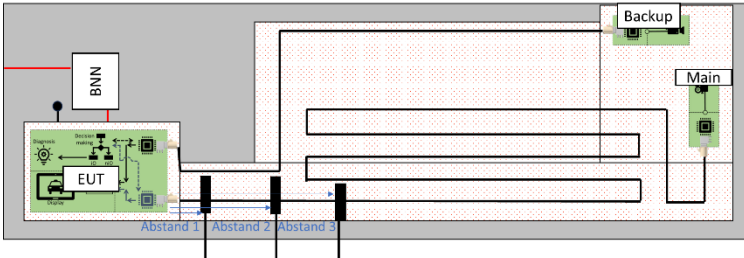
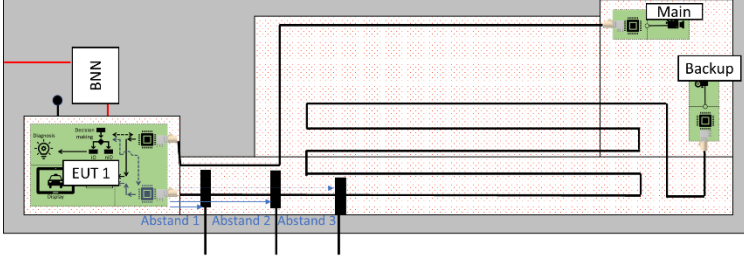
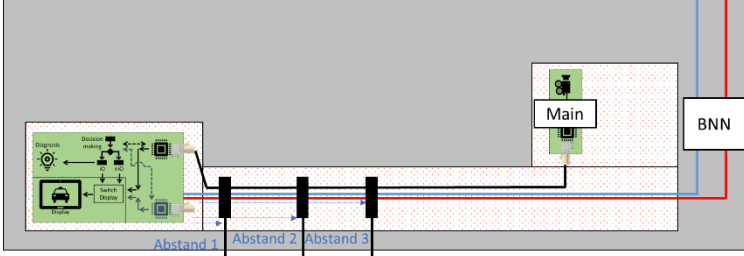
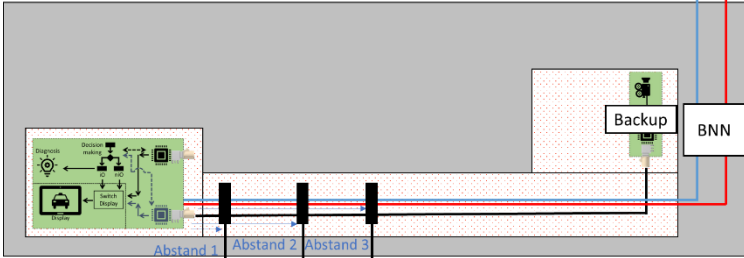
*Die Feldstärke von 126 V/m
wird für die horizontale
Polarisation zwischen 200 und
300 MHz nicht erreicht*

9.7.3. ISO 11452-4 BCI-Methode – Prüfaufbauten

Die Messungen haben die Prüfnummer TTR_03 mit der Zuordnung zu den jeweiligen Sicherheitszielen.

Die Prüflingsanordnungen für das Stromzangeneinspeiseverfahren gleichen denen für die Antenne. Es kommen bei den Aufbauten noch die vorgeschriebenen Zangenpositionen hinzu. Pro Messung sind 3 Positionen in verschiedenen Abständen zum EUT normativ aufgeführt. Da hier nach ISO 26262 die Haupteinheit als auch Kameramodule als EUT betrachtet werden müssen, ergeben sich pro Konfiguration 6 Zangenpositionen. Diese Erweiterung wird in der folgenden Übersicht dargestellt.



Setup 3 Aufbau mit beiden Kameramodulen (1,9 m Coax-Leitung) und kurzer Masseleitung (local); Prüfling Haupteinheit; Einkopplung Coax-Leitung Backup-Kanal	 Positionen der Stromeinspeisung
Setup 4 Aufbau mit beiden Kameramodulen (1,9 und 14 m) und langer Coax-Leitung; Main Channel 14 m; Masseleitung (local); Prüfling Haupteinheit; Einkopplung Coax-Leitung Hauptkanal	 Positionen der Stromeinspeisung
Setup 5 Aufbau mit beiden Kameramodulen (1,9 und 14 m) und langer Coax-Leitung; Backup Channel 14 m; Masseleitung (local); Prüfling Haupteinheit; Einkopplung Coax-Leitung Backup-Kanal	 Positionen der Stromeinspeisung
Setup 6 Aufbau mit Kameramodul 1 (1,9 m Coax-Leitung) und langer Masseleitung (remote); Prüfling Haupteinheit; Einkopplung auf Coax Hauptkanal und Versorgungsleitungen	 Positionen der Stromeinspeisung
Setup 7 Aufbau mit Kameramodul 2 (1,9 m Coax-Leitung) und langer Masseleitung (remote); Prüfling Haupteinheit; Einkopplung auf Coax Backup-Kanal und Versorgungsleitungen	 Positionen der Stromeinspeisung

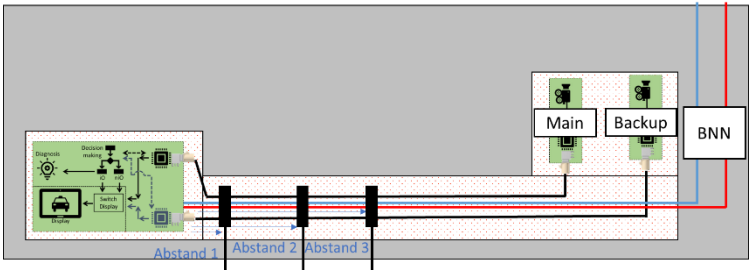
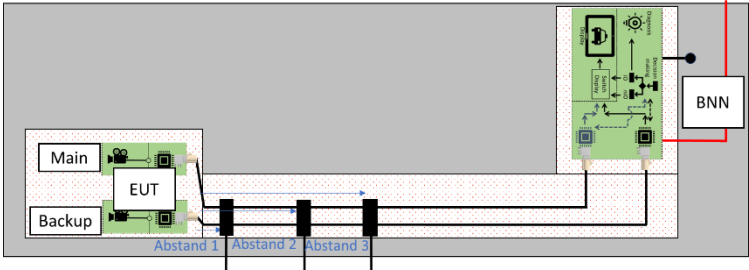
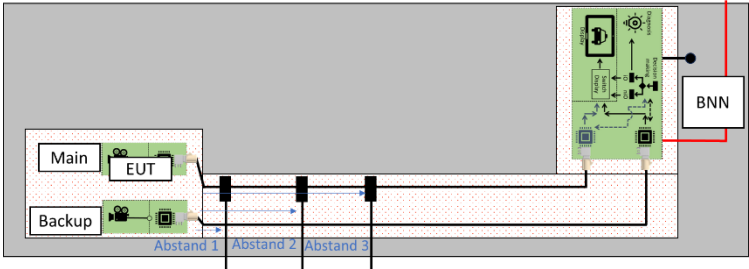
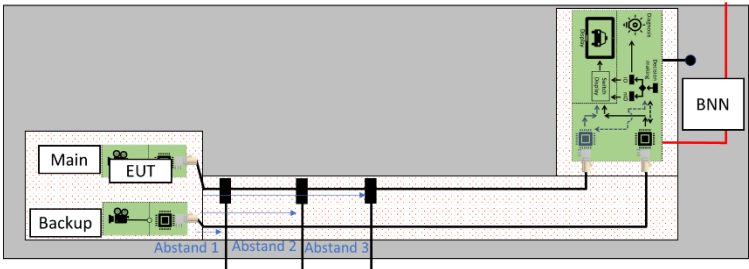
Setup 8 Aufbau mit beiden Kameramodulen (1,9 m Coax-Leitung) und langer Masseleitung; Prüfling Haupteinheit; Einkopplung auf Coax- und Versorgungsleitungen	 Positionen der Stromeinspeisestelle
Setup 9 Aufbau mit Einkopplung in beide Kameramodule (2x 1,9 m Coax-Leitung) und kurzer Masseleitung an der Haupteinheit; Prüfling Kameraeinheit; Einkopplung auf beide Coax-Leitungen	 Positionen der Stromeinspeisestelle
Setup 10 Aufbau mit Einkopplung in Kameramodul 1 (2x 1,9 m Coax-Leitung) und kurzer Masseleitung an der Haupteinheit; Prüfling Kameraeinheit Hauptkanal; Einkopplung Coax-Leitung Hauptkanal	 Positionen der Stromeinspeisestelle
Setup 11 Aufbau mit Einkopplung in Kameramodul 2 (2x 1,9 m Coax-Leitung) und kurzer Masseleitung an der Haupteinheit; Prüfling Kameraeinheit Backup-Kanal; Einkopplung Coax-Leitung Backup-Kanal	 Positionen der Stromeinspeisestelle

Tabelle 32 Übersicht Zangenpositionen BCI

Set-up	EUT	Einkopplung	Einkoppel- punkte	Prüfpegel	Modulation	Kanal- länge	Masse Haupteinheit
1	Haupteinheit	Main + Backup Channel	1, 2, 3	Prüfpegel Level IV nach ISO 11452-4 + Erhöhung nach 5.10.5 mit Berücksichtigung der Messunsicherheit	CW, AM	2x 1.9 m	local, kurz auf Masse
2	Haupteinheit	Main Channel				2x 1.9 m	local, kurz auf Masse
3	Haupteinheit	Backup Channel				2x 1.9 m	local, kurz auf Masse
4	Haupteinheit	Main Channel				1x 14 m, 1x 1.9 m	local, kurz auf Masse
5	Haupteinheit	Backup Channel				1x 14 m, 1x 1.9 m	local, kurz auf Masse
6	Haupteinheit	Main + Backup Channel, Versorgung				2x 1.9 m	remote, über BNN
7	Kameraeinheit	Main Channel				1x 1.9 m	remote, über BNN
8	Kameraeinheit	Backup Channel				1x 1.9 m	remote, über BNN
9	Kameraeinheit	Main + Backup Channel				2x 1.9 m	kurz auf Masse an Haupteinheit
10	Kameraeinheit	Main Channel				2x 1.9 m	kurz auf Masse an Haupteinheit
11	Kameraeinheit	Backup Channel				2x 1.9 m	kurz auf Masse an Haupteinheit

Tabelle 33 Prüfmatrix BCI-Prüfung



Abbildung 38
Beispiel Prüfaufbau BCI EUT Haupteinheit



Abbildung 39
Beispiel Prüfaufbau BCI EUT Kameraeinheit
(Serializer)

9.7.4. ISO 11452-4 BCI-Methode – Ergebnisse

Für alle geprüften Aufbauten und Prüfpegel traten keine Fehler auf. Es erfolgten auch keine internen Fehlereinträge während der Tests.

ASIL	Nominale Prüfschärfe [dB μ A]	Unsicherheit [dB]	Unsicherheit [%]	Erhöhte Prüfschärfe [dB μ A]
D	106	3,5	48,3	109,5

Tabelle 34 Verwendete Prüfpegel

EMV-Test-ID	Ergebnis	Bemerkung
SG01_TTR03	bestanden	keine Fehler
SG02_TTR03	bestanden	keine Fehler
SG03_TTR03	bestanden	keine Fehler
SG04_TTR03	bestanden	keine Fehler
SG05_TTR03	bestanden	keine Fehler

