Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Michael Gustav Jordan Gandolfo

Sicherheitsgerichtete Entwicklung und Sicherheitsnachweis eines bahntechnischen SIL3-Systems am Beispiel einer Sicherheitsfahrschaltung gemäß TSI und UIC641

Fakultät Technik und Informatik
Department Elektro- und Informationstechnik

Faculty of Engineering and Computer Science
Department of Information and Electrical Engineering

Michael Gustav Jordan Gandolfo

Sicherheitsgerichtete Entwicklung und Sicherheitsnachweis eines bahntechnischen SIL3-Systems am Beispiel einer Sicherheitsfahrschaltung gemäß TSI und UIC641

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Elektro- und Informationstechnik
am Department Informations- und Elektrotechnik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Björn Lange
Zweitgutachter: Dipl.-Ing. Eggert Jung

Eingereicht am: 14. Februar 2025

Michael Gustav Jordan Gandolfo

Thema der Arbeit

Sicherheitsgerichtete Entwicklung und Sicherheitsnachweis eines bahntechnischen SIL3-Systems am Beispiel einer Sicherheitsfahrschaltung gemäß TSI und UIC641

Stichworte

Bahntechnik, Normen, Sicherheitsnachweis, SIL3, Risikoanalyse, Normenkonformität, Sicherheitsfahrschaltung (Sifa), TSI

Kurzzusammenfassung

Diese Arbeit behandelt die Entwicklung und den Sicherheitsnachweis eines SIL3-zertifizierten bahntechnischen Systems, am Beispiel einer Sicherheitsfahrschaltung gemäß TSI und UIC641. Es wird durch systematische Entwicklungsprozesse und umfassende Sicherheitsanalysen gezeigt, wie das System die hohen Anforderungen der Sicherheitsintegritätsstufe 3 erfüllt.

Michael Gustav Jordan Gandolfo

Title of the paper

Safety-oriented development and safety verification of a railway SIL3 system using the example of a safety driving circuit in accordance with TSI and UIC641

Keywords

Railway technology, standards, proof of safety, SIL3, risk analysis, conformity to standards, safety drive circuit (Sifa), TSI

Abstract

This thesis deals with the development and safety verification of a SIL3-certified railway system, using the example of a safety drive circuit in accordance with TSI and UIC641. It shows how the system fulfils the high requirements of safety integrity level 3 through systematic development processes and comprehensive safety analyses.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Listings

1 Einleitung

Ein zentraler Bestandteil der modernen Bahntechnik ist die Entwicklung hochsicherer Systeme, wie beispielsweise einer Sicherheitsfahrschaltung (Sifa) unter Berücksichtigung geltender Normen und Standards. Die Sifa fungiert als autonomes Überwachungssystem, das bei Handlungsfähigkeit des Triebfahrzeugführers oder fehlerhafter Bedienung eine Zwangsbremsung initiiert. Diese Arbeit befasst sich mit der exemplarischen Entwicklung eines normgerechten Bahnsystems, das den Anforderungen der Sicherheitsintegritätsstufe (SIL) 3 entspricht, sowie mit der Erstellung eines Sicherheitsnachweises für ein solches System. Unter Berücksichtigung der Technischen Spezifikationen für Interoperabilität (TSI) [17] sowie relevanter Normen der Bahntechnik wird ein systematischer Ansatz vorgestellt, der das Ziel der Normkonformität und Zuverlässigkeit der Sifa verfolgt. Dabei kommen in der Bahntechnik etablierte Sicherheitsanalysemethoden zum Einsatz, um die Konzeption der Sicherheitsfahrschaltung präzise und detailliert darzustellen. Ziel dieser Arbeit ist es, einen fundierten Einblick in die Entwicklung und Validierung normgerechter sicherheitstechnischer Systeme im Bahnsektor zu bieten und die Umsetzung strenger Sicherheitsstandards hervorzuheben.

1.1 Motivation und Problemstellung

Die Entwicklung sicherheitstechnischer Systeme in der Bahntechnik ist eine komplexe und anspruchsvolle Aufgabe, die weit über die reine technische Realisierung hinausgeht. Marktfähige Produkte im Bereich der Bahntechnik müssen so konzipiert sein, dass sie den Ansprüchen europäischer Normen und Sicherheitsstandards gerecht werden. Die Motivation dieser Arbeit liegt in der theoretischen Entwicklung einer Sifa der Sicherheitsintegritätsstufe 3, die durch ihre an Normen orientierte Konzeption die Grundlage für eine erfolgreiche, unabhängige Zertifizierung durch den TÜV schafft. Ein zentraler Aspekt dieser Arbeit ist es einen Einblick in die Tätigkeiten der TÜV Nord Systems GmbH & Co. KG im Bereich der funktionalen Sicherheit in der Bahntechnik zu gewähren. Die zugrunde liegende Problemstellung besteht darin, die Entwicklung einer Sifa in ihrer ganzen Komplexität und ihrem Umfang darzustellen, damit diese dem SIL 3 entspricht. Die Entwicklung einer Sifa muss nicht nur technisch fehlerfrei sein,

sondern auch die europäischen Bahntechniknormen erfüllen. Dies erfordert eine systematische, normenkonforme Vorgehensweise, die in dieser Arbeit exemplarisch dargestellt wird.

1.2 Zielsetzung der Arbeit

Das Ziel dieser Bachelorarbeit besteht in der exemplarischen Entwicklung einer Sicherheitsfahrschaltung, die den Anforderungen einer SIL 3 entspricht. In diesem Kontext werden die einschlägigen Anforderungen der DIN EN 50129 [6] sowie der Technischen Spezifikationen für die Interoperabilität (TSI) [17] und UIC641 [18] berücksichtigt, wobei ein besonderes Augenmerk auf die Aspekte der Zuverlässigkeit, Verfügbarkeit, Wartbarkeit und Sicherheit (RAMS) [3] &[4] gelegt wird. Zur Bestätigung der Konformität des entwickelten Produkts mit der Sicherheitsintegritätsstufe 3 wird ein Sicherheitsnachweis gemäß den Anforderungen der DIN EN 50129 [6] erstellt.

1.3 Aufbau der Arbeit

Diese Arbeit ist in sieben Kapitel unterteilt. Im Anschluss an das einleitende Kapitel folgt das zweite Kapitel. Dort werden die grundlegenden Konzepte erläutert, die für die Umsetzung einer Sifa entscheidend sind. Das dritte Kapitel konzentriert sich auf die Anforderungsanalyse. Es bietet eine detaillierte Darstellung der Sicherheitsanforderungen für die Sifa und präsentiert relevante Abschnitte der Normen DIN EN 50129 [6] und der TSI [17] im Hinblick auf die geplante Sicherheitsfunktion und die Systemarchitekturspezifikation. Im vierten Kapitel werden, unterteilt in drei Unterkapiteln, folgende Punkte dargestellt: das Hardware-Design, das Software-Design und die Systemsimulation. Das fünfte Kapitel behandelt das Prototyping. Es umfasst den Aufbau des Prototyps, die Überprüfung seiner Funktionalität, Tests im Fehlerfall und die Verifizierung der Sicherheitsanforderungen. Das sechste Kapitel befasst sich mit dem Sicherheitsnachweis. Es beinhaltet die Definition des Systems, den Qualitätsmanagementbericht, den Sicherheitsmanagementbericht, den technischen Sicherheitsbericht, die Validierung der funktionalen Sicherheitsprüfung, die Validierung der Systemprüfung und die Erfüllung des SIL 3. Das siebte und letzte Kapitel fasst die Ergebnisse der Arbeit zusammen, beleuchtet die Herausforderungen und Lösungen und gibt einen Ausblick auf mögliche Verbesserungs- und Erweiterungspotenziale. Der Anhang zur Arbeit befindet sich auf CD und kann beim Erstgutachter eingesehen werden. Um die Lesbarkeit dieser Bachelorarbeit zu verbessern, wird das generische Maskulinum verwendet. Alle in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich, sofern nicht anders angegeben, auf Personen jeglichen Geschlechts.

2 Theoretische Grundlagen

2.1 Funktionale Sicherheit in der Bahntechnik

Die Funktionale Sicherheit ist ein wesentlicher Bestandteil der technischen Entwicklung von Systemen. Sie definiert die notwendigen Maßnahmen zur Gewährleistung sicherer Systeme, die auf Hard- und Softwarelösungen basieren [16]. Sie beschreibt die Fähigkeit von Systemen, definierte Sicherheitsfunktionen zuverlässig und gemäß den festgelegten Spezifikationen auszuführen. Die Gestaltungsprinzipien für solche Systeme sind in der sieben Teile umfassenden internationalen Basisnorm für Sicherheit, der IEC 61508 [27], verankert. Diese Norm wurde in das deutsche Normensystem als DIN EN 61508 [28] übernommen und basiert auf wissenschaftlich fundierten Modellannahmen [9]. Die funktionale Sicherheit in der technischen Entwicklung verfolgt das Ziel Risiken für Menschen und Objekte durch Fehlfunktionen sicherheitskritischer Systeme zu verhindern oder auf ein vertretbares Niveau zu minimieren [52]. Damit ist die funktionale Sicherheit ein wesentlicher Aspekt der Gesamtsicherheit eines Systems [2].

Im Weiteren wird die Vorgehensweise der IEC 61508 betrachtet. Zunächst wird zur Risikoreduktion ein präzises Verständnis für das Versagen von Maßnahmen erarbeitet. Es werden dabei zwei Ausfallmodelle berücksichtigt: Zum einen zufällige Ausfälle von Komponenten und zum anderen systematische Ausfälle, die auf spezifische Ursachen zurückzuführen sind. Letztere entstehen häufig aufgrund menschlicher Einschränkungen, wie etwa durch Fehler im Entwurfsprozess [9].

Dieser Abschnitt beschreibt die relevanten Normen sowie das Management von RAMS (Reliability, Availability, Maintainability, and Safety) für Bahnen und Bahnanlagen und stellt das V-Modell vor [3].

2.1.1 Relevante Normen

Die europäischen Normen für Bahntechnik bilden die Grundlage für die Sicherheit, Interoperabilität und Effizienz des Eisenbahnverkehrs in Europa. Diese Normen werden von der Europäischen Eisenbahnagentur (ERA) und verschiedenen Normungsgremien wie dem Europäischen Komitee für Normung (CEN) und dem Europäischen Komitee für elektrotechnische Normung (CENELEC) entwickelt. Dieser Abschnitt gibt einen Überblick über relevante Normen und Richtlinien, die im Rahmen dieser Bachelorarbeit verwendet werden.

In der folgenden Tabelle 2.1 werden die relevanten Normen dargestellt.