Tabelle 35 Ergebnisse Prüfungen BCI-Methode

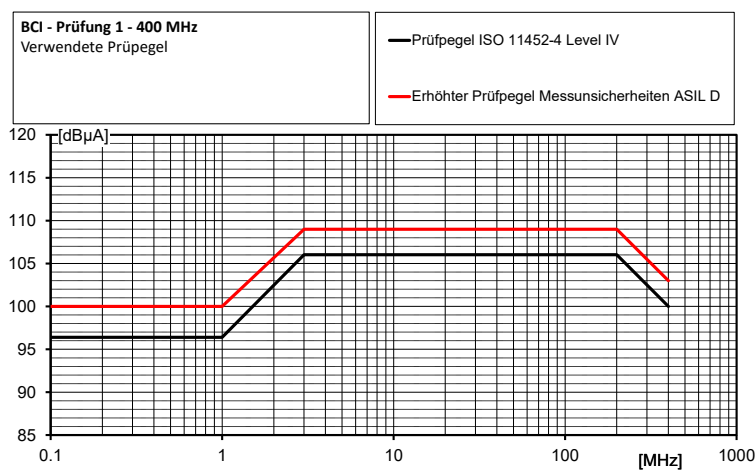


Abbildung 40

Verwendete Prüfpegel
für den
BCI-Prüfstrom in dB μ A
über der Frequenz in
MHz

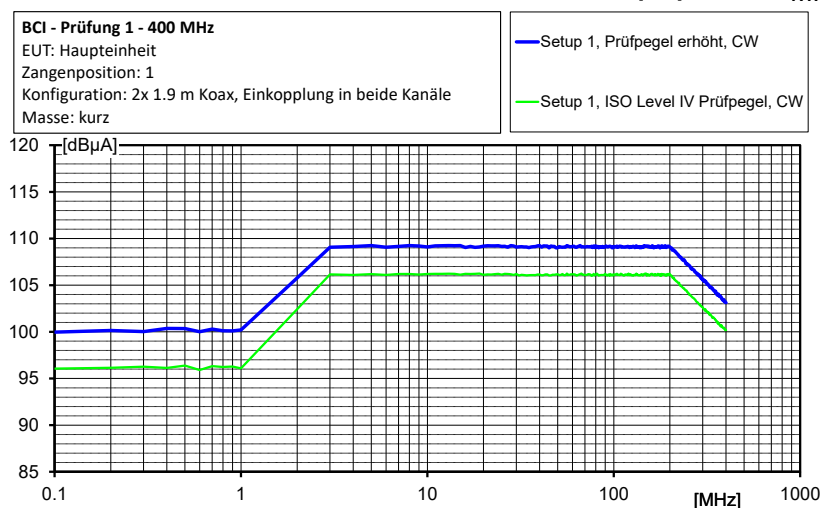


Abbildung 41

BCI-Prüfungen,
Setup 1
Vergleich
Prüfpegel

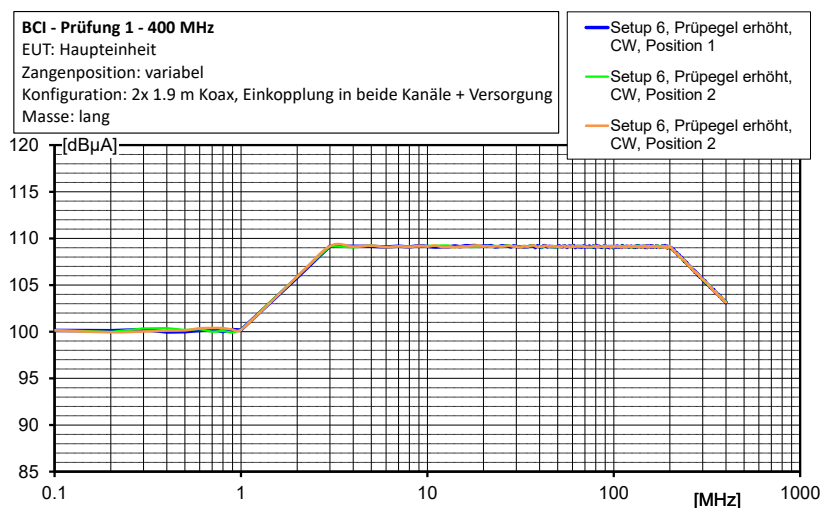


Abbildung 42

BCI-Prüfungen,
 Setup 6
 Vergleich
 Koppelpunkte

9.7.5. ISO 7637-3 – Impulsförmige Störgrößen – Prüfaufbauten

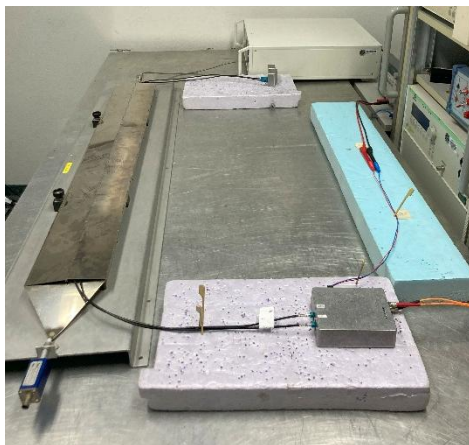
In Abweichung zu den Festlegungen in den TTR wurden für die Prüfungen nur die schnellen Pulse 3a und 3b ausgewählt, da im Projekt vor allem der Fokus auf der Kanalschaltung im möglichen Fehlerfall lag. Die Einkopplung erfolgt mit der kapazitiven Koppelzange (CCC). Diese Prüfungen werden somit nur im vorliegenden Projektbezug nicht betrachtet. Dies umfasst keinen generellen Ausschluss.

Schematische Darstellung der Leitungskonfigurationen für die Kapazitive Koppelzange nach ISO 7637-3 für beide Kameramodule	
Schematische Darstellung der Leitungskonfigurationen für die Kapazitive Koppelzange nach ISO 7637-3 für 1 Kameramodul (Hauptkanal)	
Schematische Darstellung der Leitungskonfigurationen für die Kapazitive Koppelzange nach ISO 7637-3 für 1 Kameramodul (Rückfallkanal)	

Tabelle 36 Übersicht Messkonfigurationen ISO 7637-3

Set-up	EUT	Einkopplung	Ltg. in CCC	Prüfpegel	Pulse	Kanal-länge	Masse Haupteinheit
1	Haupteinheit	Main and Backup Channel	1, 2	Prüfpegel Level IV nach ISO 7637-3 + Erhöhung nach 5.10.5 mit Berücksichtigung der Messunsicherheit	3a, 3b	2x 1.9 m	Power Supply
2	Haupteinheit	Main Channel	1			1x 1.9 m	
3	Haupteinheit	Backup Channel	2			1x 1.9 m	
4	Kameraeinheit	Main Channel	1			1x 1.9 m	
5	Kameraeinheit	Backup Channel	2			1x 1.9 m	
6	Kameraeinheit	Main and Backup Channel	1, 2			2x 1.9 m	

Tabelle 37 Prüfmatrix Pulse auf Signalleitungen ISO 7637-3

Abbildung 43
Beispiel Prüfaufbau mit kapazitiver Koppelzange

9.7.6. ISO 7637-3 – Leitungsgebundene Störungen – Ergebnisse

Es wurde Prüfungen mit den in Tabelle 34 aufgeführten Setups und den Prüfschärfegraden Level IV aus der ISO 7637-3 und ermittelter Amplitudenerhöhung nach Tabelle 36 und 37. Für alle geprüften Aufbauten und Prüfpegel traten keine Fehler auf. Es erfolgten auch keine internen Fehlereinträge während der Tests.

Für die Berücksichtigung der Messunsicherheiten wurde auf den Kalibrierbericht des Generators sowie auf generelle Angaben zur kapazitiven Koppelzange vom Hersteller zurückgegriffen. Es resultiert eine notwendige Erhöhung um 18% zum Pulswert für ISO 7637-3 Level IV.

Damit ergeben sich für

- 3a – Normativer Wert (Level IV): -110 V, erhöhter Wert: -130 V
- 3b – Normativer Wert (Level IV): +75 V, erhöhter Wert: +90 V

Einflussgröße	Symbol	Unsicherheit	Verteilung	Divisor d	c_i	$u_i(x_i)$	$u_i(y)$	Quelle
Beitrag vertikaler Messbereich Scope	V_{pr}	0,02	Dreieck	2,45	10	0,008	0,08 V	IEC 61000-4-4
Gleichstromdämpfung des Tastkopfes	A	0,5	Rechteck	1,73	1	0,29	0,08 V	IEC 61000-4-4
Wiederholbarkeit der Prüfung	δR	0,03	Normal	1	100	0,3	0,09 V	IEC 61000-4-4
Gleichstromdämpfung Messsystem	δV	0,02	Rechteck	1,73	100	0,01	1,15 V	IEC 61000-4-4

Maximale Abweichung Spannungswert U_s (6%) Generator 3a/3b	V_{US}	0,006	Rechteck	1,73	100	0,035	3,50 V	Kalibrierzertifikat
Maximale Abweichung Spannungswert U_s (4,22%) CCC	V_{UCC}	0,00422	Rechteck	1,73	100	0,024	2,40 V	Herstellerangabe
Sprungantwort des Messsystems	β	0,8 MHz	Rechteck	1,73	0,462 V/MHz	0,328	0,152 V	IEC 61000-4-4
-3-dB-Bandbreite des Messsystems	B	30 MHz	Rechteck	1,73	0,006 V/MHz	17,32	0,01 V	IEC 61000-4-4
Kombinierte Standardunsicherheit							7,5 V ^{*1)}	

*1) Der ermittelte Wert gilt für eine Amplitude von absolut 100 V gemessen mit einem 10:1 Tastkopf

Tabelle 38 Messunsicherheiten des verwendeten Generators als Grundlage für die Erhöhung der Prüfgrößen für 3a und 3b

ASIL	Erhöhungsfaktor Testlevel	Resultierender Wert mit ermittelter kombinierter Standardunsicherheit
D	2,32	18 %

Tabelle 39 Messunsicherheiten des verwendeten Generators als Grundlage für die Erhöhung der Prüfgrößen für 3b

EMV-Test-ID	Ergebnis	Bemerkung
SG01_TTR06	bestanden	keine Fehler
SG02_TTR06	bestanden	keine Fehler
SG03_TTR06	bestanden	keine Fehler
SG04_TTR06	bestanden	keine Fehler
SG05_TTR06	bestanden	keine Fehler

Tabelle 40 Ergebnisse Prüfungen ISO 7637-3

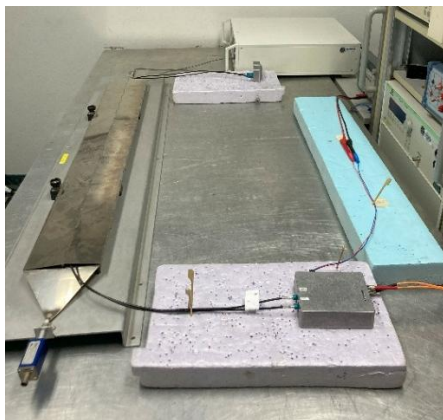
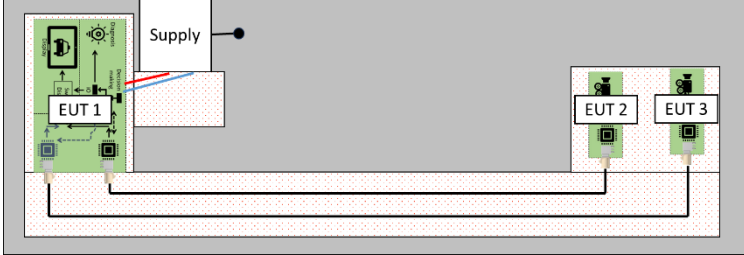
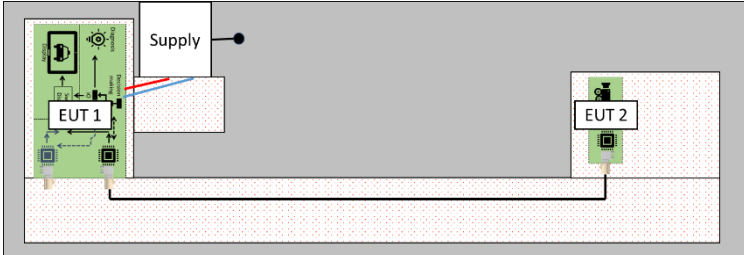
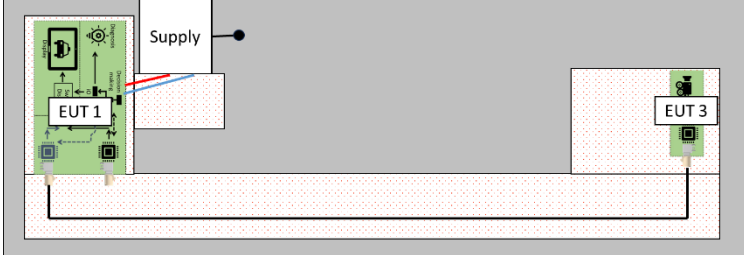
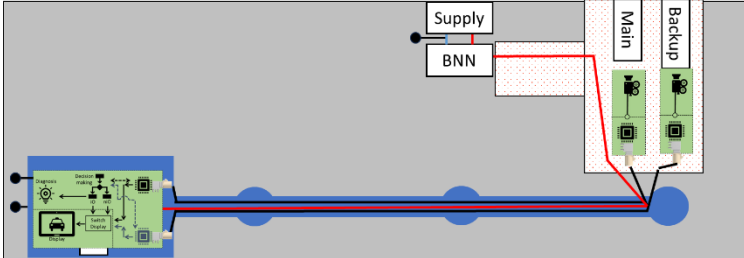
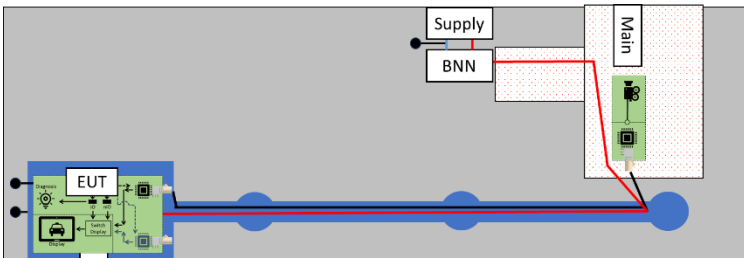
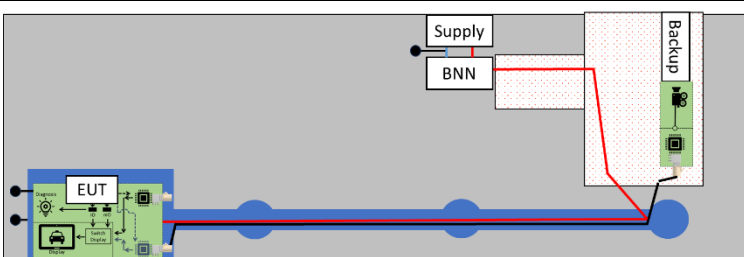


Abbildung 44
Beispiel Prüfaufbau mit kapazitiver Koppelzange

9.7.7. ISO 10605 elektrostatische Entladungen – Prüfaufbauten

Für die Prüfung der Störfestigkeit gegenüber elektrostatischen Entladungen wird die TTR-Zuordnung TTR09 genutzt. Es sind normativ zwei Setups definiert, jeweils mit und ohne Koppelplatte. Die Konfiguration ohne Koppelplatte dient im Projekt zur direkten Entladung in zugängliche Teile des Systems. Die andere Variante wird für diese Prüfungen zur indirekten Entladung genutzt. Die Entladungen erfolgen an vorgeschriebenen Stellen auf die Koppelplatte entlang des Kabelbaums.

Setup 1 Schematische Darstellung der Konfiguration ohne Koppelplatte	
Setup 2 Schematische Darstellung der Konfiguration ohne Koppelplatte für 1 Kanal	
Setup 3 Schematische Darstellung der Konfiguration ohne Koppelplatte für 1 Kanal	
Setup Koppelplatte 1 Schematische Darstellung der Konfiguration mit Koppelplatte und der Haupteinheit als EUT Massebezug auf Referenzpunkt der Masseplatte	
Setup Koppelplatte 2 Schematische Darstellung der Konfiguration mit Koppelplatte und der Haupteinheit als EUT für 1 Kanal	
Setup Koppelplatte 3 Schematische Darstellung der Konfiguration mit Koppelplatte und der Haupteinheit als EUT für 1 Kanal	

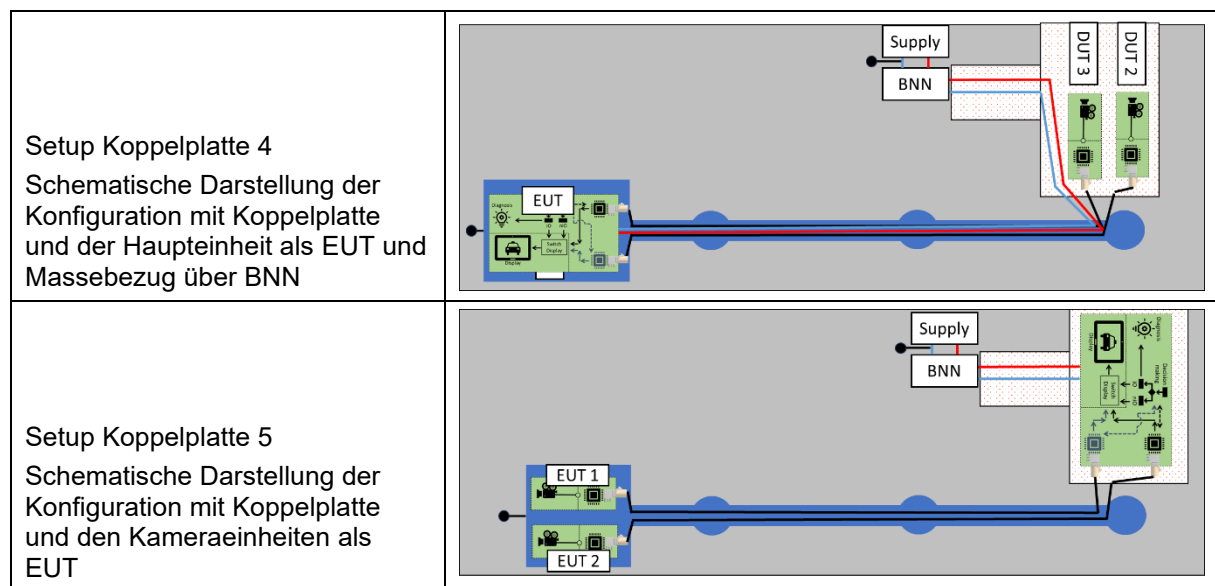


Tabelle 41 Übersicht Konfigurationen für elektrostatische Entladungen

Für die Untersuchungen wurde auch die Masseanbindung variiert:

- an der Haupteinheit über BNN auf Masse geführt (remote),
- Massebezug auf den Referenzpunkt der Koppelplatte gelegt (local).

Set-up	EUT	Einkoppelpunkte	Prüfpegel	Kanallänge	Masse Haupteinheit
1	System beide Kanäle aktiv	Stecker, Gehäuse Main und Backup Channel	Prüfpegel Level ISO 10605 Erhöhung bis Beeinflussung System	2x 1.9 m	Supply
2	System Hauptkanal aktiv	Stecker, Gehäuse Main und Backup Channel		1x 1.9 m	Supply
3	System Rückfallkanal aktiv	Stecker, Gehäuse Main und Backup Channel		1x 1.9 m	Supply

Tabelle 42 Prüfmatrix Konfigurationen für elektrostatische Entladungen ohne Koppelplatte

Setup	EUT	Einkopplung	Einkoppel-punkte	Prüfpegel	Kanallänge	Masse Haupteinheit
1	Haupteinheit	Main and Backup Channel	1, 2, 3	Prüfpegel Level ISO 10605 Erhöhung bis Beeinflussung System	2x 1.9 m	local
2	Haupteinheit	Main Channel			1x 1.9 m	local
3	Haupteinheit	Backup Channel			1x 1.9 m	local
4	Haupteinheit	Main, Backup Channel, Versorgung			2x 1.9 m	remote
5	Kameraeinheit	Main Channel			2x 1.9 m	BNN, auf GP
6	Kameraeinheit	Backup Channel			2x 1.9 m	BNN, auf GP

Tabelle 43 Prüfmatrix Konfigurationen für elektrostatische Entladungen mit Koppelplatte



Abbildung 45
Beispiel ESD-Prüfaufbau mit Koppelplatte

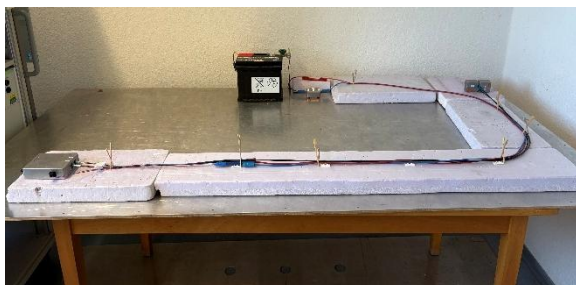


Abbildung 46
Beispiel ESD-Prüfaufbau ohne Koppelplatte

9.7.8. ISO 10605 elektrostatische Entladungen – Ergebnisse

ISO 10605 Bewertungskriterien

Nach Norm wird das erreichte Ergebnis bei den Prüfungen in Prüfschärfegrade unterteilt, die sich in dem Funktionsstatus unterscheiden, der bei Störeintrag aufrechterhalten wird. Zusätzlich ist noch eine Einteilung in Kategorien möglich. Die Definitionen der Funktionsstatus sind in Abschnitt 5.10.9 aufgeführt.

Funktionsstatus	Prüfschärfegrad
Status I, II, III erlaubt	L_{4i}
Status I, II erlaubt	L_{3i}
Status I erlaubt	L_{3i}
Uneingeschränkte Funktion	L_{1i}

Abbildung 47 Zuordnung Funktionsleistungsstatus und Prüfschärfegrade nach ISO 10605
Index i referenziert die Kategorie nach ISO 10605

ISO 10605 Prüfergebnisse

Während der Prüfungen traten keine Beschädigungen auf und das System kehrte auch bei Auftreten von Fehlern wieder in den nominalen Zustand zurück.

Für die indirekten Entladungen gibt es einen Sicherheitsabstand zwischen dem Auftreten erster interner Fehler und der Beeinflussung der Videoübertragung. Die Fehlerdetektion funktionierte für alle Prüfungen.

Für die direkten Entladungen lag die Beeinflussungsschwelle für die internen Fehler und den Funktionsverlust gleich. Die kritischen Schwellen unterschieden sich nur geringfügig (1kV) zwischen den gewählten Setups. Ein erhöhter Vertrauensbereich der Messungen konnte durch das Vorgehen und die Diagnosemaßnahmen bei diesem Verfahren nicht erreicht werden.

Erreichte Prüfschärfgrade für systeminterne Fehlererkennungs- und Behandlungsroutinen

EMV-Test-ID	Ergebnis direkte Entladung	Ergebnis indirekte Entladung	Bemerkung
SG01_TTR09	L ₁₁	L ₃₁	Fehlerregistereinträge, Fehler ein Datenkanal, Kanalschaltung
SG02_TTR09	L ₁₁	L ₃₁	Fehlerregistereinträge, Fehler ein Datenkanal, Kanalschaltung
SG03_TTR09	L ₁₁	L ₃₁	Fehlerregistereinträge, Fehler ein Datenkanal, Kanalschaltung
SG04_TTR09	L ₁₁	L ₃₁	Fehlerregistereinträge, Fehler ein Datenkanal, Kanalschaltung
SG05_TTR09	L ₁₁	L ₃₁	Fehlerregistereinträge, Fehler ein Datenkanal, Kanalschaltung

Tabelle 44 Ergebnis für Prüfungen gegenüber elektrostatischen Entladungen – interne Fehler

Erreichte Prüfschärfgrade für Funktionserhalt (Videoübertragung)

EMV-Test-ID	Ergebnis direkte Entladung	Ergebnis indirekte Entladung	Bemerkung
SG01_TTR09	L ₁₁	L ₄₁	Fehler beide Datenkanäle, Fehlerdetektion und -meldung
SG02_TTR09	L ₁₁	L ₄₁	Fehler beide Datenkanäle, Fehlerdetektion und -meldung
SG03_TTR09	L ₁₁	L ₄₁	Fehler beide Datenkanäle, Fehlerdetektion und -meldung
SG04_TTR09	L ₁₁	L ₄₁	Fehler beide Datenkanäle, Fehlerdetektion und -meldung
SG05_TTR09	L ₁₁	L ₄₁	Fehler beide Datenkanäle, Fehlerdetektion und -meldung

Tabelle 45 Ergebnis für Prüfungen gegenüber elektrostatischen Entladungen – Systemverhalten

10. Zusammenfassung

Das Ziel der funktionalen Sicherheitsbewertung von E/E-Systemen ist die Minimierung von (lebensbedrohlichen) Risiken auf ein akzeptables Maß durch die systematische Ermittlung der Ursachen von Fehlfunktionen. Elektromagnetische Phänomene können Fehler auslösen. Die ISO 26262 fordert daher, dass diese Risiken im Rahmen der Gefahrenanalyse und Risikobewertung berücksichtigt werden. EMV und elektrostatische Entladungen (ESD) werden in 5 der 10 Teile der ISO 26262 referenziert. Die Betrachtung der EMV ist im gesamten Entwicklungsprozess notwendig. Eine enge Abstimmung zwischen EMV-Ingenieuren und den Experten für funktionale Sicherheit ist zwingend erforderlich.

Am Beispiel des Frontkamerasystems im Projekt wurde das Vorgehen von den HARA bis zu den EMV-Prüfungen abgebildet. Bei der Entwicklung des Demonstrators wurden systematisch Maßnahmen zur Einhaltung der Vorgaben aus der Sicherheitsbewertung, wie die ASIL-Dekomposition, angewendet. Es wurden die Schritte der Analyse exemplarisch aus Sicht der Safety und der EMV angewendet. Es wurde eine qualitative Analyse durchgeführt, die geringere Anforderungen an die Metriken stellt. Dieses Vorgehen wurde gewählt, um eine Möglichkeit aufzuzeigen, die Problematik der quantitativen Analysen für die Prüfungen zu vereinfachen.