Tabelle 2.1: Relevante Normen

Abkürzung	**Norm**
/EN 50129/	Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, Sicherheitsrelevante elektronische Systeme für Signaltechnik [6]
/EN 50159/	DIN EN 50159; Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in Übertragungssystemen [7]
/EN 50126/	DIN EN 50126; Bahnanwendungen, Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) [3] & [4]
/EN 50128/	DIN EN 50128; Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, Software für Eisenbahnsteuerungs- und -Überwachungssysteme [5]
/EN 50125-1/	Bahnanwendungen – Umweltbedingungen für Betriebsmittel – Teil 1: Betriebsmittel auf Bahnfahrzeugen Deutsche Fassung EN 50125-1:2014 [70]
/TSI/	VERORDNUNG (EU) Nr. 1302/2014 DER KOMMISSION vom 18. November 2014 über eine technische Spezifikation für die Interoperabilität des Teilsystems „Fahrzeuge - Lokomotiven und Personenwagen“ des Eisenbahnsystems in der Europäischen Union [17]
/UIC 641/	UIC-Kodex 641 V; Bedingungen für Sicherheitsfahrschaltungen im internationalen Verkehr [18]

Ein Aspekt der europäischen Bahnnormen ist das Konzept der Interoperabilität, das darauf abzielt, grenzüberschreitende Bahnverbindungen zu erleichtern. Dies wird durch die Harmonisierung technischer Spezifikationen für die Interoperabilität (TSI – Technical Specifications for Interoperability) erreicht. Diese Spezifikationen decken verschiedene Aspekte des Bahnverkehrs ab, einschließlich Signalgebung, Schienenfahrzeuge und Telematik-Anwendungen für den Fracht- und Personenverkehr. Die europäischen Normen legen strenge Sicherheitsanforderungen fest, um das Risiko von Unfällen und Störungen im Bahnverkehr zu minimieren. Dazu

gehören Vorschriften für die Konstruktion und Wartung von Zügen und Schieneninfrastrukturen sowie für das Betriebsmanagement [17].

2.1.2 Management von RAMS für Bahnen und Bahnanlagen

Das Lebenszyklusmodell dient als Grundlage für das RAMS- Management und umfasst zudem Regeln zur Anpassungsfähigkeit. Der Lebenszyklusansatz bietet eine strukturierte Grundlage für die Planung, Steuerung, Überwachung und das Management sämtlicher Aspekte eines Systems, einschließlich RAMS, während das System alle Phasen seines Lebenszyklus' durchläuft. Die Norm DIN EN 50126-1 [3] stellt den Lebenszyklus in einer sequenziellen Form dar, wobei die einzelnen Phasen sowie deren Zusammenhänge aufgezeigt werden. Der gesamte RAMS-Prozess gliedert sich in drei Hauptkomponenten.

- Risikobewertung, basierend auf der Systemdefinition, einschließlich der Festlegung der RAMS-Anforderungen.
- Umsetzung und Nachweis, dass das System die definierten RAMS-Anforderungen erfüllt.
- Betrieb, Instandhaltung und Außerbetriebsetzung

Neben dem standardmäßigen Verlauf der Lebenszyklusphasen beinhaltet der allgemeine Prozess zusätzlich eine Feedback-Schleife sowie kontinuierliche Schleifen zur Steuerung von RAMS-Anforderungen. Die RAMS-Aufgaben leisten einen Beitrag zu den allgemeinen Projektaufgaben innerhalb der einzelnen Lebenszyklusphasen [3].

Die spezifischen Anforderungen an die RAMS-Aufgaben der DIN EN 50126-1 [4] sind in der folgenden Abbildung 2.1 dargestellt.

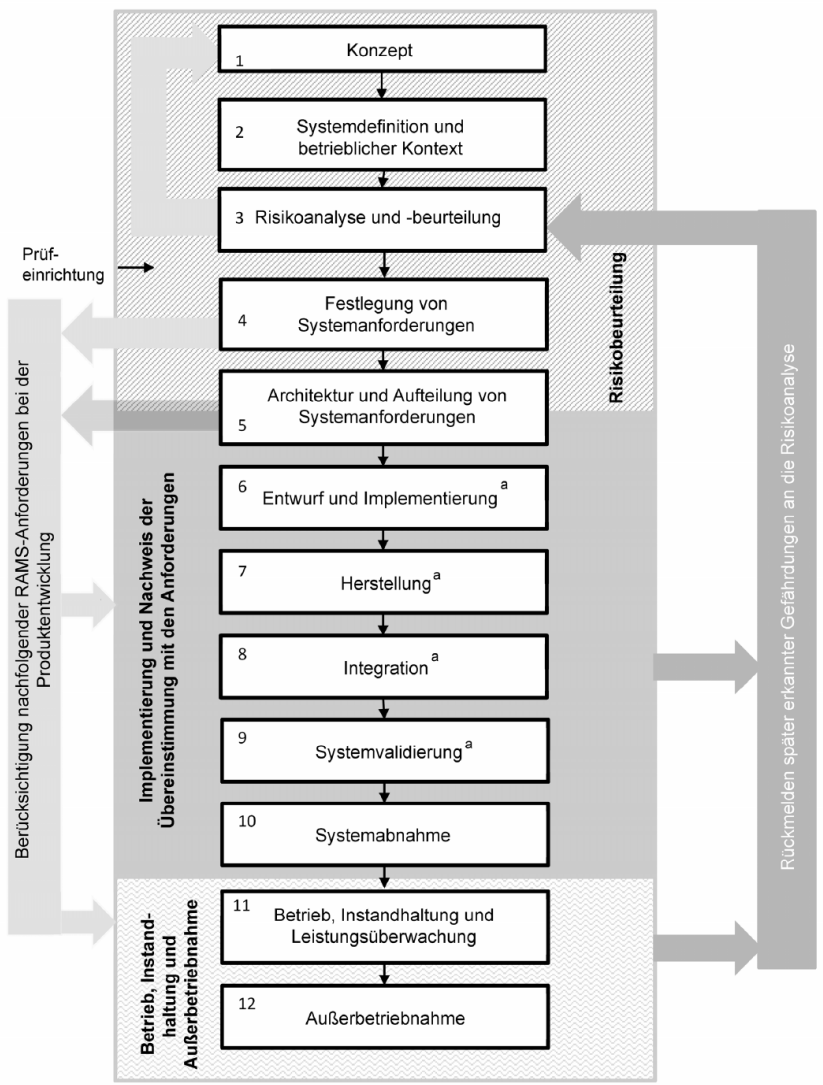


Abbildung 2.1: RAMS-Managementprozess und Lebenszyklus des Systems [3]

Der Kleinbuchstabe (a) innerhalb der Abbildung 2.1 kennzeichnet die Punkte des Lebenszyklus, die im Rahmen der Implementierung und des Nachweises der Übereinstimmung eines Systems mit den aufgezeigten Anforderungen, viele Subsysteme und Komponenten enthalten können [3].

2.1.3 Das V-Modell

Das V-Modell ist ein in Deutschland entwickeltes Softwareentwicklungsmodell, das eine systematische und strukturierte Herangehensweise an Softwareprojekte bietet. Ursprünglich wurde es in den 1980er Jahren als Teil der Qualitätssicherung in der Verteidigungsindustrie entwickelt und später für die Anwendung in anderen technischen Bereichen angepasst [1].

Das V-Modell ist charakterisiert durch seine V-förmige Struktur, die den Entwicklungsprozess in zwei Hauptphasen unterteilt: die Spezifikationsphase auf der linken Seite des V und die Testphase auf der rechten Seite. Jeder Schritt in der Spezifikationsphase hat eine korrespondierende Testphase, was eine kontinuierliche Qualitätssicherung und Verifizierung der Ergebnisse ermöglicht [10].

In der folgenden Abbildung 2.2 wird der V-Zyklus dargestellt.

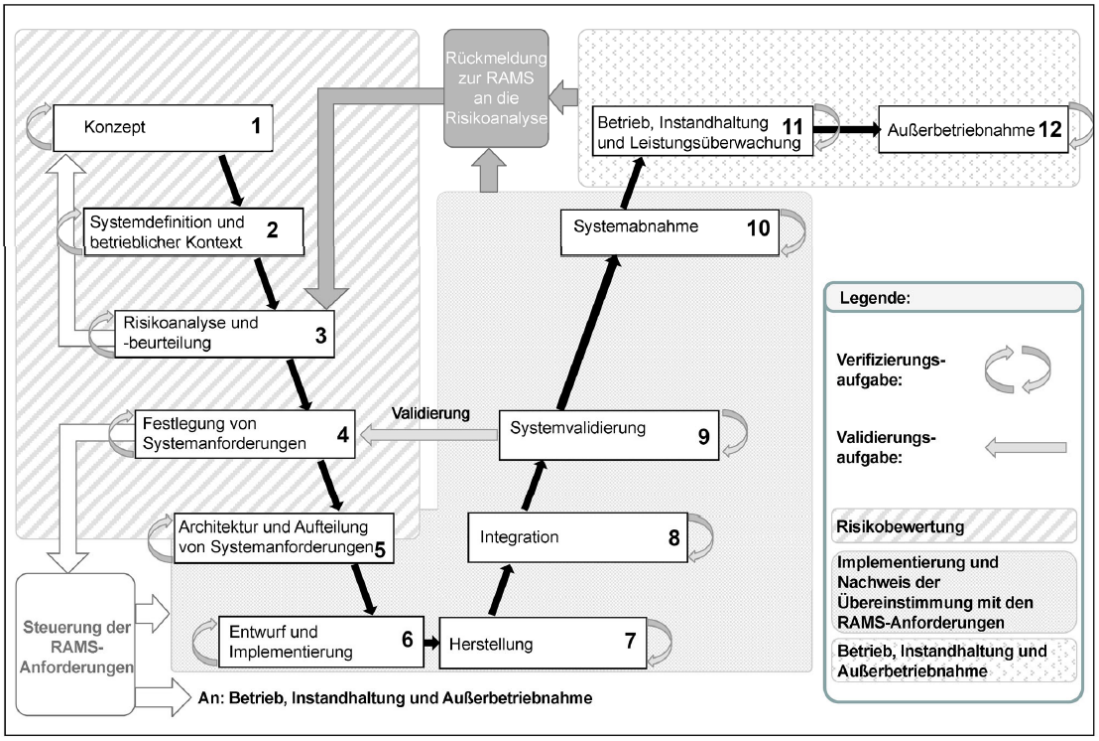


Abbildung 2.2: Der V-Zyklus [3]

Das V-Modell wird vor allem in Projekten eingesetzt, an die hohe Anforderungen an die Dokumentation und Systemqualität gestellt werden, wie die Entwicklung einer Sicherheitsfahrschaltung. Es wird häufig dort verwendet, wo Fehler in der Software gravierende Folgen haben können, wie in der Automobilindustrie und Medizintechnik. Die strukturierte Vorgehensweise

hilft dabei, Fehler frühzeitig zu erkennen und zu beheben, was sowohl die Sicherheit als auch die Zuverlässigkeit der entwickelten Systeme erhöht [15].

Das V-Modell ist der Entwicklungsstandard für IT-Systeme des Bundes und wird auch in der Industrie eingesetzt. Es basiert auf der hierarchischen Zerlegung von Systemen in immer kleinere Einheiten nach einem klar definierten Vorgehen. Dabei werden Anforderungen der höheren Ebene übernommen, eine Zerlegungsstrategie entwickelt und auf jeder Stufe neue Anforderungen definiert und weitergegeben. Um frühzeitig Fehler oder Fehlentscheidungen zu erkennen, wird jede Stufe verifiziert. Die Validierung des Systems wird im Schritt 9 durchgeführt, wie der Abbildung 2.2 zu entnehmen ist [2].

2.2 Sicherheitsfahrschaltung (Sifa)

2.2.1 Definition

Eine Sicherheitsfahrschaltung, oft auch als Sicherheitsfahrschalter oder Totmannschaltung bezeichnet, ist eine Sicherheitseinrichtung, die in verschiedenen Fahrzeugen, insbesondere in Zügen und Straßenbahnen, verwendet wird. Ihr Hauptzweck ist es, zu überprüfen, ob der Fahrzeugführer noch in der Lage ist, das Fahrzeug zu steuern. Sollte der Fahrer beispielsweise durch gesundheitliche Probleme handlungsunfähig werden, sorgt die Sicherheitsfahrschaltung dafür, dass das Fahrzeug automatisch gestoppt wird.

Die Funktionsweise der Sicherheitsfahrschaltung basiert darauf, dass der Fahrer in regelmäßigen Abständen eine Taste drücken oder einen Hebel betätigen muss. Geschieht dies nicht innerhalb eines vorgegebenen Zeitintervalls, werden Warnsignale ausgelöst. Reagiert der Fahrer auch darauf nicht, werden automatisch Bremsvorgänge eingeleitet, die das Fahrzeug sicher zum Stillstand bringen [8].

2.2.2 Historische Entwicklung

Die Geschichte der Sicherheitsfahrschaltung ist eng mit der Entwicklung der Sicherheitstechnologien im Eisenbahnwesen verbunden und hat wesentlich zur Erhöhung der Sicherheit im Schienenverkehr beigetragen. Die ersten Formen der Sicherheitsfahrschaltung entstanden im frühen 20. Jahrhundert. Ursprünglich wurden mechanische Vorrichtungen verwendet, die mit der Zeit durch elektrische und elektronische Komponenten ergänzt wurden. Die Reichsbahn-Zentral-Maschinenamt-Sifa, eine Sicherheitsfahrschaltung aus der Vorkriegszeit, blieb auch nach dem Zweiten Weltkrieg in Gebrauch. Diese Sicherheitsfahrschaltung muss während der

Fahrt kontinuierlich betätigt werden und erfordert kein periodisches Loslassen, was keinen sicheren Schutz im Falle einer Handlungsunfähigkeit des Triebfahrzeugführers bietet [8].

In den 1950er und 1960er Jahren begannen viele Eisenbahngesellschaften, elektronische Totmannschalter zu implementieren, die empfindlicher auf die Nichtaktivität des Fahrers reagierten und schneller eine Notbremsung einleiten konnten. Heute sind Sicherheitsfahrschaltungen weit fortgeschritten und oft Teil umfassenderer Sicherheitssysteme in Zügen.

Die Sifa 86 ist eine verbesserte Version der Sicherheitsfahrschaltung, die in der Deutschen Reichsbahn der DDR verwendet wurde. Diese Variante, bekannt als Aufforderungs-Sifa, erfordert, dass der Triebfahrzeugführer auf ein optisches Signal mit einem Tastendruck reagiert. Das System generiert dieses Signal in zufälligen Intervallen zwischen 40 und 50 Sekunden. Zusätzlich wird eine erneute Betätigung des Systems gefordert, wenn seit der letzten Aktivierung mehr als 400 Meter bei Fahrzeugen mit einer Höchstgeschwindigkeit unter 100 km/h bzw. 800 Meter bei Fahrzeugen mit einer Höchstgeschwindigkeit von 100 km/h oder mehr zurückgelegt wurden, unabhängig von der Zeit seit der letzten Betätigung [8].

Moderne Systeme können verschiedene Formen annehmen, von einfachen Knopfdrucksystemen bis hin zu sensorgestützten Systemen, die die Präsenz und das Bewusstsein des Fahrers überwachen. Die Einführung internationaler Sicherheitsstandards und Vorschriften hat ebenfalls dazu beigetragen, die Etablierung und die Qualität von Sicherheitsfahrschaltungen zu verbessern. Organisationen wie die Internationale Eisenbahnunion und nationale Verkehrssicherheitsbehörden haben Richtlinien und Anforderungen für die Ausrüstung von Zügen mit diesen Sicherheitssystemen festgelegt [18].

2.3 Sicherheitsintegritätslevel

In der Welt der Automatisierungstechnik und insbesondere in sicherheitskritischen Anwendungen wie der Prozessindustrie, der Energieerzeugung und der Verkehrstechnik ist die Zuverlässigkeit von Steuerungs- und Sicherheitssystemen von zentraler Bedeutung. Zur Klassifizierung solcher sicherheitskritischen Systeme dient das Konzept der Sicherheitsintegritätslevel [6].

2.3.1 Definition und Bedeutung der SIL-Level

Das Sicherheitsintegritätslevel dient als Maß für die Qualität und Zuverlässigkeit eines Sicherheitssystems und beschreibt, wie effektiv ein solches System in der Lage ist, gefährliche Fehler zu verhindern oder zu kontrollieren. Die SIL sind ein zentraler Bestandteil der funktionalen Sicherheit und werden in den internationalen Normen IEC 61508 [27] und IEC 61511 [81]

definiert, die Methoden zur Bewertung und Umsetzung der funktionalen Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Sicherheitssysteme bereitstellen [11].

2.3.2 Begriffe und Klassifizierung

Sicherheitsintegritätslevel werden in vier Stufen unterteilt: SIL 1, SIL 2, SIL 3 und SIL 4, wobei jede Stufe ein höheres Sicherheitsniveau repräsentiert. SIL 4 steht dabei für das höchste Maß an Sicherheit. Die Einstufung in ein bestimmtes SIL erfolgt auf Grundlage einer Risikoanalyse, die das potenzielle Risiko eines Systems ohne Sicherheitsfunktionen bewertet. Diese Analyse berücksichtigt die Wahrscheinlichkeit eines gefährlichen Fehlers, die Schwere möglicher Schäden und die Häufigkeit, mit der sich Personen der Gefahr aussetzen [11].

Die DIN EN 50126-1 definiert Risiko in diesem Zusammenhang als eine Kombination aus der Wahrscheinlichkeit des Eintretens eines unerwünschten Ereignisses und den potenziellen Auswirkungen dieses Ereignisses [3]. Die Eintrittswahrscheinlichkeit bezieht sich auf die Wahrscheinlichkeit, dass ein bestimmtes Ereignis eintritt. Diese Wahrscheinlichkeit kann quantitativ (z. B. als statistische Wahrscheinlichkeit) oder qualitativ (z. B. als „hoch", „mittel" oder „niedrig") ausgedrückt werden. Die Auswirkungen beziehen sich auf die möglichen Konsequenzen oder den Schweregrad der Folgen, die mit dem Eintritt des Ereignisses verbunden sind. Diese können ebenfalls quantitativ, etwa in finanziellen Verlusten (z. B. Euro), oder qualitativ, etwa durch Kategorien wie „katastrophal", „ernst" oder „gering", bewertet werden. Das Risiko wird dabei als das Produkt dieser beiden Faktoren verstanden [3].

SIL 1 wird für Systeme verwendet, bei denen das Risiko eines Schadens relativ gering ist, aber dennoch eine signifikante Reduzierung erfordert. SIL 2 kommt bei Anwendungen zum Einsatz, die eine höhere Risikoreduktion erfordern. SIL 3 definiert eine noch größere Risikoreduktion und wird für Systeme eingesetzt, deren Versagen schwerwiegende Konsequenzen haben kann. SIL 4 wird selten angewendet und ist nur für Systeme vorgesehen, in denen das Risiko für einen Schaden extrem hoch ist und katastrophale Auswirkungen haben könnte.

2.3.3 Kenngrößen der Risiko- und Zuverlässigkeitsanalyse

Die Kenngrößen der Risiko- und Zuverlässigkeitsanalyse sind entscheidend für die SIL-Bewertung gemäß IEC 61508 [27] und bahnspezifischen Normen wie DIN EN 50129 [6], da sie die Quantifizierung der Sicherheitsanforderungen eines Systems ermöglichen und als Grundlage für Maßnahmen zur Risikominimierung dienen. Zu den Kenngrößen gehören die Zuverlässigkeit, die Ausfallwahrscheinlichkeit, die mittlere Lebensdauer, die mittlere Instandsetzungszeit, die

mittlere Brauchbarkeitsdauer und die Verfügbarkeit [2]. Eine detaillierte Betrachtung dieser Kenngrößen erfolgt im Anhang A, in dem die SIL-Berechnung umfassend erläutert wird.

2.3.4 Bestimmung des SIL einer Sicherheitsfunktion

Im Anhang A, Unterkapitel 9.2, sind sowohl der Prozess zur Bestimmung des SIL einer Sicherheitsfunktion als auch die erforderlichen Formeln detailliert dargestellt. Der Prozess beginnt mit der Identifikation der Komponenten des Systems und der Ermittlung ihrer Ausfallraten anhand ihrer Datenblätter, gefolgt von einer Fehlerbaumanalyse des Ausfalls einer Sicherheitsfunktion. Anschließend wird die gesamte Zuverlässigkeit berechnet, ebenso wie die mittlere Ausfallzeit (Mean Time to Failure, MTTF) und die tolerierbare funktionale Ausfallrate (Tolerable Functional Failure Rate, TFFR). Die SIL-Einstufung erfolgt dabei auf Basis des TFFR-Werts.

2.4 Sicherheitsaspekte gemäß EN 50129

Der erste Teil des Kapitels behandelt die Sicherheitsanforderungen der Norm DIN EN 50129 [6], welche zentrale Kriterien für die Signaltechnik im Eisenbahnwesen festlegt. Es werden die Anforderungen an RAMS für sicherheitsrelevante elektronische Systeme und die spezifischen Anforderungen für ein SIL3-konformes System vorgestellt.

2.4.1 Qualitätsmanagementprozess

Die grundlegende Bedingung für die Sicherheitsanerkennung eines Systems, Subsystems oder einer Einrichtung ist die kontinuierliche Überwachung der Qualität über dessen gesamte Lebensdauer hinweg durch ein effektives Qualitätsmanagementsystem. Dieses System zielt darauf ab, menschliche Fehler in jeder Phase des Lebenszyklus zu minimieren und die Prozesseffizienz zu steigern, um das Risiko systematischer Fehler zu reduzieren. Gemäß der DIN EN 50126-1 muss das Qualitätsmanagementsystem während der gesamten Lebensdauer des betreffenden Systems oder Subsystems angewendet werden und sollte den Standards der DIN EN ISO 9001 entsprechen [3]. Ein Qualitätsmanagementsystem überwacht und dokumentiert wesentliche Elemente wie Organisationsstruktur, Qualitätssicherungsverfahren, Anforderungsspezifikationen, Designüberwachung, Entwicklungs-, Beschaffungs- und Herstellungsprozesse. Es umfasst Produktidentifikation, Handhabung, Lagerung, Inspektionen, Tests, den Umgang mit Nichtkonformitäten, Verpackung, Versand, Installation, Betrieb, Wartung, Qualitätskontrolle, Berichterstattung, Dokumentation, Konfigurationsmanagement, Personalqualifikation, Schulung, Qualitätsaudits sowie Stilllegung und Entsorgung. Dieser Prozess ist für alle sicherheitsgerichteten Systeme verpflichtend [6].

2.4.2 Der Sicherheitsnachweis

Bevor das betrachtete System als hinreichend sicher für seine vorgesehenen Anwendungen anerkannt werden kann, müssen wesentliche Nachweise erbracht werden. Diese umfassen den Nachweis des Qualitätsmanagements, den Nachweis des Sicherheitsmanagements sowie den Nachweis der funktionalen und technischen Sicherheit. Der Sicherheitsnachweis besteht aus der dokumentierten Bestätigung der Sicherheit für das jeweilige System, Subsystem oder die Einrichtung [6]. In der folgenden Abbildung 2.3 wird die Struktur des Sicherheitsnachweises nach DIN EN 50129 dargestellt.