Für die Messungen wurden verschiedene Ansätze aufgeführt, die den Vertrauensbereich der Ergebnisse erhöhen sollen, wie interne Fehlerdiagnose, Anpassung der Prüfaufbauten an die Applikation im Fahrzeug und die Berücksichtigung von Messunsicherheiten. Diese wurden auch bei den Messungen angewendet. Andere Ansätze wie die Prüfung bis zur Ausfallschwelle und der abschließende Vergleich mit den Vorgaben wurden auf den Demonstrator nicht angewendet. Durch die Zusatzmaßnahmen konnten kritische Beeinflussungsschwellen aufgedeckt werden. Es ist im Rahmen der funktionalen Sicherheit nicht zwingend notwendig, Prüfpegel zu erhöhen.

Phase der Sicherheitsanalyse	Notwendige Informationen	Aktivitäten / Aufgaben EMV-Ingenieur
ITEM Definition	Definition elektromagnetische Randbedingungen (Worst-Case-Betrachtung) für Emission und Immunität	Definition der elektromagnetischen Randbedingungen (Worst-Case-Betrachtung) für Emissionen und Störfestigkeit; Definition der Anforderungen an die Betriebsumgebung des ITEM
Generelle Festlegungen	Projektlastenheft	Zuständigkeiten (inhouse, Zulieferer, Kunde), Budget, Zeitplan
HARA	Sicherheitsziele, Betriebsmodi, Szenarien für Einsatzbereich	EMV-relevante Fehlermodi mit Auswirkungen auf Sicherheitsziele, bekannte / erwartete Einwirkungen der elektromagnetischen Umgebung (Einsatzbereich), Aufstellung Worst-Case Inter-/Intrasystem EMV-Analyse
FTA	Definitionsgrad der Systemarchitektur	Ermittlung und Zuordnung EMV-bedingter Fehler zur Systemarchitektur, Common-Cause-Fehler-Analyse
FSC	Definitionsgrad der Systemarchitektur	Zuordnung EMV-bedingter Fehler zu den Sicherheitszielen

FMEA	Erfahrungen aus vorherigen Projekten, Erfahrung aus Prüfpraxis	Fehlermodi, Diagnosemechanismen (Test)
FMEDA	Erfahrungen aus vorherigen Projekten, Erfahrung aus Prüfpraxis	Mitarbeit bei Festlegung der Diagnoseabdeckung und erwartbaren EMV-bedingten Fehlerraten
TTR	Lastenheft, Risikoanalyse	Festlegung der Anforderungen an die EMV-Prüfungen und -Messungen
Verifikation and Validierung	Prüfplan, Experten Review	Experten Review: - Checklisten - Kontrollen - Revisionen Festlegung Prüfplan mit Grenzwertvorgaben und evtl. angepassten Randbedingungen, Durchführung EMV-Prüfungen, Dokumentation

Tabelle 46 EMV-Expertise im Sicherheitsprozess

Phasen	EMV-Prozessschritt	EMV-Prozess ohne funktionale Sicherheitsbetrachtung	EMV-Prozess unter Berücksichtigung der ISO 26262
Konzeption	Konzeptionsphase / Definition EMV-Anforderungen	EMV-Unterstützung bei Bauteilfestlegungen und Produktdesign, Analyse EMV-relevanter Fehler, evtl. FMEA	EMV-Unterstützung bei BauteilAuswahl, Leiterplattenlayout und Produktdesign, Fehleranalysemethoden nach ISO 26262, z.B. HARA, FMEA, FMEDA, FTA; Zuarbeiten von EMV-relevanten Fehlermöglichkeiten
Design	Designphase Entwicklung und Simulation	EMV-Unterstützung bei BauteilAuswahl, Leiterplattendesign, Massekonzept, Verkabelung, Simulation, EMV-Review Software	BauteilAuswahl, Leiterplattendesign, Massekonzepte, Verkabelung, Simulation, EMV-Review Software; Verfeinerung der Analysemethoden nach ISO 26262 auf Basis der Hard- und Softwareentwicklung, Zuarbeiten von EMV-relevanten Fehlermöglichkeiten, Unterstützung bei der Erstellung von Funktionalem Sicherheitskonzept and Technischem Sicherheitskonzept

Validierung Komponente	Prüfplan Komponente	Prüfplan mit Standardprüfungen nach Normvorgaben und kundespezifischen Vorgaben, Einhaltung von kundespezifischen Vorgaben (OEM-Lastenheft) und gesetzlichen Vorgaben; Präzisierung FMEA	Zuarbeit der EMV-relevanten Einflüsse für FMEA & FMEDA, Verifikations- und Validierungsplan mit Standardprüfungen nach Normvorgaben und kundespezifischen Vorgaben, evtl. Fehlerinjektionstests, evtl. erhöhte projektspezifische Anforderungen; Berücksichtigung der Sicherheitsziele und Safe States im Testplan und bei der Diagnose, Abstimmung zwischen OEM und Komponentenhersteller zu Diagnosemöglichkeiten für Sicherheitsziele und Safe States (Einhaltungskriterien, Timing, ...) auf Komponenten und Fahrzeugebene Zuordnung der Sicherheitsanforderungen zum Prüfplan, eindeutige Identifikation von Prüfungen (z.B. über Bezeichner (IDs) für Nachweisführung) Dokumentation von Prüfplänen; Prüfung von Möglichkeiten zur Erhöhung des Vertrauensbereiches der Prüfungen
	Validierungsphase / Prüfungen Komponente	Standardbedingungen, Prüfungen nach Prüfplan, Prüfberichte	Erweiterungen, Sicherheitsziele und Safe States als Fehlerkriterien, Nachweis dass die Anforderungen an die Sicherheitsziele, Diagnosemöglichkeiten für Sicherheitsziele und Safe States (Einhaltung, Timing, ...), Dokumentation von Prüfberichten; eindeutige Zuordnungen (Hardwarestände, Softwarestände, Prüfungen) im Sinne der Rückverfolgbarkeit
Integration	Integrationsphase	EMV-Unterstützung bei Festlegung Verbauort, Verkabelungskonzept, Massekonzept, Einbringen von Erfahrungen aus Vorläuferprojekten	EMV-Unterstützung des Sicherheitsteams, Zuarbeiten bei Festlegung Verbauort, Verkabelungskonzept, Massekonzept; rückverfolgbare Dokumentation von Änderungen in Hard- und Software wegen EMV, Einbringen von Erfahrungen aus Vorläuferprojekten

Validierung Fahrzeug	Prüfplan Gesamtfahrzeug	Standardprüfungen nach Normvorgaben, Einhaltung von Vorgaben (gesetzliche Anforderungen, zulassungsrelevante Anforderungen, OEM-Lastenheft)	Abstimmung OEM mit Lieferanten zu Sicherheitszielen Safe States und Diagnosemöglichkeiten auf Fahrzeugebene, Zuordnung der Sicherheitsanforderungen zum Prüfplan, evtl. erhöhte projektspezifische Anforderungen; Aufstellung der Konformitätsmatrix, einschließlich der Abdeckung von: Technischen Sicherheitsanforderungen und funktionalen Sicherheitsanforderungen
	Prüfungen Gesamtfahrzeug	Prüfungen nach Prüfplan; Einhaltung der Funktionszustände	Prüfungen nach Prüfplan, Diagnose der notwendigen Funktionen zu Einhaltung der Sicherheitsziele und Safe States; Nachweis der Einhaltung der Anforderungen an die Sicherheitsziele in Abstimmung OEM/Zulieferer
Alle Phasen	Dokumentation	EMV-Prüfberichte; Änderungsmanagement nach ISO 9001 mit Risikobewertung	EMV-Prüfberichte, Rückverfolgbarkeit erfordert verpflichtende Nachweisführung von Anforderung – Implementierung – Prüfung; Nachweise, dass die Sicherheitsanforderungen erfüllt sind (Prüfberichte, Testdaten, Pass/Fail-Kriterien) Auflistung aller verbleibenden Risiken und erforderliche Maßnahmen für den sicheren Betrieb, Protokollierung jeder Änderung an sicherheitsbezogener Software oder Hardware (z.B. EMV-Optimierung)

*1) zusätzliche Tests können auf Basis der HARA optional in den Testumfang aufgenommen werden

Tabelle 47 Vergleich der EMV-Prozesse mit und ohne Umfängen nach ISO 26262

Kurzbeschreibung Vorgehen

Die Einbeziehung von EMV-Expertise erfolgt in den Analyseschritten wie in Tabelle 46 gezeigt. Eine Übersicht über notwendige oder mögliche zusätzliche Umfänge im EMV-Prozess auf Basis der hier dargelegten Betrachtungen ist in der Tabelle 47 gegeben.

1. **ITEM-Definition:**
 - Zuarbeit EMV-Anforderungen aus geplanten Einsatzbereich und gesetzlichen Anforderungen
2. **HARA:**
 - Zuarbeit bekannter / erwarteter Einwirkungen der elektromagnetischen Umgebung auf Basis bekannter Randbedingungen des geplanten Einsatzbereiches
 - Aufstellung einer Worst-Case-EMV-Analyse (Inter-/Intrasystem)
 - Abschätzung EMV-relevanter Fehlermodi mit möglichen Auswirkungen auf Sicherheitsziele
3. **FTA:**
 - Ermittlung und Zuordnung EMV-bedingter Fehler zur Systemarchitektur
 - Common-Cause-Fehler-Analyse (EMV-bedingt)
4. **FSC:**
 - Zuordnung EMV-bedingter Fehler zu den Sicherheitszielen sowie zu der im vorliegenden Projektstand definierten Soft- und Hardware-Architektur des ITEM
5. **FMEA:**
 - Zuarbeit EMV-bedingter Fehlermodi und EMV-prüfungsrelevanter Diagnosemechanismen auf Basis der Erfahrungen aus vorherigen Projekten und Prüfpraxis
6. **FMEDA:**
 - Mitarbeit bei Festlegung der Diagnoseabdeckung und erwartbaren EMV-bedingten Fehlerraten mit Zuordnung zu den Architekturblöcken auf Basis der Erfahrungen aus vorherigen Projekten und Prüfpraxis (*Vorgehen bei qualitativer Analyse*)
7. **TTR:**
 - Festlegung der Anforderungen an die EMV-Prüfungen und -Messungen auf Basis der Lastenheft und Risikoanalyse (HARA)
8. **Verification und Validation:**
 - Experten Review: Checklisten, Kontrollen, Revisionen EMV-relevanter Umfänge
 - endgültige Festlegung Prüfplan mit Grenzwertvorgaben und evtl. angepassten Randbedingungen,
 - Durchführung EMV-Prüfungen:
 - Für die Bewertungskriterien während der Tests sind die Sicherheitsziele und die definierten Zustände des Prüflings maßgeblich:
 - Das EUT muss sich immer in einem definierten Zustand oder Betriebsmodus während und nach den Tests befinden.
 - Die PASS/FAIL-Entscheidung wird auf Systemebene auf Basis der festgelegten Sicherheitsziele getroffen.
 - Dokumentation Ergebnisse mit Beachtung der Rückführbarkeit über IDs oder Safety-tools
 - Rückführung von evtl. Fehlern auf definierte Sicherheitsmaßnahmen und Sicherheitszustände (safe states) des Prüflings

11. Anhang zu Messunsicherheiten

Die Messunsicherheit ist ein Schätzwert, der die Streuung angibt, innerhalb derer der richtige Wert des Messergebnisses liegt. Sinn und Zweck der Messunsicherheit ist es, diese Variabilität quantitativ zu fassen und in einem Zahlenwert auszudrücken.

Es gibt zwei Arten von Messunsicherheiten. Einmal den Typ A, der sich aus den statistischen Abweichungen von Messreihen ergibt, und den Typ B, der sich aus anderen Erkenntnissen ergibt, wie

- Daten und Ergebnisse aus vorangegangenen Messungen
- allgemeine Kenntnisse und Erfahrungen über die
- Eigenschaften und das Verhalten von Messinstrumenten und Materialien
- Herstellerangaben
- Kalibrierscheine oder anderen Zertifikate
- Referenzdaten / Literaturwerte

Alle Messungen unterliegen Unsicherheiten. Diese speisen sich aus allen Einflussgrößen auf die jeweilige Messung. Die Unsicherheiten lassen sich in zufällige und systematische Anteile untergliedern. Zufällige Anteile weichen bei Wiederholungen der Messungen unter gleichen Bedingungen in beide Richtungen um das eigentliche Ergebnis ab, systematische immer in die gleiche. Die Praxis zeigt, dass Messbedingungen nicht exakt angegeben und eingehalten werden können, damit eine exakte Ergebnismiederholung möglich ist. Die Abweichungen unterliegen statistischen Wahrscheinlichkeiten. Die Wahrscheinlichkeitsverteilung der Ergebnisse ergibt sich aus den statischen Grundlagen, die der Entstehung der Verteilung zugrunde liegen (siehe Abbildung 10 Relevante Messunsicherheitsverteilungen für EMV-Messungen).

Kalibrierung und Rückführbarkeit

Ein wesentliches Element zur Reduzierung von Messunsicherheiten ist die Kalibrierung der Messgeräte. Eine Kalibrierung stellt sicher, dass Messgeräte genaue und zuverlässige Ergebnisse liefern. Rückführbarkeit bedeutet, dass die Messergebnisse auf nationale oder internationale Standards zurückgeführt werden können, was die Vergleichbarkeit und Vertrauenswürdigkeit der Ergebnisse erhöht.

Gauß'sche Verteilung

Diese Verteilung, auch **Normalverteilung** genannt, tritt immer bei Typ A Unsicherheiten auf. Durch Wiederholungen ergibt sich die glockenförmige Verteilung der Ergebnisse um einen Mittelwert. Beispiele sind Unsicherheitsangaben auf Kalibrierscheinen.

$$u(x) = \sqrt{\sum_{i=1}^m u_i^2(x)} \quad (6)$$

Rechteckförmige Verteilung

Für einige Fälle lässt sich für die Abweichung nur die Ober- und Untergrenze a_+ und a_- angeben, wobei alle Werte innerhalb der Grenzen als gleich wahrscheinlich angesehen werden können.

Beispiel hierfür sind Angaben in Fehlergrenzen in Spezifikation und Datenblättern oder die digitale Auflösung in Softwareeingabefeldern oder Anzeigen.

$$u(x) = \frac{1}{2\sqrt{3}}(a_+ - a_-) = \frac{a}{\sqrt{3}} \quad (7)$$

Dreieckförmige Verteilung

Liegen die Werte mit größerer Wahrscheinlichkeit in der Mitte des Bereiches, nimmt man eine dreieckförmige Verteilung an.

Beispiel hierfür sind Interpolationsabweichungen.

$$u(x) = \frac{1}{2\sqrt{6}}(a_+ - a_-) = \frac{a}{\sqrt{6}} \quad (8)$$

U-förmige Verteilung

Wenn bei harmonischen Schwingungen keine Angaben über die Phase angegeben sind, dann ist für die Phase eine Rechteckverteilung anzunehmen. Mathematisch folgt daraus für die Amplitude eine U-förmige Verteilung.

Beispiele sind HF- und EMV-Messungen.

$$u(x) = \frac{a}{\sqrt{2}} \quad (9)$$

Kombinierte Messunsicherheit

Der beste Schätzwert für das Messergebnis ist der arithmetische Mittelwert aller ermittelten Werte. Die dazugehörige Messunsicherheit ergibt sich aus der Wurzel der Summe aller quadrierten Einzelabweichungen.

$$u_c(x) = \sqrt{u_1^2 + u_2^2 + \dots u_n^2} \quad (10)$$

Erweiterte Messunsicherheit

Die Standardmessunsicherheit ist eine universelle Größe zur Charakterisierung des Vertrauensintervalls eines Messergebnisses. Für den Nachweis der Konformität ist sie nur bedingt geeignet, da sie nur einen geringen Anteil der möglichen Messwerte umfasst und damit hohe Anforderungen an die Messbedingungen stellt. In Industrie und Wirtschaft wird daher aus praktischen Gründen mit der erweiterten Messunsicherheit gearbeitet. Hier wird der Vertrauensbereich der Ergebnisse erweitert. Dazu wird der Erweiterungsfaktor oder Überdeckungsfaktor k eingeführt (siehe Abbildung 11 Verteilung der Messergebnisse auf Grund der Gesamtmessunsicherheit).

$$U(x) = k * u_c(x) \quad (11)$$

Ziel ist ein Vertrauensbereich von 95 %. Der Faktor k muss dann durch eine detaillierte Analyse je nach der Verteilung der Ergebnisse gewonnen werden. Bei einer angenommenen oder approximierten Normalverteilung der Ergebnisse für die kombinierte Messunsicherheit ergibt sich der Faktor $k = 2$.

Sensitivitätskoeffizient

Der Sensitivitätskoeffizient ist ein Gewichtungsfaktor, der den Einfluss auf den Schätzwert der Ergebnisgröße durch Änderungen des Schätzwertes der Eingangsgröße angibt. Er kann aus Modellfunktionen oder numerisch ermittelt werden.

Messunsicherheitsbudget

Für das Messunsicherheitsbudget werden alle Einflussgrößen zusammengefasst. Für die Ermittlung des Gesamtbudgets werden die einzelnen Unsicherheiten mit den Angaben zur Verteilungsfunktion und den daraus resultierenden Divisoren, den Quellen der Gewichtung zusammengefasst.

Nachfolgend sind die Gesamtbudgets an Beispielen mit Werten aus Normen und teilweise für die Messtechnik am FTZ dargestellt. Diese EMV-Prüfverfahren nach ISO 26262 sind berücksichtigt:

1. ISO 11452-2 ISO: Road vehicles —Component test methods for electrical disturbances by narrowband radiated electromagnetic energy — Part 2: ALSE
2. ISO 11452-4: Road vehicles —Component test methods for electrical disturbances by narrowband radiated electromagnetic energy — Part 4: Bulk current injection (BCI)
3. ISO 7637-2: Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction/coupling
4. ISO 10605: Road vehicles — Test methods for electrical disturbances from electrostatic discharge

Die Berechnungen basieren im Wesentlichen auf den grundlegenden Dokumenten zu diesem Thema, sofern die oben genannten Normen keine Informationen dazu enthalten. Die grundlegenden Dokumente sind [22, 23, 24, 26, 27, 28]:

- The United Kingdom Accreditation Service (UKAS) LAB34:2002-08: The Expression of Uncertainty in EMC testing
- Leitfaden zur Angabe der Unsicherheit beim Messen, Originaltitel: Guide to the expression of uncertainty in measurement (GUM), DIN, Deutsches Institut für Normung e.V, Berlin; Wien; Zürich: Beuth, 1995
- Fachnormen, die Angaben zu Messunsicherheit enthalten.

Die Berechnungen müssen für jeden Aufbau mit der jeweils eingesetzten Technik bestimmt werden. Die dazu notwendigen Angaben lassen sich in den Herstellunterlagen und den Kalibrierberichten der jeweiligen Prüfgeräte finden. Damit kann man die Messunsicherheiten in vergleichsweise engen Grenzen festlegen. Ein weiterer möglicher Ansatz ist die Übernahme der Werte aus den o.g. Papieren. Damit lassen sich generelle Festlegungen treffen, welche den Messunsicherheitsbereich allerdings oft mit größeren Toleranzen definieren.

Die Berechnung der Erhöhung der Störpegel für die Prüfverfahren aus den Werten für die ASIL und die Messunsicherheiten ergeben sich für die Werte in dB folgende Berechnungsvorschriften nach [UKAS M3003 Edition 6 - The expression of uncertainty and confidence in measurement, 2024]:

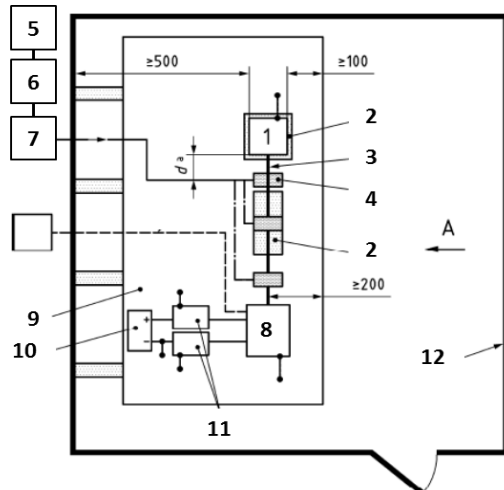
- Relativ kleine Unsicherheiten in dB können auf Grund des resultierenden geringen Fehlers direkt mit den Erhöhungsfaktoren in den Tabellen verrechnet werden.
- Das mathematisch korrekte Vorgehen ist, diese Werte in Prozentangaben zu wandeln, dann mit den Erhöhungsfaktoren in den Tabellen zu multiplizieren und die Ergebnisse dann wieder in dB umzurechnen.

Für die im unteren Teil von Tabelle A.1 aufgeführten Werte bedeutet die Anpassung auf die aus den entsprechenden Normen entnommenen Messunsicherheiten beispielsweise, dass für

- ASIL B der eingeregelter Feldstärkewert auf 114 V/m,
- ASIL C auf 122 V/m und
- ASIL D auf 126 V/m

bei einer nominell spezifizierten Testfeldstärke von 100 V/m angehoben muss.

Das ermittelte Messunsicherheitsbudget basiert auf der Annahme, dass während der Kalibrierung die 6 dB Feldgleichmäßigkeit erreicht wurde.

ISO 11452-4 – Bulk Current Injection

- 1 DUT
- 2 Isolierung
- 3 Testkabelsatz
- 4 BCI-Zange
- 5 Signalgenerator
- 6 HF-Verstärker
- 7 Leistungsmesser
- 8 Lastnachbildung
- 9 Masseplatte
- 10 Spannungsversorgung
- 11 BNN
- 12 Absorberkabine

Abbildung A.2 Störfestigkeit, BCI – Prüfaufbau auf Komponentenebene

Einflussgröße	Symbol	Unsicherheit in dB	Verteilung	Divisor d	c_i	$u(x_i)$	$u(x_i)^2$	Quelle
Kalibrierung ^{*1)}	δ_{CAL}	1,46	Normal	2	1	0,73	0,53	IEC 61000-4-6
Pegelmessgerät in der Regelungsschleife	δ_{LMC_t}	0,3	Rechteck	1,73	1	0,17	0,03	IEC 61000-4-6
Prüfgenerator ^{*2)}	δ_{TG_t}	0	Rechteck	1,73	1	0	0	IEC 61000-4-6
Fehlanpassung zwischen Prüfgenerator und Stromzange	δ_{MT_t}	0	U-förmig	1,41	1	0	0	IEC 61000-4-6
Präzision der Pegeleinstellung mittels Software	δ_{SW_t}	0,3	Rechteck	1,73	1	0,17	0,03	IEC 61000-4-6
Abschluss der Zusatz-/Hilfseinrichtung	δ_{AETERM}	2,5	Rechteck	1,73	1	1,45	2,09	IEC 61000-4-6
Reproduzierbarkeit des Betriebszustandes	R_{EUT}	0,0	Normal	1 ^{*3)}	1	0,00	0,0	UKAS Lab 34
Kombinierte Standardunsicherheit						1,64		

ASIL	Erhöhungsfaktor Testlevel	Resultierender Wert mit ermittelter kombinierter Standardunsicherheit [dB]
B	1,28	2,1
C	1,88	2,9
D	2,32	3,5

^{*1)} Unsicherheitsbudget der Kalibrierung, hier beispielhaft aus [25] übernommen

^{*2)} Abhängig davon, ob die Regelschleife die Ausgangswerte des Pegelmessgerätes oder des Prüfgenerators verwendet, gehen die jeweiligen Beiträge hier ein. Da das Beispiel die Beiträge des Pegelmessgerätes nutzt, wird der Beitrag für den Prüfgenerator auf 0 gesetzt.

^{*3)} Sollte der Einfluss des EUT bekannt sein, kann dieser hier mit dem entsprechenden Wert eingetragen werden, um die Aussagekraft der Berechnung zu verbessern.

Tabelle A.2 Ermittlung der Messunsicherheit und der Erhöhungsfaktoren für einen beispielhaften Aufbau nach ISO 11452-4

Beispielhafte Angaben zur Messunsicherheit für den BCI-Aufbau sind in [25] zu finden. Die Angaben beziehen sich auf den Aufbau, der vorher mit gleichen Prüfequipment im JIG kalibriert worden ist. Die Unsicherheiten der JIG-Pegeleinstellung sind in dem Beitrag δCAL zusammengefasst. Die Aufschlüsselung der Beiträge für δCAL hierzu ist in [25] dargelegt. Die Werte in der Tabelle A.2 gelten beispielhaft für einen Aufbau, der vorkalibrierte Stromwerte ohne Messstromzange in den Kabelbaum einprägt. Für den Aufbau mit Monitoring Clamp sind die Messunsicherheiten für die Messeinrichtung mit einzubeziehen. Beispielhafte Angaben hierfür sind in [22] zu finden.