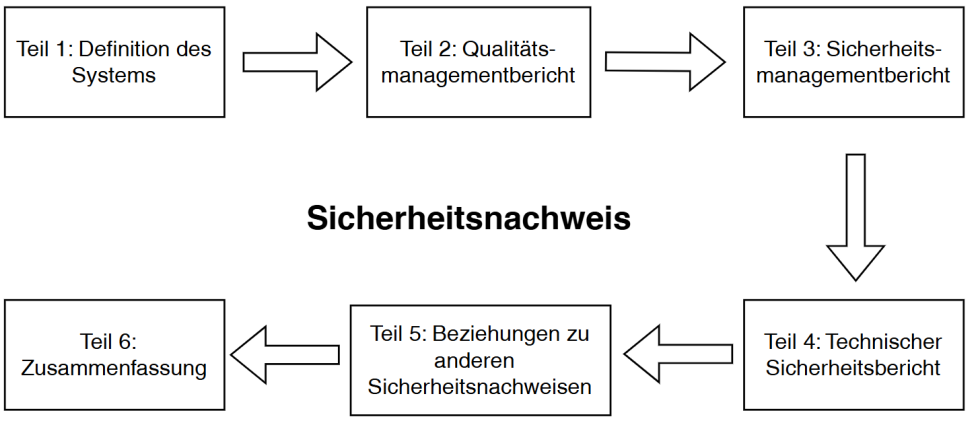


Abbildung 2.3: Struktur des Sicherheitsnachweises [6]

Gemäß der Norm DIN EN 50129 [6] muss der Sicherheitsnachweis wie folgt strukturiert werden:

Teil 1 – Definition des Systems

In diesem Teil muss das System, Subsystem oder die Einrichtung, auf das sich der Sicherheitsnachweis bezieht, präzise definiert oder referenziert werden. Dies schließt Versionsnummern und den Änderungsstatus aller relevanten Dokumentationen zu Anforderungen, Entwürfen und Anwendungen ein.

Teil 2 – Qualitätsmanagementbericht

In diesem Teil muss dokumentiert werden, dass die Effektivität des Qualitätsmanagementsystems nachgewiesen wurde.

Teil 3 – Sicherheitsmanagementbericht

Dieser Teil muss einen dokumentierten Beleg enthalten, der die Einhaltung aller Aspekte des Sicherheitsmanagementsprozesses über den gesamten Lebenszyklus hinweg bestätigt.

Teil 4 – Technischer Sicherheitsbericht
Dieser Teil muss den technischen Nachweis der Sicherheit des Entwurfs enthalten.

Teil 5 – Beziehungen zu anderen Sicherheitsnachweisen
Dieser Teil sollte Verweise auf die Sicherheitsnachweise aller Systeme, Subsysteme oder Einrichtungen enthalten, von denen das betrachtete System abhängig ist. Zudem muss dargelegt werden, dass alle sicherheitsrelevanten Anwendungsbedingungen aus diesen Nachweisen im betrachteten System erfüllt oder als sicherheitsrelevante Anwendungsbedingungen übernommen wurden.

Teil 6 – Zusammenfassung
In diesem Teil sollte eine Zusammenfassung der in den vorherigen Teilen des Sicherheitsnachweises dargelegten Belege erfolgen. Es muss bestätigt werden, dass das betrachtete System, Subsystem oder die Einrichtung unter Einhaltung der festgelegten Anwendungsbedingungen angemessen sicher ist.

Diese Arbeit legt besonderen Fokus auf den technischen Sicherheitsbericht. Dies liegt vor allem daran, dass die DIN EN 50129 diesen Bereich umfassend behandelt. Aufgrund zeitlicher Einschränkungen und des Umfangs der Arbeit wird es deshalb nicht möglich sein, die Teile zwei und drei des Sicherheitsnachweises ausführlich zu erörtern. In Kapitel 6 werden daher ausschließlich die wesentlichen Punkte dieser Abschnitte in tabellarischer Form präsentiert, um einen umfassenden Überblick über die relevanten Aspekte eines Sicherheitsnachweises gemäß der Norm zu bieten.

Der Technische Sicherheitsbericht

Der technische Nachweis für die Sicherheit des Entwurfs muss im technischen Sicherheitsbericht dokumentiert werden, welcher Teil 4 des Sicherheitsnachweises darstellt. Dieser Bericht muss folgende Anforderungen erfüllen: Erstens muss die Erfüllung der System- und Sicherheitsanforderungen nachgewiesen werden, beispielsweise durch einen Verweis auf einen Validierungsbericht. Zweitens muss die Erfüllung der TFFRs (Tolerable Functional Failure Rate) begründet werden. Drittens müssen die Umgebungsbedingungen und die SRACs (Safety Related Application Conditions) definiert werden. Zudem müssen sicherheitsrelevante Funktionen der Basisintegrität in die Sicherheitserprobung einbezogen werden [6].

Die Gliederung des Technischen Sicherheitsberichts entspricht den Anforderungen der Norm DIN EN 50129 [6] und wird in der folgenden Abbildung 2.4 veranschaulicht.

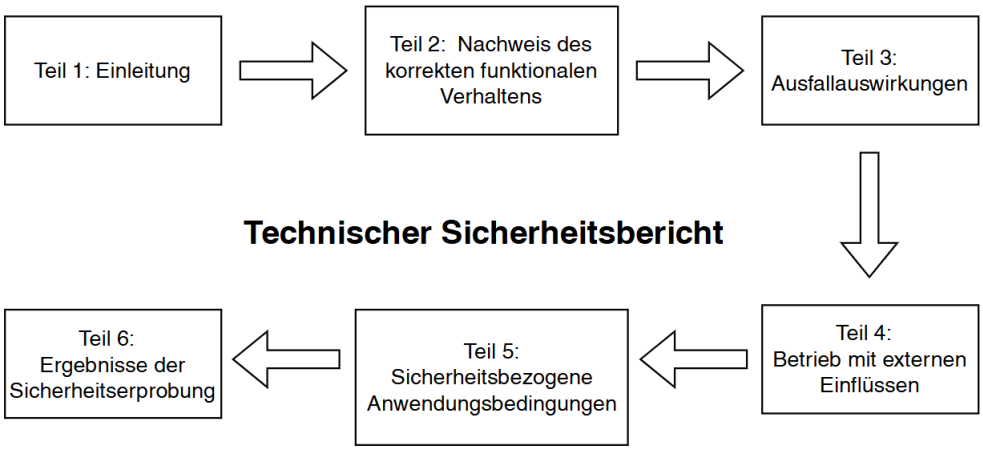


Abbildung 2.4: Struktur des Technischen Sicherheitsberichts [6]

Im Folgenden werden die einzelnen Aspekte des Sicherheitsberichts schematisch dargestellt. Eine detailliertere Ausarbeitung der einzelnen Abschnitte im Kontext des Sicherheitsnachweises für das Sifa-System erfolgt in Kapitel 6, Abschnitt 6.4 „Technischer Sicherheitsbericht“.

Abschnitt 1: Einleitung
Dieser Abschnitt soll den Entwurf umfassend darstellen, einschließlich einer Übersicht über die technischen Sicherheitsprinzipien, die für die Sicherheit des Systems, Subsystems oder der Einrichtung maßgeblich sind [6].

Abschnitt 2: Nachweis des korrekten funktionalen Verhaltens
In diesem Abschnitt muss dokumentiert werden, dass das System, das Subsystem oder die Einrichtung unter störungsfreien Bedingungen und im regulären Betrieb gemäß den definierten Betriebs- und Sicherheitsanforderungen korrekt funktioniert. Dabei sollten die Beschreibung der Systemarchitektur, die Definition der Schnittstellen, die Erfüllung der Systemanforderungsspezifikation und der Sicherheitsanforderungsspezifikation sowie der Nachweis der korrekten Hardwarefunktionalität und Softwarefunktionalität berücksichtigt werden [6].

Abschnitt 3: Ausfallauswirkungen
In diesem Abschnitt ist nachzuweisen, dass das System auch im Falle zufälliger Hardwareausfälle weiterhin die spezifizierten Sicherheitsanforderungen und das quantifizierte Sicherheitsziel

erfüllt. Zudem wird aufgezeigt, welche technischen Schritte unternommen werden, um das resultierende Risiko eines Ausfalls auf ein akzeptables Maß zu reduzieren. Dieser Abschnitt sollte dabei die Auswirkungen von Einzelausfällen, die Unabhängigkeit von Betrachtungseinheiten, die Offenbarung von Einzelausfällen, die Aktion nach der Offenbarung, die Auswirkungen von Mehrfachausfällen sowie den Schutz gegen systematische Fehler beinhalten [6].

Abschnitt 4: Betrieb mit externen Einflüssen
In diesem Abschnitt ist darzulegen, dass das System auch unter den externen Einflüssen, wie in der Systemanforderungsspezifikation festgelegt, sowohl seine definierten betrieblichen als auch seine festgelegten Sicherheitsanforderungen erfüllt. Zu den zu berücksichtigenden relevanten Einflüssen gehören, gemäß der Norm DIN EN 50129 [6], klimatische, mechanische, elektrische und erschwerte Bedingungen sowie Höhe und der Schutz vor unberechtigtem Zugriff.

Abschnitt 5: Sicherheitsbezogene Anwendungsbedingungen
In diesem Abschnitt sind die Regeln, Bedingungen und Einschränkungen zu definieren, die für die funktionale Sicherheit wichtig sind und bei der Nutzung des Systems, Subsystems oder der Einrichtung eingehalten werden müssen. Dazu gehören Systemprojektierung und -aufbau, SRAC für Betrieb, Instandhaltung und Sicherheitsüberwachung sowie SRACs für Stilllegung und Entsorgung [6].

Abschnitt 6: Ergebnisse der Sicherheitserprobung
Dieser Abschnitt muss belegen, dass die Sicherheitstests im Normalbetrieb erfolgreich durchgeführt und abgeschlossen wurden.

2.5 Ausfall- und Gefährdungsanalysemethoden

Die Ausfall- und Gefährdungsanalyse technischer Systeme ist ein wesentlicher Bestandteil des Lebenszyklusmodells (siehe Abb. 2.1) im Rahmen der Risikobeurteilung. Im Folgenden werden die Fehlermöglichkeits- und Einflussanalyse (FMEA) und die Fehlerbaumanalyse (FTA) vorgestellt. Diese sind grundlegend für die Risikobewertung und Sicherheitsgewährleistung technischer Systeme. Sie dienen dazu, potenzielle Fehlerquellen systematisch zu identifizieren, ihre Auswirkungen zu bewerten und geeignete Gegenmaßnahmen abzuleiten.[71]. Der Einsatz beider Methoden wird in Tabelle 6 des Anhangs E der Norm DIN EN 50129 für SIL3 und SIL4 Systeme ausdrücklich empfohlen [6].

2.5.1 Fehlermöglichkeits- und Einflussanalyse (FMEA)

Die Fehlermöglichkeits- und Einflussanalyse (FMEA) ist eine systematische Methode zur Identifizierung und Bewertung potenzieller Fehler in einem Produkt oder Prozess. Der Prozess der FMEA beginnt mit der Identifikation aller möglichen Fehlerarten in einem System, gefolgt von der Bewertung der Schwere (engl. „Severity"), der Auftretenswahrscheinlichkeit (engl. „ocurrence") und der Entdeckungswahrscheinlichkeit (engl. „Detection") jedes Fehlers. Diese Faktoren werden zu einer Risikoprioritätszahl (RPZ) multipliziert, die als Grundlage für die Priorisierung von Maßnahmen dient. Die FMEA umfasst verschiedene Varianten, darunter die Design-FMEA (DFMEA), die potenzielle Fehler im Produktdesign untersucht, und die Prozess-FMEA (PFMEA), die sich mit Fehlern im Fertigungsprozess befasst. Beide Methoden dienen der Erhöhung der Zuverlässigkeit und Sicherheit von Produkten und Prozessen [72].