ISO 7637-2/3 – Transienten

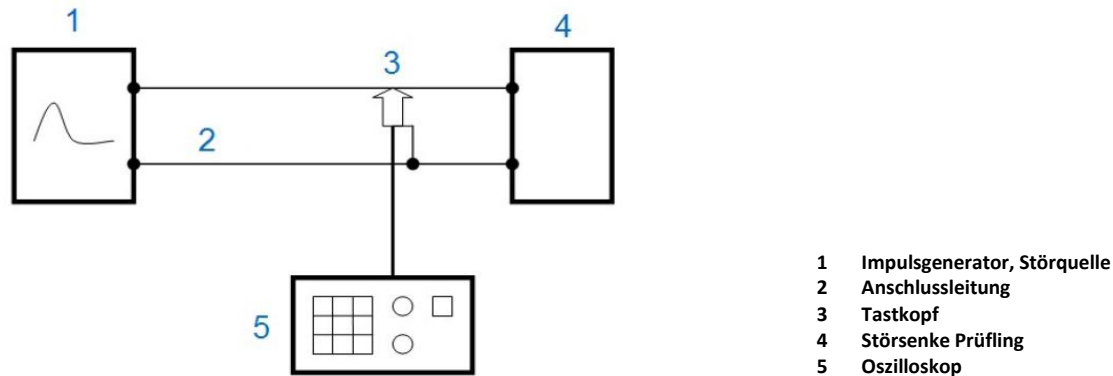


Abbildung A.3 Störfestigkeit, leitungsgeführt (Pulse) – Prüfaufbau auf Baugruppenebene

Der Standard ISO 7637 gibt Toleranzen für die Prüfparameter vor. In diesem Fall besagt die ISO 17025 (die Norm für Akkreditierung), dass die Anforderung zur Schätzung der Unsicherheit als erfüllt angesehen werden kann, wenn die Testmethode und ihre Berichtsanweisungen befolgt werden. Es ist dann nur noch erforderlich sicherzustellen, dass der verwendete Testgenerator tatsächlich den Anforderungen der Norm entspricht. Das ist konsistent mit dem in UKAS LAB 34 [22] angegebenen Vorgehen für transiente Störgrößen. Damit ist eine Angabe der Unsicherheitsbilanz für die Messungen formal nicht erforderlich. Für die Abschätzung der Ergebnisschwankungen in Bezug auf die funktionale Sicherheit kann dieses Vorgehen unzureichend sein.

Soll diese dennoch erfolgen, wird hier eine mögliche Vorgehensweise als Idee vorgestellt. Eine Herausforderung bei der Erstellung eines Unsicherheitsbudgets für Transientenimmunitätstests besteht darin, dass die Wechselwirkung zwischen den verschiedenen Zeit- und Amplitudenparametern, die für die Generatoren angegeben sind, nicht analysiert werden kann, um eine Gesamtunsicherheit für die angewandte Belastung abzuleiten. Darüber hinaus können Effekte wie Variationen in der Layoutgestaltung und Kopplungsimpedanzen Beiträge hinzufügen, die wiederum schwer zu analysieren sind. Da Generatoren normativ im Aufbau nicht definiert sind, können abweichende Ergebnisse in Abhängigkeit von der Impedanz des Prüflings mit verschiedener Prüftechnik auftreten.

Eine Abschätzung der Unsicherheiten kann daher nur für die Einhaltung der normativen Vorgaben der Prüfpulse bei der Verifikation der Prüftechnik erfolgen. Sind die Parameter des Generators bekannt, sollten diese verwendet werden. Für die Pulse sind Anstiegszeiten, Pulsdauer und Spitzwert der Amplitude in Abhängigkeit von Abschlussimpedanzen definiert. Das führt zu Unsicherheitsbilanzen für den jeweiligen Parameter.

Die Definition der Pulse nach [ISO 7637-2] lässt eine große Schwankungsbreite der Pulsformen als normkonform zu. Damit ergeben sich große Abweichungen in den

resultierenden Werten für die Pulsleistung und -energie. Das ist hier am Beispiel von Testpuls 1 mit $U_s = 100\text{ V}$ und $R_i = R_L = 10\ \Omega$ aufgeführt (Tabelle A.3).

	maximal definierte Abweichung im Standard		Normpuls	zulässiges Testergebnis		Unterschied zw. min und max Testergebnis
	min	max		min	max	
Pulsamplitude $U_s = 100\text{ V}$	- 20 %	+ 20 %	- 50 V	- 40 V	- 60 V	50 %
Pulsstrom I_s			- 5 A	- 4 A	- 6 A	50 %
Pulsdauer t_d	- 20 %	+ 20 %	1,5 ms	1,2 ms	1,8 ms	50%
Pulsleistung P_s			250 W	160W	360 W	125 %
Pulsenergie E_s			82 mJ	42 mJ	141 mJ	238 %

Tabelle A.3 Toleranzbetrachtung anhand von Testpuls 1 mit $U_s = - 100\text{ V}$ und $R_L = 10\ \Omega$ nach Normvorgaben nach [ISO 7637-2]

Die Auslegung von Schutzmaßnahmen wie Überspannungsableitern sollte auf die normativ maximal festgelegten Werte der Prüfpulse oder zumindest auf die nominellen Werte ausgelegt sein. Eine Verifikation kann dann aber nur entsprechend der mit den Prüfequipment realisierbaren Störgrößen erfolgen. Für die Transienten wird daher eine Messunsicherheitsbetrachtung anhand der Werte nach Kalibrierung des Prüfgenerators vorgenommen. Für eine Absicherung anhand der normativen Maximalwerte müssen, sofern möglich, die Parameter des Generators beim Einmessen der Pulse nach Norm entsprechend erhöht werden.

Nachfolgend eine Tabelle mit den Werten für den Pulsgenerator des FTZ (Tabelle A.4). Es ergeben sich deutlich geringere Abweichungen als für die normativ erlaubten Abweichungen bedingt durch die Messunsicherheiten beim Kalibrieren. Die Werte des genutzten Generators liegen für den hier aufgeführten Puls 1 über dem Normwert, aber unterhalb der maximal zulässigen Abweichung des Normwertes für Pulsdauer und Amplitude von +20%.

	Abweichung nach Kalibrierbericht		Kalibrierwert	Testergebnis mit Toleranzen durch Messunsicherheit		Unterschied zw. min und max Testergebnis
	min	max		min	max	
Pulsamplitude $U_s = 100\text{ V}$	+ 2,8 %	+ 14%	- 50 V	- 51,4 V	- 57,0 V	11 %
Pulsstrom I_s			5 A	- 5,1 A	5,7 A	11 %
Pulsdauer t_d	+ 9,4%	+ 18,4 %	1,5 ms	1,642 ms	1,776 ms	8 %
Pulsleistung P_s			250 W	262 W	325 W	24 %
Pulsenergie E_s			82 mJ	96 mJ	125 mJ	33 %

Tabelle A.4 Toleranzbetrachtung anhand von Testpuls 1 mit $U_s = - 100\text{ V}$ und $R_L = 10\ \Omega$ für den Pulsgenerator des FTZ anhand des Kalibrierberichtes

Die nachfolgenden Tabellen A.5 und A.6 sind auf Basis von [26] entstanden. In der Norm werden Messunsicherheiten von schnellen Transienten betrachtet. Für die 3-dB-Grenze und die Sprungantwort des Messsystems wurden typischen Werte angenommen, für die „eine ausgedehnte Klasse an (Mess-)Systemen repräsentativ“ sind. Die Unsicherheiten des Oszilloskops beruhen auf einer zu Grunde gelegten Abtastfrequenz von 5 Giga-sample pro Sekunde.

Für die zeitlichen Unsicherheitsbilanzen ist eine Korrektur der Parameter Anstiegszeit und Pulsdauer bei den Messungen oft nicht möglich, da man bei den Generatoren diese Parameter

nicht immer anpassen kann, sondern je nach Modell nur die Pulsamplitude. Für die energetische Bilanz sind diese Informationen, wie gezeigt, notwendig

Einflussgröße	Symbol	Unsicherheit	Verteilung	Divisor d	c_i	$u(x_i)$	$u_i(y)$	Quelle
Ablesewert bei 10% Anstiegszeit	$T_{10\%}$	0,10 ns	Dreieck	2,45	1	0,041	0,041	IEC 61000-4-4
Ablesewert bei 90% Anstiegszeit	$T_{90\%}$	0,10 ns	Dreieck	2,45	1	0,041	0,041	IEC 61000-4-4
Wiederholbarkeit der Prüfung	δR	0,15 ns	Normal	1	1	0,150	0,150	IEC 61000-4-4
Sprungantwort des Messsystems	A	40 ns MHz	Rechteck	1,73	$-44 \cdot 10^{-5}$ 1/MHz	23,09	0,010	IEC 61000-4-4
-3-dB-Bandbreite des Messsystems	B	30 MHz	Rechteck	1,73	$39 \cdot 10^{-5}$ ns/MHz	17,32	0,007	IEC 61000-4-4
Zulässige Abweichung Anstiegszeit	t_r	-0,5 μ s	Rechteck	1,73	1	290 ns	290 ns	ISO 7637-2
Kombinierte Standardunsicherheit							290,16 ns	

Tabelle A.5 Ermittlung der Messunsicherheit für die Anstiegszeit für einen beispielhaften Aufbau nach ISO 7637-2 nach [26]

Einflussgröße	Symbol	Unsicherheit	Verteilung	Divisor d	c_i	$u(x_i)$	$u_i(y)$	Quelle
Ablesewert bei 50% steigende Flanke	$T_{50\%F}$	0,10 ns	Dreieck	2,45	1	0,041	0,041 ns	IEC 61000-4-4
Ablesewert bei 50% fallende Flanke	$T_{50\%R}$	0,10 ns	Dreieck	2,45	1	0,041	0,041 ns	IEC 61000-4-4
Wiederholbarkeit der Prüfung	δR	1,5 ns	Normal	1	1	1,5	1,5 ns	IEC 61000-4-4
Sprungantwort des Messsystems	β	0,8 MHz	Rechteck	1,73	$-44 \cdot 10^{-4}$ ns/MHz	0,462	0,002 ns	IEC 61000-4-4
-3-dB-Bandbreite des Messsystems	B	30 MHz	Rechteck	1,73	$8 \cdot 10^{-5}$ ns/MHz	17,32	0,001 ns	IEC 61000-4-4
Zulässige Abweichung Anstiegszeit	t_d	20 ms	Rechteck	1,73	1	11,55	11,55 ms	ISO 7637-2
Kombinierte Standardunsicherheit							11,55 ms	

Tabelle A.6 Ermittlung der Messunsicherheit für die Impulsdauer für einen beispielhaften Aufbau nach ISO 7637-2 nach [26]

Die Tabellen A.5 und A.6 zeigen, dass die normativ zulässigen Abweichungen wesentlich größer sind als die Unsicherheit des Prüfaufbaus. Die Tabelle A.7 enthält die Unsicherheitsbetrachtung aus [26] erweitert um die normativ festgelegte Abweichung der Spannungswerte.

Einflussgröße	Symbol	Unsicherheit	Verteilung	Divisor d	c_i	$u(x_i)$	$u_i(y)$	Quelle
Beitrag vertikaler Messbereich Scope	V_{pr}	0,02	Dreieck	2,45	10	0,008	0,08 V	IEC 61000-4-4
Gleichstromdämpfung des Tastkopfes	A	0,5	Rechteck	1,73	1	0,29	0,08 V	IEC 61000-4-4
Wiederholbarkeit der Prüfung	δR	0,03	Normal	1	100	0,3	0,09 V	IEC 61000-4-4
Gleichstromdämpfung Messsystem	δV	0,02	Rechteck	1,73	100	0,01	1,15 V	IEC 61000-4-4
Zulässige Abweichung Spannungswert U_s (+/-20%)	V_{us}	0,2	Rechteck	1,73	100	0,115	11,50 V	ISO 7637-2
Sprungantwort des Messsystems	β	0,8 MHz	Rechteck	1,73	0,462 V/MHz	0,328	0,152 V	IEC 61000-4-4
-3-dB-Bandbreite des Messsystems	B	30 MHz	Rechteck	1,73	0,006 V/MHz	17,32	0,01 V	IEC 61000-4-4
Kombinierte Standardunsicherheit							13,1 V ^{*1)}	

ASIL	Erhöhungsfaktor Testlevel	Resultierender Wert mit ermittelter kombinierter Standardunsicherheit
B	1,28	17 %
C	1,88	25 %
D	2,32	30 %

^{*1)} Der ermittelte Wert gilt für eine Amplitude von absolut 100 V gemessen mit einem 10:1 Tastkopf und entspricht einer Unsicherheit von 13%.