2.5.2 Fehlerbaumanalyse (FTA)

Die Fehlerbaumanalyse (FTA) ist eine systematische Methode zur Identifikation und Analyse von Ursachen eines unerwünschten Ereignisses in komplexen Systemen. Sie verwendet einen Top-down-Ansatz, bei dem ein Baumdiagramm erstellt wird, um die logischen Beziehungen zwischen einem unerwünschten Top-Ereignis (z. B. Systemausfall) und den zugrunde liegenden Ursachen zu visualisieren. Der Prozess der FTA beginnt mit der Definition des Top-Ereignisses, gefolgt von der Erstellung eines Fehlerbaums, der die Kombination von Basis- und Zwischenereignissen darstellt, die zu diesem Ereignis führen können. Diese Ereignisse werden durch logische Gatter wie UND- und ODER verbunden, um Abhängigkeiten und Wechselwirkungen zu verdeutlichen. Die Methode ermöglicht durch die Visualisierung von Fehlerpfaden eine gezielte Identifikation von Schwachstellen und die Entwicklung effektiver Maßnahmen zur Risikominderung [73].

3 Anforderungsanalyse

In diesem Kapitel wird die Anforderungsanalyse für die sicherheitsgerichtete Entwicklung und den Sicherheitsnachweis eines bahntechnischen SIL3-Systems, am Beispiel einer Sifa, behandelt. Die Analyse ist in vier Teile gegliedert, die Systemanforderungen gemäß den TSI und dem Internationalen Eisenbahnverband UIC 641 sowie die Sicherheitsanforderungen für die Funktionen und Integrität. Zudem werden im Kontext der Anforderungsanalyse die Sicherheitsanforderungen und Systemarchitekturspezifikationen der Norm DIN EN 50129 [6] und die Ausfall- und Gefährdungsanalyse der Sifa vorgestellt.

3.1 Systemanforderungen

3.1.1 Systemanforderungen gemäß TSI

Die Spezifikationen der TSI sind entscheidend für die Gewährleistung der Interoperabilität und Sicherheit im europäischen Eisenbahnnetz. Der Fokus liegt hier sowohl auf der Identifikation und Analyse der relevanten TSI-Anforderungen, die speziell für die Sicherheitsfahrschaltung gelten als auch auf deren Einhaltung. Die TSI definieren im Rahmen der Inspektionsanforderungen spezifische Punkte, die im weiteren Verlauf detailliert tabellarisch dargestellt werden [17]. Zur Überprüfung der Einhaltung der TSI im Rahmen der Validierung der Anforderungen, beinhalten die Tabellen eine Nachweisspalte, in der der jeweilige Prüfstatus der Anforderung dokumentiert wird. In der folgenden Tabelle 3.1 wird der erste Punkt der Inspektionsanforderung für die Kontrolle der Wachsamkeit des Triebfahrzeugführers vorgestellt.

Tabelle 3.1: Kontrolle der Wachsamkeit des Triebfahrzeugführers[17]

Punkt	Inspektionsanforderung	Nachweis
(1)	Der Führerraum ist mit einer Vorrichtung auszustatten, mit der die Aktivität des Triebfahrzeugführers überwacht und der Zug automatisch angehalten werden kann, wenn eine fehlende Aktivität des Triebfahrzeugführers erkannt wird. Mit dieser fahrzeugseitigen technischen Vorrichtung kann das Eisenbahnunternehmen die Anforderung des Abschnitts 4.2.2.9 der TSI OPE erfüllen.	Wird geprüft

In der folgenden Tabelle 3.2 wird der zweite Punkt der Inspektionsanforderung über die Spezifikationen für die Vorrichtungen zur Überwachung der Aktivität für die Kontrolle der Wachsamkeit des Triebfahrzeugführers vorgestellt.

Tabelle 3.2: Spezifikationen für die Vorrichtungen zur Überwachung der Aktivität [17]

Punkt	Inspektionsanforderung	Nachweis
(2)	Spezifikationen für die Vorrichtungen zur Überwachung der Aktivität (und zur Erkennung einer fehlenden Aktivität) des Triebfahrzeugführers:	
	Die Aktivität des Triebfahrzeugführers ist zu überwachen, sofern sich der Zug in Fahrkonfiguration im Zustand „Fahren“ befindet. (Kriterium für die Bewegungserkennung ist eine niedrige Geschwindigkeitsschwelle.) Diese Überwachung hat über die Kontrolle der Aktivität des Triebfahrzeugführers in Bezug auf anerkannte Schnittstellen zwischen dem Triebfahrzeugführer und dem Fahrzeug wie z. B. bestimmte Vorrichtungen (Pedal, Druckknöpfe, Sensoren usw.) und/oder anerkannte Schnittstellen zwischen dem Triebfahrzeugführer und der Leit- und Steuerungselektronik zu erfolgen.	Wird geprüft
	Wird an den anerkannten Schnittstellen zwischen Triebfahrzeugführer und Fahrzeug während eines Zeitraums von mehr als X Sekunden keine Aktivität beobachtet, wird eine fehlende Aktivität des Triebfahrzeugführers festgestellt.	Wird überprüft
	Das System muss (in der Werkstatt im Rahmen der Instandhaltung) eine Anpassung der Zeit X innerhalb einer Spanne von 5 bis 60 Sekunden ermöglichen.	Wird geprüft
	Wird die gleiche Aktivität fortlaufend über einen Zeitraum von mehr als maximal 60 Sekunden ohne weitere Aktivitäten an einer anerkannten Schnittstelle zwischen Triebfahrzeugführer und Fahrzeug beobachtet, stellt das System ebenfalls eine fehlende Aktivität des Triebfahrzeugführers fest.	Wird geprüft
	Vor dem Feststellen einer fehlenden Aktivität des Triebfahrzeugführers erfolgt eine entsprechende Warnung an den Triebfahrzeugführer, damit dieser reagieren und das System zurücksetzen kann.	Wird geprüft
	Dem System soll die Information „Fehlende Aktivität des Triebfahrzeugführers erkannt“ zur Übermittlung an andere Systeme (z. B. das Funksystem) zur Verfügung stehen.	Wird geprüft

In der folgenden Tabelle 3.3 wird der dritte Punkt der Inspektionsanforderung für die Kontrolle der Wachsamkeit des Triebfahrzeugführers vorgestellt.

Tabelle 3.3: TSI-Kontrolle der Wachsamkeit des Triebfahrzeugführers -zusätzliche Anforderung [17]

Punkt	Inspektionsanforderung	Nachweis
(3)	Zusätzliche Anforderung:	
	Die Funktion zur Erkennung einer fehlenden Aktivität des Triebfahrzeugführers ist einer Zuverlässigkeitsuntersuchung zu unterziehen, in der Fehlermodi der betreffenden Komponenten ebenso zu berücksichtigen sind wie Redundanzen, die eingesetzte Software, regelmäßige Prüfungen und sonstige Vorschriften. Die geschätzte Ausfallquote der Funktion (d. h. die Wahrscheinlichkeit, dass eine fehlende Aktivität des Triebfahrzeugführers im oben beschriebenen Sinne nicht erkannt wird) ist in Abschnitt 4.2.12 beschriebenen und in der technischen Dokumentation anzugeben.	Wird geprüft

In der folgenden Tabelle 3.4 wird der vierte Punkt der Inspektionsanforderung zur Anzeige von Aktivitäten für die Kontrolle der Wachsamkeit des Triebfahrzeugführers vorgestellt.

Tabelle 3.4: TSI-Spezifikationen zur Anzeige von Aktivitäten [17]

Punkt	Inspektionsanforderung	Nachweis
(4)	Spezifikationen zur Anzeige von Aktivitäten auf Zugebene, wenn eine fehlende Aktivität des Triebfahrzeugführers erkannt wird:	
	Bei fehlender Aktivität des Triebfahrzeugführers in einem Zug, der sich in Fahrkonfiguration im Zustand „Fahren“ befindet (Kriterium für die Bewegungserkennung ist eine niedrige Geschwindigkeitsschwelle), muss eine Vollbremsung erfolgen.	Wird geprüft

Die detaillierte Beschreibung der Sicherheitsanforderungen für die Sifa befindet sich in der Verordnung (EU) Nr. 1302/2014 der Kommission vom 18. November 2014 über eine technische Spezifikation für die Interoperabilität des Teilsystems „Fahrzeuge — Lokomotiven und Personenwagen“ des Eisenbahnsystems in der Europäischen Union. Die Überwachung der Wachsamkeit des Triebfahrzeugführers (4.2.9.3.1.) ist in der Schnittstelle zwischen Triebfahrzeugführer und Maschine angesiedelt, speziell unter den Bereichen Führerraum und Schnittstelle Triebfahrzeugführer-Maschine [17]. Diese ist weiterhin Teil der funktionalen und technischen Spezifikationen des Teilsystems im vierten Kapitel, welches die Merkmale des Teilsystems „Fahrzeuge“ behandelt.

3.1.2 System Bedingungen der Sifa gemäß UIC 641

Die Norm 641 des internationalen Eisenbahnverbandes (UIC) definiert Anforderungen für Sicherheitsfahrschaltungen im internationalen Verkehr [18]. In der folgenden Tabelle 3.5 werden die UIC Anforderungen 1 bis 3 zur Inspektion einer Sifa dargestellt. Zur Dokumentation der Einhaltung der Inspektionsanforderungen im Rahmen der Validierung der Anforderungen in Kapitel 6, enthalten die kommenden Tabellen eine Nachweisspalte.

Tabelle 3.5: UIC 641 Anforderungen 1-3 [18]

	Inspektionsanforderung	**Nachweis**
1	Aufgabe	
	Die Sicherheitsfahrschaltung überwacht die Dienstfähigkeit des Triebfahrzeugführers vom Fahrzeug aus. Sie wirkt unabhängig von ortsfesten Einrichtungen. Bei nicht ordnungsgemäßer Bedienung durch den Triebfahrzeugführer veranlasst sie die Abschaltung der Antriebskraft des Triebfahrzeugs und eine Zwangsbremsung.	Wird geprüft
2	Einrichtung auf dem Führerraum	
	Die Führerraumeinrichtungen umfassen: 1. Betätigungseinrichtungen wie zum Beispiel Handtaster, Fußtaster, Kniehebel, 2. eine akustische Signaleinrichtung wie zum Beispiel Summer, Hupe, Wecker. Dieses Signal muss unter allen Betriebsbedingungen hörbar sein, 3. es können zusätzliche optische Signaleinrichtungen vorgesehen werden.	Wird geprüft
3	Bereitschaftsstellung	
3.1.	Die Sicherheitsfahrschaltung schaltet sich spätestens selbsttätig ein, wenn die Geschwindigkeit von $20\,\mathrm{km/h}$ erreicht ist, und bleibt eingeschaltet, solange die Geschwindigkeit diesen Wert überschreitet.	Wird geprüft
3.2.	Einzelne Bahnen können jedoch im gegenseitigen Einvernehmen eine Sicherheitsfahrschaltung verwenden, die vor dem Anfahren vom Triebfahrzeugführer einzuschalten ist.	Wird geprüft

In der folgenden Tabelle 3.6 werden die UIC 641 Anforderungen 4 und 5 dargestellt.

Tabelle 3.6: UIC 641 Anforderungen 4-5 [18]

	Inspektionsanforderung	**Nachweis**
4	Eingriffsstellung	
4.1.	Wenn in Bereitschaftsstellung: 1. keine der Betätigungseinrichtungen betätigt wird oder 2. die Betätigungseinrichtungen ohne Unterbrechung länger als t= 30 sek. betätigt werden, a) ertönt spätestens nach 2, 5 sek. ein akustisches Signal, b) wird nach spätestens weiteren 2, 5 sek. die Antriebskraft abgeschaltet und eine Zwangsbremsung eingeleitet. Die angegebenen Zeiten können mit Toleranzen von 15% behaftet sein.	Wird geprüft
4.2.	An Stelle der Zeiten nach Punkt 4.1 - Seite 5 der UIC-Norm 641 kann die Sicherheitsfahrschaltung auch nach bestimmten Wegen eingreifen, die so festgelegt werden, dass sich bei Fahrgeschwindigkeiten von 100 km/h die Zeiten nach Punkt 4.1 ergeben.	Wird geprüft
4.3.	An Stelle der Unterbrechung der Betätigung der Betätigungseinrichtungen kann die Betätigung eines anderen Steuerorgans treten, wenn das im Schema der Sicherheitsfahrschaltung vorgesehen ist und dadurch die gleiche Wirkung hervorgerufen wird wie durch das Loslassen.	Wird geprüft
4.4.	Ein Ausfall der zum Betrieb der Sicherheitsfahrschaltung nötigen Versorgungsspannung führt zur Abschaltung der Antriebszugkraft und zur Zwangsbremsung.	Wird geprüft
4.5.	Bei Einleitung der Zwangsbremsung durch die Sicherheitsfahrschaltung muss die Entlüftung der Hauptluftleitung in einer Zeit erfolgen, die nicht grösser ist als bei Einleitung einer Schnellbremsung durch das Führerbremsventil. Die bei Entlüftung entweichende Luftmenge per Zeiteinheit muss merklich grösser als die durch die Bremseinrichtung in Füllstellung des Führerbremsventils nachgespeiste Luftmenge sein, um ein sicheres Ansprechen der Bremsen des Zuges zu gewährleisten.	Wird geprüft
5	Aufhebung des Eingriffes	
5.1.	Vor Eintreten der Zwangsbremsung kann das Eingreifen der Sicherheitsfahrschaltung aufgehoben werden, indem bei Ansprechen entweder eine der Betätigungseinrichtungen nach Punkt 2, Absatz 1 betätigt wird oder die Betätigung der Betätigungseinrichtungen kurzzeitig unterbrochen wird.	Wird geprüft
5.2.	Nach Abschalten der Antriebskraft und Eintreten der Zwangsbremsung kann das Eingreifen der Sicherheitsfahrschaltung nur aufgehoben werden, wenn zusätzlich zu den unter Punkt 5.1 genannten Betätigungshandlungen vom Triebfahrzeugführer mindestens eine weitere Tätigkeit ausgeführt wird, zum Beispiel das Auslösen der Bremse oder Wiederherstellung der Antriebskraft.	Wird geprüft

3.1.3 Gefährdungsanalyse und Risikobewertung der Sifa

Die Gefährdungsanalyse und Risikobewertung technischer Systeme ist ein wesentlicher Bestandteil des RAMS-Managements des Lebenszyklusmodells (siehe Abbildung 2.1) und ist im Rahmen der Risikobeurteilung durchzuführen. Die Gefährdungsanalyse und Risikobewertung der Sifa wird mit Unterstützung der Methode zum Festlegen und Nachweisen sicherheitsbezogener Anforderungen und Bewertung der Risiken im Rahmen der Umsetzung der CSM-RA (Common Safety Method for Risk Evaluation and Assessment) und der EN 50126 der Sicherheitsregelung Fahrzeug (SIRF) durchgeführt [13]. In der folgenden Tabelle 3.7 wird die Eisenbahnfahrzeugfunktion dargestellt.

Tabelle 3.7: Eisenbahnfahrzeugfunktion - SIRF [13]

Funktion	**Erläuterung der Funktion**	**Themen**	**Betriebs- und Umgebungsbedingungen**
Handlungsunfähigkeit Fahrzeugführer beherrschen	—	Sifa, alternierende Überwachung	—

In der folgenden Tabelle 3.8 wird die Gefährdungsermittlung dargestellt.

Tabelle 3.8: Gefährdungsermittlung - SIRF [13]

Sichere Gewährleistung von…	**Gefährdung ist gegeben, wenn….**	**Nr. Teilgefährdung**	**Maßgebliche Teilgefährdung**
Überwachung im notwendigen Umfang und auf geeignete Weise	Erkennung auf ungeeignete Weise erfolgt	1d	Ausfall Triebfahrzeugführer wird nicht erkannt

Die zulässigen Parameter zur Berechnung des Einstufungsindikators (I) werden in der folgenden Tabelle 3.9 dargestellt.

Tabelle 3.9: Zulässige Parameter für die Gefährdungseinstufung [13]

Schaden (S) = $S_A \cdot S_V$			
Anzahl (S_A)		**Verletzungsgrad** (S_V)	
einer (1 Person)	3	Leichtverletzte	2
mehrere(bis 10 Personen)	5	Schwerverletzte	4
viele (mehr als 10 Personen)	8	Tote	9
Eintrittswahrscheinlichkeit (W)			
niedrig			1
mittel			1,7
hoch			3
Expositionsdauer (E)			
kurz			1
lang			1,3
Vermeidung (V)			
nicht möglich			1
möglich			1,7

In der folgenden Tabelle 3.10 wird die Gefährdungseinstufung dargestellt.

Tabelle 3.10: Gefährdungseinstufung - SIRF [13]

Schaden Anzahl S_A	**Schaden Verletzungsgrad** S_V	**Eintrittswahrscheinlichkeit** W	**Exposition Dauer** E	**Vermeidung** V
Viele (> 10 Personen)	Tote	Niedrig	Lang	Nicht möglich
$8,0$	$9,0$	$1,0$	$1,3$	$1,0$

Im Falle eines Versagens der Überwachung der Wachsamkeit des Triebfahrzeugführers wird die Gefahr wie folgt eingestuft: Der Schaden, der entsteht, wenn ein Zug ohne Lokführer fährt, könnte das Leben von mehreren Hundert Passagieren und anderen Verkehrsteilnehmenden gefährden. Daher erfolgt die Einstufung für die Schadensanzahl (S_A) als „viele" (mehr als 10 Personen) und für den Verletzungsgrad (S_V) als „Tote". Die Eintrittswahrscheinlichkeit (W) wird als niedrig eingestuft, wenn das Schadensausmaß nach Versagen der Funktion nahezu ausgeschlossen ist [13]. Die Expositionsdauer (E) wird als lang eingestuft, wenn die betroffene

Person während der überwiegenden Aufenthaltsdauer im Gefahrenbereich der möglichen Gefährdung ausgesetzt ist. Die Vermeidung (V) wird als „nicht möglich" eingestuft weil die betroffene Person durch eigenes Handeln keine Möglichkeit hat, den Schaden zu vermeiden [13].

Gefährdungseinstufung:

Verwendet wird die Methode zum Festlegen und Nachweisen sicherheitsbezogener Anforderungen und Bewertung der Risiken im Rahmen der Umsetzung der CSM-RA und der EN 50126 [13]. Um die Sicherheitsanforderungsstufe (I) zu berechenn, wird die folgende Formel 3.1 verwendet:

$$I = \frac{S \cdot W \cdot E}{V} \tag{3.1}$$

Der Schaden (S) wird wie folgt berechnet:

$$S = S_A \cdot S_V = 8,0 \cdot 9,0 = 72,0 \tag{3.2}$$

Für die Sicherheitsfahrschaltung wird die Sicherheitsanforderungsstufe wie folgt berechnet:

$$I = \frac{S \cdot W \cdot E}{V} = \frac{72,0 \cdot 1,0 \cdot 1,3}{1,0} = 93,60 \tag{3.3}$$

In der folgenden Tabelle 3.11 wird der Einstufungsindikator gezeigt.

Tabelle 3.11: Einteilung der Sicherheitsanforderungsstufe (SAS) [13]

Einstufungsindikator (I)	**Sicherheitsanforderungsstufe (SAS)**
$I < 21$	0
$21 \leq I < 36$	1
$36 \leq I < 72$	2
$72 \leq I < 122$	3
$122 \leq I < 281$	4

Wie in Tabelle 3.11 ersichtlich, ist die Sicherheitsfahrschaltung der Sicherheitsanforderungsstufe 3 (SAS 3) zugeordnet. Obwohl SAS 3 und SIL 3 nicht identisch sind, weisen sie eine inhaltliche Verbindung auf. Die Sicherheitsanforderungsstufe legt die funktionalen und betrieblichen Sicherheitsanforderungen fest, während das Sicherheits-Integritätslevel quantifiziert, mit welcher Zuverlässigkeit diese Anforderungen erfüllt werden müssen. Beide Konzepte gewährleisten, dass sicherheitskritische Systeme in der Lage sind, Risiken in potenziell gefährlichen Umgebungen wirksam zu minimieren. In Kapitel 6 wird demonstriert, ob die Entwicklung dieser Arbeit die SIL-3-Einstufung erreicht hat.

3.2 Sicherheitsanforderungen

In den folgenden Unterkapiteln werden die Sicherheitsanforderungen einer Sicherheitsfahrschaltung gemäß der Norm DIN EN 50129 [6] dargelegt.

3.2.1 Anforderungen an die Sicherheitsfunktionen

- **Aktivitätserkennung:** Das System muss die Aktivität des Triebfahrzeugführers kontinuierlich überwachen [17] & [18].
- **Warnsignal:** Bei Inaktivität des Triebfahrzeugführers über einen Zeitraum von 30 Sekunden muss innerhalb von weiteren 2,5 ein optisches Signal ausgelöst werden [18].
- **Notbremssignal:** Wenn innerhalb von 2,5 Sekunden nach dem Warnsignal keine Aktivität festgestellt wird, muss sowohl ein optisches als auch ein akustisches Signal ausgelöst werden und das System eine Notbremsung einleiten, sobald die Zeit abläuft [18].
- **Manuelle Übersteuerung:** Das System muss eine Schnittstelle für die manuelle Übersteuerung durch den Triebfahrzeugführer bieten, um das Warnsignal zurückzusetzen oder die Notbremsung zu stoppen [18].
- **Benutzerschnittstelle:** Das System muss über eine klare und intuitive Benutzerschnittstelle verfügen, die es dem Triebfahrzeugführer ermöglicht, schnell und effektiv auf Warnsignale zu reagieren und das System bei Bedarf zu übersteuern [17] & [18].

3.2.2 Anforderungen an die Sicherheitsintegrität

- **Zuverlässigkeit:** Die Funktionalität der Sifa entspricht der Sicherheitsanforderungsstufe SIL-3 gemäß den CENELEC-Normen. Das System muss gewährleisten, dass im Zustand „Aktiv“ eine Zwangsbremsung ausgelöst wird, falls das Wachsamkeitssignal über den festgelegten Zeitraum ausbleibt. Die Wahrscheinlichkeit, dass die Signalisierung der Zwangsbremsung ausbleibt, muss geringer als $1 \cdot 10^{-7} \frac{1}{h}$ sein, wie in der Tabelle 9.2 zu sehen ist [6].
- **Reaktionszeit:** Die Reaktionszeit für die Auslösung des Warnsignals und die Aktivierung der Notbremsung darf maximal 5,0 Sekunden betragen [18].
- **Umweltbedingungen und Höhe:** Das System wird in einem Temperaturbereich T3 im Fahrzeugabteil von $-25°$ C bis $+55°$ C und bei einer relativen Luftfeuchtigkeit mit

einem Jahresmittelwert von 75 % funktionieren. Die Höhenlage wird die Klasse A3, die nicht 1 200 m über dem Meeresspiegel überschreitet [6] & [70].