Tabelle A.7 Ermittlung der Messunsicherheit und der Erhöhungsfaktoren für die Pulsamplitude für einen beispielhaften Aufbau nach ISO 7637-2

Einflussgröße	Symbol	Unsicherheit	Verteilung	Divisor d	c_i	$u(x_i)$	$u_i(y)$	Quelle
Beitrag vertikaler Messbereich Scope	V_{pr}	0,02	Dreieck	2,45	10	0,008	0,08 V	IEC 61000-4-4
Gleichstromdämpfung des Tastkopfes	A	0,5	Rechteck	1,73	1	0,29	0,08 V	IEC 61000-4-4
Wiederholbarkeit der Prüfung	δR	0,03	Normal	1	100	0,3	0,09 V	IEC 61000-4-4
Gleichstromdämpfung Messsystem	δV	0,02	Rechteck	1,73	100	0,01	1,15 V	IEC 61000-4-4
Zulässige Abweichung Spannungswert U_s (+2,8/+14%)	V_{US}	0,028	Rechteck	1,73	100	0,015	1,50 V	Kalibrierzertifikat
Sprungantwort des Messsystems	β	0,8 MHz	Rechteck	1,73	0,462 V/MHz	0,328	0,152 V	IEC 61000-4-4
-3-dB-Bandbreite des Messsystems	B	30 MHz	Rechteck	1,73	0,006 V/MHz	17,32	0,01 V	IEC 61000-4-4
Kombinierte Standardunsicherheit							3,1 V ^{*1)}	

ASIL	Erhöhungsfaktor Testlevel	Resultierender Wert mit ermittelter kombinierter Standardunsicherheit
B	1,28	4 %
C	1,88	6 %
D	2,32	7 %

*1) Der ermittelte Wert gilt für eine Amplitude von absolut 100 V gemessen mit einem 10:1 Tastkopf und entspricht einer Unsicherheit von 13%.

Tabelle A.8 Ermittlung der Messunsicherheit und der nominalen Erhöhungsfaktoren für die Pulsamplitude für den Aufbau nach ISO 7637-2 für die kalibrierte Prüftechnik am FTZ

Da die Prüfgeneratoren im Allgemeinen genauer spezifiziert sind als die Normvorgaben, ergeben sich deutlich geringere Unsicherheitsbilanzen. Der im FTZ eingesetzte Prüfgenerator liegt mit seinem im Kalibrierprotokoll nachgewiesenen Parametern im normativen Bereich für die Amplituden.

Die zeitliche Abweichung liegt für den Prüfgenerator immer im Bereich über dem Nominalwert. Durch die Unsicherheitsbetrachtung der horizontalen Auslenkung des Scopes ergeben sich Toleranzen im Bereich von ns und sind damit klein gegenüber der Abweichung der kalibrierten Werte zum Nominalwert.

Formal müssten die einzelnen Beiträge zur Messunsicherheit für Amplitude U_s und Pulsdauer t_d einzeln aufgeführt werden. Die Pulsdauer t_d kann für den verwendeten Generator nicht eingestellt werden, daher wird hier auf eine Betrachtung der horizontalen Unsicherheiten verzichtet.

Da alle Prüfparameter für den FTZ-Generator über dem nominal geforderten Werten liegen, muss der Prüfpegel nicht mit den Tabelle A.4 Werten erhöht werden. Wie aus Tabelle A.4 zu erkennen ist, liegt die minimale Überschreitung gegenüber den Normwerten bei 2,8 % für die Pulsamplitude. Die berechnete kombinierte Standardunsicherheit resultiert in einer prozentualen Spannungsabweichung von 3,1 %. Damit ergibt sich eine verbleibende mögliche Unterschreitung von 3,1 % - 2,8 % = 0,3 %. Es verbleibt dabei nur ein geringes berechnetes Unsicherheitsbudget für die Multiplikation mit den Erhöhungsfaktoren.

ISO 10605 – Test methods for electrical disturbances from electrostatic discharge

Der Ansatz für die Darstellung des Unsicherheitsbudgets für ESD-Tests bezieht sich auf Anmerkung 1 von Abschnitt 7.6.3 der ISO/IEC 17025:2018, die besagt: "In den Fällen, in denen eine anerkannte Testmethode Grenzwerte für die Werte der Hauptquellen der Messunsicherheit festlegt und die Form der Präsentation der berechneten Ergebnisse festlegt, erfüllt das Labor diese Klausel, indem es die Testmethode und die Berichtsanweisungen befolgt". Daher gelten die Anforderungen an die Messunsicherheit bei ESD-Tests als erfüllt, wenn das Labor nachweisen kann, dass der ESD-Generator die Anforderungen der relevanten Norm erfüllt und die Testdurchführung entsprechend den relevanten Normen nachgewiesen werden (IEC 17025:2018).

Um dennoch eine Unsicherheitsbilanz aufzustellen, verweist die ISO 10605 auf die entsprechenden Abschnitte der IEC 61000-4-2 [27]. Diese umfassen die Messunsicherheiten beim Kalibriervorgang von ESD-Prüftechnik mit den folgenden Einschränkungen:

- Die Unsicherheitsbilanz bezieht sich auf den Beitrag, der von der Messausrüstung kommt. Zusätzliche Unsicherheitsbeträge sollten je nach Labor mitbetrachtet werden, um ein genaueres Ergebnis zu erhalten.
- Es wird angenommen, dass alle Beiträge zur Unsicherheit nicht miteinander korreliert sind.

Die nachfolgenden Betrachtungen beziehen sich auf die Unsicherheiten des Kalibriervorgangs der ESD-Generatoren und die Messung des Prüfpulses im Labor. Die Ermittlung dieser Werte geschieht gemäß IEC 61000-4-2. Die IEC-Norm enthält Angaben zu Ermittlung von Messunsicherheiten bei ESD-Prüfungen. Die Angaben beziehen sich nur auf die Kontaktentladung.

ESD-Prüfungen führen zu einfachen Bewertungsaussagen wie „Prüfung bestanden“ oder „Prüfung nicht bestanden“. Es können keine numerischen Bewertungen abgeleitet werden. Das Systemverhalten des Prüflings ist im Allgemeinen nicht bekannt. Daher kann bei ESD auch keine Gesamtunsicherheitsbilanz abgeleitet werden. Es kann nur festgestellt werden, wie hoch der Grad der Übereinstimmung des Kalibriervorgangs mit der Normvorgabe ist. Das erfolgt für alle als relevant angesehenen Beiträge. Unter den hier betrachteten Bilanzen für

- die Anstiegszeit des ESD-Entladestroms,
- den Spitzenwert des ESD-Entladestroms,
- die Unsicherheiten der I_{30} und I_{60} -Werte des ESD-Entladestroms

sind diese in den Tabellen aufgeführt.

Damit sollte diese Betrachtung nur mit den für die jeweilige verwendete Prüftechnik verwendeten Kalibrierprotokollen durchgeführt werden. Die Angaben in den Tabellen, die als Beispiele zu verstehen sind, sind entsprechend zu ergänzen.

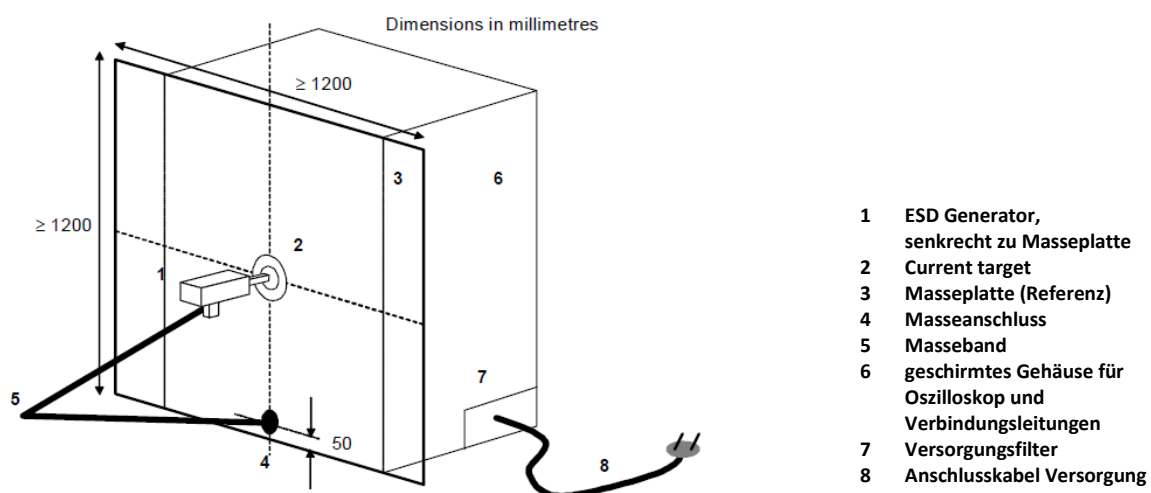


Abbildung A.4 Störfestigkeit, ESD – Kalibrieraufbau

Anstiegszeit des ESD-Entladestroms

Einflussgröße	Symbol	Wert in ps	Verteilung	Divisor d	$u(x_i)$ [ps]	c_i	$u(x_i)^2$ [ps ²]	Quelle	Bemerkung
Anzeige des Spitzenwerts	S_P	50	Normal	2	25,0	1	625,0	IEC 61000-4-2	6,3% der Gemessenen Anstiegszeit: $6,3\% \cdot 800\text{ps} = 50\text{ ps}$
Zeit bei 90% des Spitzenstroms	$T_{90\%}$	25	Rechteck	1,73	14	1	196	IEC 61000-4-2	Samplingrate Oszilloskop: 20 GS/s
Zeit bei 10% des Spitzenstroms	$T_{10\%}$	25	Rechteck	1,73	14	1	196	IEC 61000-4-2	Sampling-rate Oszilloskop: 20 GS/s
Beitrag horizontaler Messbereich Scope	B_h	36	Normal	2	18	1	324	IEC 61000-4-2	
Kette Kalibrierlast, Dämpfungsglied und Kabel	K_{DK}	30	Normal	2	15	1	225	IEC 61000-4-2	
Wiederholbarkeit der Prüfung	W_P	45	Normal	1	45	1	2025	IEC 61000-4-2	

Kombinierte Standardunsicherheit	Normal $k=1$	$u_c(x)$	60 ps
---	--------------	----------	--------------

Tabelle A.9 Ermittlung der Messunsicherheit für die Anstiegszeit des ESD-Entladestroms

Spitzenwert des ESD-Entladestroms

Einflussgröße	Symbol	Wert in %	Verteilung	Divisor d	$u(x_i)$	c_i	$u(x_i)^2$	Quelle
Beitrag vertikaler Messbereich Scope	S_P	3,2	Normal	2	1,6	1	2,56	IEC 61000-4-2
Kette Kalibrierlast, Dämpfungsglied und Kabel	K_{DK}	3,6	Normal	2	1,8	1	3,24	IEC 61000-4-2
Fehlanpassung Messkette - Scope	F_{MS}	2,0	U-Verteilung	1,414	1,4	1	2,00	IEC 61000-4-2
Wiederholbarkeit der Prüfung	W_P	1,5	Normal	1	1,5	1	2,25	IEC 61000-4-2

Kombinierte Standardunsicherheit	Normal $k=1$	$u_c(x)$	3,17 %
---	--------------	----------	---------------

Tabelle A.10 Ermittlung der Messunsicherheit für den Spitzenwert des ESD-Entladestroms

Unsicherheiten der I_{30} und I_{60} - Werte des ESD-Entladestroms

Einflussgröße	Symbol	Wert in %	Verteilung	Divisor d	$u(x_i)$	c_i	$u(x_i)^2$	Quelle
Unsicherheit entsprechend Wert aus Abschn. 6.2	U_{Sp}	6,3	Normal	2	3,2	1	9,92	IEC 61000-4-2
Auslesung der Zeit bei 30 ns oder 60 ns	K_{DK}	0,17	Normal	1,73	0,1	1	0,01	IEC 61000-4-2

Kombinierte Standardunsicherheit	Normal k=1	$u_c(x)$	3,15 %
---	------------	----------	---------------