- **Mechanische Bedingungen:** Das Sytem muss eine Vibrations- und Stoßfestigkeit, eine Temperaturbeständigkeit, einen Feuchtigkeits- und Korrosionsschutz sowie eine Montage- und Wartungsfreundlichkeit aufweisen [6].

3.2.3 Integrität gegen systematische Fehler

- **Fail-Safe-Mechanismen:** Das System muss in einem sicheren Zustand verbleiben, auch bei Ausfall von zwei Komponenten, aufgrund der Unabhängigkeit zwischen den Betrachtungseinheiten [6].
- **Permanente Sifa-Tastenbetätigung:** Das System ist darauf ausgelegt, eine kontinuierliche Betätigung der Sifa-Taste zu erkennen und unverzüglich darauf zu reagieren [6].
- **Einhaltung von Normen:** Das System muss den Sicherheitsnormen gemäß UIC 641 [18] und anderen relevanten Eisenbahnstandards wie DIN EN 50129 [7] und den TSI [17] entsprechen .

3.2.4 Integrität gegen zufällige Ausfälle

- **Redundanz:** Um die Integrität gegen zufällige Ausfälle zu gewährleisten, muss das System redundante Komponenten verwenden, insbesondere in kritischen Bereichen wie der Signalverarbeitung und der Energieversorgung [6].
- **Common-Cause-Failure:** Ein Common-Cause-Failure ist der Ausfall mehrerer Komponenten oder Strukturen als Folge desselben auslösenden Ereignisses oder Fehlers [67]. Um Common-Cause-Failures zu verhindern, ist der Einsatz einer zweikanaligen, diversitären Mikrocontrollerarchitektur erforderlich. Sämtliche Eingänge und Ausgänge müssen dabei von beiden Kanälen evaluiert werden [6].
- **Selbsttest:** Das System sollte einen Selbsttest am Anfang der Aktivierung des Systems durchführen, um sicherzustellen, dass alle Komponenten und Funktionen ordnungsgemäß arbeiten. Diese Tests helfen, potenzielle Ausfälle frühzeitig zu erkennen und zu beheben [6].
- **Fehlererkennung und -management:** Das System muss in der Lage sein, Fehler zu erkennen und entsprechende Maßnahmen zu ergreifen. [6].

- **Dokumentation und Protokollierung:** Alle Vorfälle und Systemzustände sollten dokumentiert und protokolliert werden, um eine nachträgliche Analyse und eine kontinuierliche Verbesserung des Systems zu ermöglichen [6].
- **Software:** Die Software muss geeignete Mechanismen implementieren, um die Überwachung potenzieller Fehler sicherzustellen [5].
- **Unabhängigkeit der Kanäle:** Um die Demonstration der Unabhängigkeit der beiden Kanäle zu vereinfachen, führt man eine galvanische Trennung zwischen den Kanälen durch [6].

3.3 Systemarchitekturspezifikation

Die Tabelle 4 des Anhangs E der Norm DIN EN 50129 [6] wird für die Architektur des Sifa-Systems verwendet. In der Tabelle ist zu sehen, welche Techniken bzw. Maßnahmen zu verwenden sind, um ein Sicherheitsintegritätslevel zu erreichen. Für die Systemarchitektur des Sifa-Systems ist die Zeile (6) zu beachten mit der Verwendung von einer zweikanaligen elektronischen Struktur basierend auf „fail-safety“ durch mindestens zwei Betrachtungseinheiten mit dem „fail-safe“ Vergleich. In der folgenden Tabelle 3.12 wird die Architektur des Systems gezeigt. R: Recommended, HR: High Recommended und NR: Not Recommended.

Tabelle 3.12: Architektur des Systems, des Subsystems oder der Einrichtung [6]

Techniken/Maßnahmen	**SIL1**	**SIL2**	**SIL3**	**SIL4**
(1) Trennung von sicherheitsbezogenen Funktionen von nicht sicherheitsbezogenen Funktionen zur Verhinderung nicht beabsichtigter Einflüsse	Abschnitt 3 im Technischen Sicherheitsbericht			
(2) Einkanalige elektronische Struktur mit Selbsttests und Überwachung	R	R	NR	NR
(3) Einkanalige elektronische Struktur basierend auf „fail-safety“ durch unverlierbare Eigenschaften	R	R	HR	HR
(4) Einkanalige elektronische Struktur basierend auf „fail-safety“ durch sicherheitsgerichtete Ausfallreaktion	R	R	HR	HR
(5) Zweikanalige elektronische Struktur	R	R	NR	NR
(6) Zweikanalige elektronische Struktur basierend auf „fail-safety“ durch mindestens zwei Betrachtungseinheiten mit dem „fail-safe“ Vergleich	R	R	HR	HR
(7) Diversitäre elektronische Struktur mit dem „fail-safe“ Vergleich	R	R	HR	HR

3.3.1 System Definition: Zeit-Sifa

Die Sicherheitsfahrschaltung ist darauf ausgelegt, einen Zug durch eine Zwangsbremsung innerhalb eines festgelegten Zeitraumes zum Stillstand zu bringen, falls sie aufgrund der Handlungsunfähigkeit des Triebfahrzeugführers während der Fahrt aktiviert wird. Eine Zeit-Sifa ist eine Variante der Sicherheitsfahrschaltung, die auf einem zeitbasierten Überwachungsprinzip beruht [8]. Die entsprechenden zeitlichen Anforderungen an eine solche Sifa sind dem Kapitel 3.2.1 und der Norm UIC 641 [18] zu entnehmen. Um den Umfang dieser Arbeit zu begrenzen, wird die Zeit-Sifa behandelt, während die Weg-Sifa und die Zeit-Weg-Sifa nicht berücksichtigt werden.

3.3.2 Systemgrenze und Schnittstellen

Das System ist auf die Fahrerkabine und die zugehörigen Steuerungssysteme des Zuges beschränkt. In diesem Abschnitt werden sowohl die Eingangs- und Ausgangsschnittstellen als auch das Sifa-System beschrieben. In der folgenden Abbildung 3.1 es ist zu sehen wie die Systemgrenze definiert ist.

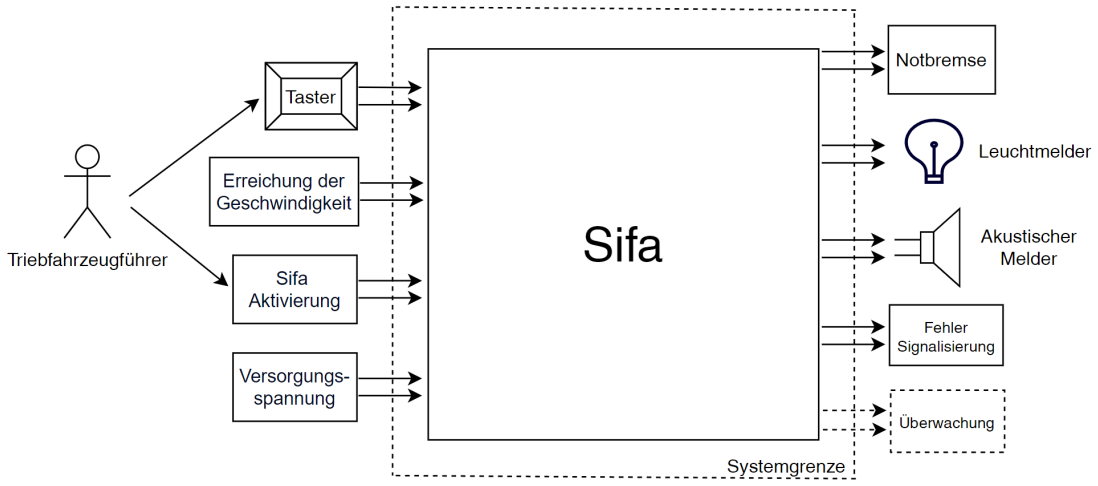


Abbildung 3.1: Sifa Systemabgrenzung

- **Eingangsschnittstelle:**
  - Sifa-Drucktaster: Erfasst die Aktivität des Triebfahrzeugführers.
  - Erreichung der Geschwindigkeit: Bestätigung, dass eine Geschwindigkeit von $20\,\mathrm{km/h}$ erreicht wurde [18]. Dieses Signal stammt aus einem anderen Subsystem und soll mit einem Schalter simuliert werden.
  - Sifa Aktivierung: Der Lokführer soll die Möglichkeit haben, das System zu deaktivieren.
  - Versorgungsspannung: Je eine Spannungsquellen für jeden Mikrocontroller.
- **Ausgangsschnittstelle:**
  - Notbremssignal: Anbindung an das Bremssystem des Zuges für die Notbremsung.
  - Leuchtmelder: Schaltet sich nach 30 Sekunden ohne Betätigung des Sifa-Drucktasters ein.
  - Akustischer Melder: Schaltet sich nach 32,5 Sekunden ohne Bestätigung des Sifa-Drucktasters ein.
  - Fehler Signalisierung: Durch eine gelbe LED.
- **Sifa System:**
  - Mikrocontroller: Vewendung von zwei Mikrocontrollern für das zweikanalige Sifa-System.
  - Galvanische Trennung: Für die Unabhängigkeit der Kanäle.
  - Die Sifa soll alle Arten von Fehlern identifizieren.

3.3.3 Anforderungen an die Simulationssoftware

Ein geeignetes Simulationswerkzeug sollte die Fähigkeit besitzen, sowohl die elektronische Schaltung als auch die Softwarelogik realitätsnah zu modellieren.

- Es sollte eine benutzerfreundliche Oberfläche haben, um die Interaktion mit den simulierten Komponenten zu erleichtern.
- Es sollte die Möglichkeit bieten, verschiedene Szenarien und Fehlermodi zu testen.
- Die Kompatibilität mit den verwendeten Mikrocontrollern und der Einsatz von Echtzeit-Datenanalysen sind wichtige Kriterien, um sicherzustellen, dass das Werkzeug den Anforderungen des Projekts gerecht wird.

3.3.4 Anforderungen an den Entwurf der Software

Bei der Entwicklung einer Sifa mit Mikrocontrollern gibt es verschiedene Programmieransätze, die in Betracht gezogen werden können. In der folgenden Tabelle 3.13 werden die Programmieralternativen dargestellt, die im Anhang D der Norm DIN EN 50128 [5] präsentiert werden.