Tabelle A.11 Ermittlung der Messunsicherheit

12. Quellen

- [1] ISO 26262:2018 Normenreihe Teil 1 – 12, Road vehicles – Functional safety
- [2] Hippeli, J.; Gierstorfer, A.; Jewoh, S.; Abid, M. A.; Obermeier, F.; Pasquet, T.: EMV & FuSi – Strategien zur Absicherung automatisierter Fahrzeuge; Tagungsband 8. GMM-Fachtagung - Elektromagnetische Verträglichkeit in der Kfz-Technik, VDE-Verlag, 2022
- [3] EC 61000-1-2:2016, Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena
- [4] Mardiguian, M., Combined Effects of Several, Simultaneous EMI Couplings', 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25 2000, ISBN 0-7803-5680-2, pp. 181-184
- [5] Parker, W. H., Tustin, W., Masone, T.: The Case for Combining EMC and Environmental Testing, ITEM 2002, www.rbitem.com, pp 54-60.
- [6] ECE R10 Ed.6; Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations; 2017
- [7] ISO 11451-1:2014, Road vehicles — Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 1: General principles and terminology
- [8] ISO 11452-2: Road vehicles — Component test methods for electrical disturbances by narrowband radiated electromagnetic energy — Part 2: Absorber-lined shielded enclosure (ALSE)
- [9] ISO 11452-4: Road vehicles — Component test methods for electrical disturbances by narrowband radiated electromagnetic energy — Part 4: Bulk current injection (BCI)
- [10] ISO 7637-1: Road vehicles — Electrical disturbances from conduction and coupling — Part 1: Vocabulary and general considerations
- [11] ISO 7637-2: Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines only
- [12] ISO 7637-3: Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines
- [13] ISO 10605:2008; Road vehicles — Test methods for electrical disturbances from electrostatic discharge
- [14] Armstrong, K., Introduction to EMC for Functional Safety, EMC-UK Conference, 2004
- [15] Deutschmann, B., Klotz, F., Wahl, A.: Abhängigkeit der Pulsfestigkeitsergebnisse von Kfz-Komponenten von den verwendeten Testpulsgeneratoren; EMV 2014, VDE-Verlag Berlin, 2014
- [16] <https://www.analog.com/en/solutions/gigabit-multimedia-serial-link.html>, o.J., aufgerufen am 30.5.2024
- [17] <https://www.ti.com/de-de/interface/high-speed-serdes/fpd-link-serdes/overview.html>, o.J., aufgerufen am 30.5.2024

- [18] Analog Devices, GMSL2 General User Guide, 2023
- [19] Ostrem, G.: GMSL: Gigabit Multimedia Serial Link – An Introduction, Handbook of Visual Display Technology, Springer living reference work, 2020
- [20] Sakamoto; C; Phyo, W.: Using 2.5Gbps SerDes with Built-In Bit-Error Rate Test Circuitry Makes Measuring Link Quality Easy; APPLICATION NOTE 5053; Analog Devices; 2011
- [21] Maxim Integrated, how to use gmsl line fault detection for power over coax, Application Note, 2014
- [22] The United Kingdom Accreditation Service (UKAS) LAB34:2002-08: The Expression of Uncertainty in EMC testing
- [23] Leitfaden zur Angabe der Unsicherheit beim Messen, Originaltitel: Guide to the expression of uncertainty in measurement (GUM), DIN, Deutsches Institut für Normung e.V, Berlin; Wien; Zürich: Beuth, 1995
- [24] DIN EN 55016-4-2: 2019-09: Anforderungen an Geräte und Einrichtungen sowie Festlegung der Verfahren zur Messung der hochfrequenten Störaussendung (Funkstörungen) und Störfestigkeit - Teil 4-2: Unsicherheiten, Statistik und Modelle zur Ableitung von Grenzwerten (Störmodell) - Messgeräte-Unsicherheit
- [25] DIN EN 61000-4-6: 2014-08: Elektromagnetische Verträglichkeit (EMV), Teil 4-6: Prüf- und Messverfahren – Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder
- [26] DIN EN 61000-4-4:2013-04: Elektromagnetische Verträglichkeit (EMV), Teil 4-4: Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen
- [27] IEC 61000-4-2:2008: Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test

Bisher in der FAT-Schriftenreihe erschienen (ab 2021)

Nr.	Titel
340	Schnelle, breitbandige Datenübertragung zwischen Truck und Trailer als Voraussetzung für das hochautomatisierte Fahren von Lastzügen, 2021
341	Wasserstoffkompatibilität von Aluminium-Legierungen für Brennstoffzellenfahrzeuge, 2021
342	Anforderungen an eine elektrische Lade- und Wasserstoffinfrastruktur für gewerbliche Nutzfahrzeuge mit dem Zeithorizont 2030, 2021
343	Objective assessment of database quality for use in the automotive research and development process, 2021
344	Review of non-exhaust particle emissions from road vehicles, 2021
345	Ganzheitliche Betrachtung von Rollwiderstandsverlusten an einem schweren Sattelzug unter realen Umgebungsbedingungen, 2021
346	Studie zur Abschätzung der Anwendungspotentiale, Risiken und notwendigen Forschungsbedarfe bei der Verwendung von Glashohlkugeln in Kombination mit thermoplastischem Schaumspritzguss, 2021
347	Typgenehmigungsanforderungen an Level-3-Autobahnssysteme - Hintergrundbetrachtungen zu technischen Anforderungen für eine automatisierte Fahrfunktion, 2021
348	Einfluss der Kantenbearbeitung von Aluminiumblechen auf das Restumformvermögen sowie die Festigkeitseigenschaften unter quasistatischer und schwingender Beanspruchung, 2021
349	Verstärkung dünner formgehärteter Bauteile mittels FVK-Verrippungen, 2021
350	HMI Anforderungen für den automatisierten Individualverkehr unter Berücksichtigung von Leistungsmöglichkeiten und -grenzen älterer Nutzer, 2021
351	Compatibility of polymers for fuel cell automobiles, 2021
352	Entwicklung einer gewichtsoptimierten Batteriegehäusestruktur für Volumenfahrzeuge, 2021
353	Charakterisierung und Modellierung des Deformations- und Versagensverhaltens von nicht-faserverstärkten Thermoplasten unter mehrachsiger Crashbelastung, 2021
354	Untersuchung zum thermischen Komfort im Pkw für den Grenzbereich des Luftzugempfindens, 2021
355	Anforderungen an die Güte, Verfügbarkeit und Vorausschau einer Reibwertschätzung aus Funktionssicht, 2021
356	Entwicklung einer standardisierten Prüfanordnung zur Bewertung der Übernahmeleistung beim automatisierten Fahren, 2022
357	Vorstudie zu Verkehrsemissionen - Räumlich und zeitlich aufgelöste Daten durch Schwarmmessungen, 2022
358	Produktivitätssteigerung und Kostensenkung der laser-additiven Fertigung für den Automobilbau, 2022
359	Analyse der Einflussfaktoren auf die Abweichung zwischen CFD und Fahrversuch bei der Bestimmung des Luftwiderstands von Nutzfahrzeugen mit Fokus auf den Ventilationswiderstand von Nfz-Rädern, 2022
360	Werkstoffmodelle und Kennwertermittlung für die industrielle Anwendung der Umform- und Crash-Simulation unter Berücksichtigung der thermischen Behandlungen beim Lackieren im Prozess bei hochfesten Werkstoffen, 2022

- 361 Compatibility of polymers for fuel cell automobiles, 2022
- 362 Ermüdung kurzfaserverstärkter thermoplastischer Polymerwerkstoffe, 2022
- 363 Market research and definition of procedure to comparison of comfort measuring systems for a vehicle cabin, 2022
- 364 Methodische Ansätze zur Auswahl von Bordnetzstrukturen mit erhöhten Zuverlässigkeitsanforderungen, 2022
- 365 Fahrwiderstand von Lenk- und Liftachsen in Kurven und auf gerader Strecke unter realen Umgebungsbedingungen, 2022
- 366 Klimadaten und Nutzungsverhalten zu Auslegung, Versuch und Simulation an Kraftfahrzeug-Kälte-/Heizanlagen, 2022
- 367 Experimentelle und numerische Untersuchung des selbsttätigen Losdrehens von Schraubenverbindungen mit konstanten und variablen Amplituden und Entwicklung einer Bewertungsmethode, 2022
- 368 Objective assessment of database quality for use in the automotive research and development process – Part 2, 2023
- 369 Level 2 hands-off – Recommendations and guidance, 2023
- 370 Funktionale Sicherheitsbewertung und Cybersecurity Analysen relevanter Use Cases für die Datenübertragung zwischen Truck und Trailer als Voraussetzung für das hochautomatisierte Fahren von Lastzügen, 2023
- 371 Study on the technical evaluation of decentralization based de-identification procedures for personal data in the automotive sector, 2023
- 372 Legal evaluation of decentralization based de-identification procedures for personal and non-personal data in the automotive sector, 2023
- 373 Quantifizierung der mechanischen Belastbarkeit von Infrarot-Schweißverbindungen in zyklisch belasteten Thermoplast-Bauteilen, 2023
- 374 Lebensdauerbewertung von geschweißten Verbindungselementen unter Montagevorspannung, 2023
- 375 Einfluss verschiedener Scherschneidparameter auf die elektro-magnetischen Eigenschaften von NO-Elektroblech automobiler Traktionsantriebe, 2023
- 376 Automatisierte Demontage von Traktionsmotoren der E-Mobilität - Eine Studie zur Optimierung der Demontage, 2023
- 377 Untersuchungen zum Einfluss von feuchtem Wasserstoff auf die Spannungsrisskorrosionsempfindlichkeit von Aluminium-Legierungen für den Einsatz in Brennstoffzellenfahrzeugen, 2024
- 378 Diagnosekonzepte für zonale und teilredundante Bordnetzarchitekturen, 2024
- 379 Dynamische Erfassung und Beurteilung von Situationsbewusstsein im Kontext des automatisierten Fahrens, 2024
- 380 Charakterisierung zukunfts-trächtiger Zellmaterialien im Hinblick auf deren Anforderungen an das Batteriepack, 2024
- 381 Fahrdynamik des Automatisierten Fahrens, 2024
- 382 Forschungsperspektiven für Mobilität in klimaneutralen Städten 2045 - Explorative Szenarioanalyse und innovationspolitische Handlungsempfehlungen, 2024
- 383 Codierung und Analyse der AO-Klassifikation für Fuß- und Sprunggelenksverletzungen zur Evaluation potentieller Langzeitfolgen, 2024
- 384 EMV-Nachweis der Störfestigkeit auf Komponenten- und Systemebene für FailOp ab Level 3 im Hinblick auf die Funktionssicherheit - Erster Projektteil, 2024

- 385 Retrospektive Berechnung des Crashpulses aus Fahrzeugdeformationen basierend auf EES-Berechnung von Fahrzeug-Voxelmodellen unter Berücksichtigung des zeitlichen Verlaufes, 2024
- 386 Energieverluste infolge von Rad-/Achsfeststellungen am schweren Sattelzug bei realen Umgebungsbedingungen, 2025
- 387 Recycling von Permanentmagneten und Bewertung der Rezyklierbarkeit von Permanentmagnet-Synchronmotoren, 2025
- 388 Graphen- und heuristikbasierte Topologieoptimierung von 3D-Crash-Strukturen von Personenkraftwagen, 2025
- 389 Bewertung und Erhöhung des Potentials von Binder Jetting durch Nutzung kosteneffizienter Stahlpulver für den Einsatz in der Automobilindustrie, 2025
- 390 Driver performance models as reference for the quality of automated driving functions, 2025
- 391 Experimentelle und numerische Analyse des Fließverhaltens von hochviskosen Wärmeleitstoffen im Fertigungsprozess, 2025
- 392 Maßnahmen zum Aufbau und Erhalt von Situationsbewusstsein im Kontext des automatisierten Fahrens, 2025
- 393 Reduktion von Kupfer und Eisen in geschmolzenem Aluminium – modernes Aluminium aus alten Fahrzeugen, 2025
- 394 PCM-F³: PCM Fit For Future, 2025
- 395 Blech-Umformeinfluss mittels Machine Learning für Konzept-Crashsimulationen (UmMatCra-ML), 2025
- 396 Absicherung moderner Fahrzeug-Bordnetze mittels elektronischer Sicherungen (eFuses), 2025
- 397 Fahrdynamik des automatisierten Fahrens 2.0, 2025
- 398 Machbarkeitsstudie zur Koppelung von Methoden des maschinellen Lernens und CFD zur Vorhersage von Be- und Enttaugung an Fahrzeugscheiben, 2025
- 399 Charakterisierung der Radumströmung bei realer Reifendeformation, 2026
- 400 Reduzierung von Kaltaufschweißungen durch gezielte Anpassung des Seebeck-Koeffizienten von Werkzeugwerkstoffen mittels Laserauftragschweißen, 2026
- 401 Variable Digitalisierung von Materialkarten für FVK und ihre Rezyklate, 2026
- 402 EMV-Nachweis der Störfestigkeit auf Komponenten- und Systemebene für FailOp ab Level 3 im Hinblick auf die Funktionssicherheit – Erster und zweiter Projektteil

Impressum

Herausgeber	FAT Forschungsvereinigung Automobiltechnik e.V. Behrenstraße 35 10117 Berlin Telefon +49 30 897842-0 Fax +49 30 897842-600 www.fat-ev.de
ISSN	2192-7863
Copyright	Forschungsvereinigung Automobiltechnik e.V. (FAT) 2026

Verband der Automobilindustrie e.V. (VDA)
Behrenstraße 35, 10117 Berlin
www.vda.de
Twitter @VDA_online

VDA | Verband der
Automobilindustrie

Forschungsvereinigung Automobiltechnik e.V. (FAT)
Behrenstraße 35, 10117 Berlin
www.vda.de/fat

FAT | Forschungsvereinigung
Automobiltechnik