Tabelle 3.13: Programmieralternativen [5]

Alternative	**Beschreibung**	**Vorteile**	**Nachteile**
Prozedurale Programmierung	Der Code wird in Prozeduren oder Funktionen organisiert, die sequentiell ausgeführt werden.	Einfach zu verstehen und zu implementieren für kleinere, lineare Aufgaben.	Kann bei komplexen Systemen unübersichtlich werden, da die Steuerlogik nicht klar strukturiert ist.
Ereignisgesteuerte Programmierung	Der Code reagiert auf Ereignisse oder Interrupts, die durch externe Signale ausgelöst werden.	Gut geeignet für Systeme, die auf externe Eingaben reagieren müssen.	Kann komplex werden, wenn viele Ereignisse und Zustände verwaltet werden müssen.
Zustandsautomaten	Das System wird als eine Reihe von Zuständen modelliert, mit definierten Übergängen basierend auf Eingaben oder Ereignissen.	Klarheit und Struktur, Vorhersehbarkeit und Fehlervermeidung	Kann bei sehr vielen Zuständen und Übergängen komplex werden.
Objektorientierte Programmierung	Der Code wird in Klassen und Objekten organisiert, die Daten und Funktionen kapseln.	Gut geeignet für komplexe Systeme mit vielen interagierenden Komponenten.	Kann für einfache Mikrocontroller-Anwendungen überdimensioniert sein.

Die Wahl fällt auf die Zustandsautomaten-Alternative, da sie durch ihre Modularität ermöglicht, die Logik in überschaubare Module zu unterteilen, was die Entwicklung und Fehlersuche erheblich erleichtert. Ein weiterer Vorteil besteht darin, dass neue Zustände oder Übergänge relativ einfach hinzugefügt werden können, ohne das gesamte System überarbeiten zu müssen. Zudem tragen Zustandsautomaten dazu bei, unerwartete Zustände oder Übergänge zu vermeiden, was insbesondere in sicherheitskritischen Anwendungen wie einer Sifa-Schaltung von großer Bedeutung ist. Die funktionalen Anforderungen an den Entwurf der Software werden in den folgenden Tabellen dargestellt. Diese enthalten neben einer inhaltlichen Beschreibung auch eine Nachweisspalte, in der der aktuelle Prüfstand angegeben wird. In der Tabelle 3.14 werden die funktionalen Anforderungen an den Entwurf der Software gezeigt.

Tabelle 3.14: Funktionale Anforderungen an den Entwurf der Software

Nummer	Funktionale Anforderungen Software	Nachweis
1	Selbsttest-Zustand:	
	Nach Anlegen der Versorgungsspannung, muss die Sicherheitsfahrschaltung einen automatischen Selbsttest durchführen.	Wird geprüft
2	Ruhezustand:	
	Nach erfolgreichem Abschluss des Selbsttests wechselt die Sifa in den Ruhezustand.	Wird geprüft
	Im Ruhezustand der Sifa darf der Ausgang für das Notbremssignal nicht aktiviert sein; zudem müssen alle Sifa-Relais deaktiviert sein.	Wird geprüft
	Die Sifa wechselt in den Ruhezustand, sobald der aktuelle Zustand „Sifa-System-Aktiv“ ist und die Geschwindigkeit unter den festgelegten Schwellenwert fällt.	Wird geprüft
3	Sifa-System-Aktiv:	
	Wenn das Sifa-System-Aktiv ist, wird es die Wachsamkeit des Triebfahrzeugführers überwachen, wenn die Mindestgeschwindigkeit erreicht wurde und das System im Ruhezustand ist.	Wird geprüft
4	Sifa-System Inaktiv-Zustand:	
	Die Sifa wechselt in den Zustand „Inaktiv“, sobald sie sich entweder im „Ruhezustand“ oder im Zustand „Sifa-System-Aktiv“ befindet und eine externe Inaktivierung erkannt wird.	Wird geprüft
	Wenn die Sifa sich im Zustand „Inaktiv“ befindet, darf der Ausgang für die Notbremse nicht aufgrund der Sifa aktiviert sein.	Wird geprüft
5	Warning-Zustand:	
	Die Sifa wechselt in den Zustand „Warning“, sobald sie im Zustand „Sifa-System-Aktiv“ ist und das Wachsamkeitssignal des externen Tasters ausbleibt.	Wird geprüft
	In diesem Zustand wird für 2,5 Sekunden ein optisches Signal angezeigt. Sollte keine Reaktion erfolgen, verbleibt das System im Zustand „Warning“, wobei zusätzlich ein akustisches Signal nach weiteren 2,5 Sekunden ausgelöst wird.	Wird geprüft
6	Emergency-Brake-Zustand:	
	Die Sifa wechselt in den Zustand „Emergency-Brake“, sobald sie im Zustand „Warning“ ist und das Wachsamkeitssignal des externen Tasters ausbleibt.	Wird geprüft
7	Fehlerdiagnose-Zustand:	
	Die Sifa-Funktion muss eine Fehlerdiagnosefähigkeit besitzen und die entsprechenden Informationen an den Systemgrenzen bereitstellen.	Wird geprüft

3.4 Ausfall- und Gefährdungsanalyse

3.4.1 Sifa- Fehlermöglichkeits- und Einflussanalyse (FMEA)

Die Fehlermöglichkeits- und -einflussanalyse (FMEA) für die Sicherheitsfahrschaltung wird in der folgenden Tabelle 3.15 dargestellt.

Tabelle 3.15: Fehlermöglichkeits- und Einflussanalyse (FMEA)

Fehlerart	**Mögliche Ursache**	**Auswirkung**	**Erkennung Methode**	**Abhilfe Maßnahme**
1. Signal des Drucktasters erreicht Mikrocontroller nicht	Kabel/Leitung defekt	Keine Erkennung der Fahreraktivität	Diagnose durch Selbsttest, Überwachung der Signalleitungen	Redundante Leitungen, regelmäßige Wartung und Inspektion
2. Notbremssignal wird nicht erkannt	Unterbrechung zwischen Mikrocontroller und Notbremse-Relais	Notbremse wird nicht ausgelöst, Gefahr eines Unfalls	Überwachung der Signalintegrität, Selbsttest	Redundante Leitungen, regelmäßige Inspektion
3. Ausfall des Mikrocontrollers	Hardware-Fehler, Überhitzung	Gesamtsystemausfall, keine Sicherheitsfunktionen aktiv	Selbsttest, Überwachung der Systemparameter	Einsatz von redundanten Mikrocontrollern, Kühlungssysteme
4. Fehlfunktion des Relais	Mechanischer Defekt, Verschleiß	Notbremse wird nicht aktiviert, Sicherheitsrisiko	Einsatz von redundanten Relais, Selbsttest	Verwendung von hochwertigen Relais, regelmäßige Wartung
5. Softwarefehler im Zustandsautomaten	Programmier-Fehler, unzureichende Tests	Falsche Zustandsübergänge, unvorhersehbares Systemverhalten	Softwaretests, Simulationen	Umfangreiche Tests, Code-Reviews, regelmäßige Updates
6. Ausfall der Stromversorgung	Defekte Stromquelle, Kabelbruch	Gesamtsystemausfall, keine Sicherheitsfunktionen aktiv	Überwachung der Stromversorgung, Selbsttest	Redundante Stromquellen

3.4.2 Fehlerbaumanalyse (FTA)

Die Abbildung 3.2 stellt die Fehlerbaumanalyse für den Ausfall des Sifa-Systems dar.

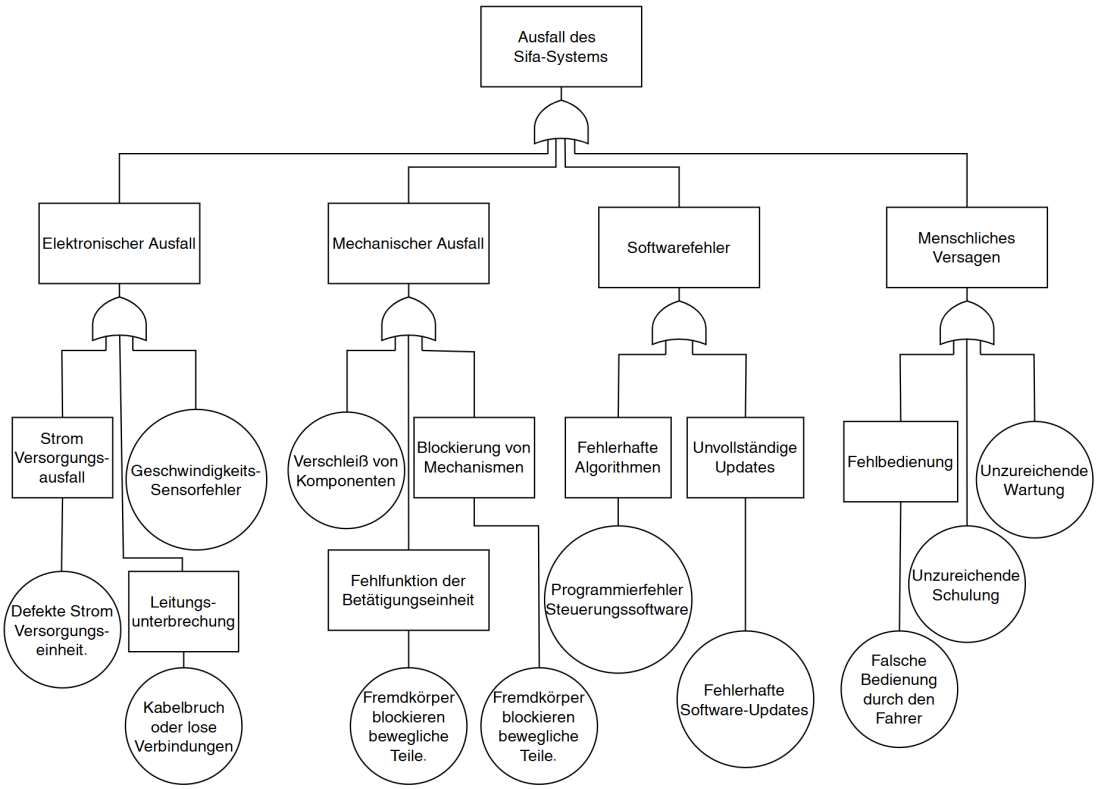


Abbildung 3.2: Sifa-Fehlerbaumanalyse (FTA)

Wie in der Abbildung 3.2 zu sehen ist, identifiziert die Fehlerbaumanalyse (FTA) des Sifa-Systems den Systemausfall als Top-Ereignis, das durch ein ODER-Gatter mit vier Hauptursachen verbunden ist: elektronischer Ausfall, mechanischer Ausfall, Softwarefehler und menschliches Versagen. Der elektronische Ausfall umfasst Stromversorgungsausfall, Leitungsunterbrechung und Geschwindigkeitssensorfehler. Der mechanische Ausfall wird durch Verschleiß von Komponenten, Fehlfunktion der Betätigungseinheit und Blockierung von Mechanismen verursacht. Softwarefehler resultieren aus fehlerhaften Algorithmen und unvollständigen Updates. Menschliches Versagen umfasst Fehlbedienung des Drucktasters, unzureichende Schulung und unzureichende Wartung. Diese Analyse bietet eine Übersicht über die potenziellen Ursachen und unterstützt die Entwicklung gezielter Maßnahmen zur Risikominderung.

3.4.3 Sicherheitsbezogene Anwendungsbedingungen

In den sicherheitsbezogenen Anwendungsbedingungen (SRAC) müssen die Regeln, Bedingungen und Einschränkungen festgelegt werden, die für die funktionale Sicherheit des Sifa-Systems relevant sind und bei dessen Anwendung beachtet werden müssen [6].

SRAC für Betrieb, Instandhaltung und Sicherheitsüberwachung:
In der folgenden Tabelle 3.16 werden die sicherheitsbezogenen Anwendungsbedingungen für Betrieb, Instandhaltung und Sicherheitsüberwachung aufgeführt [6].

Tabelle 3.16: SRAC für Betrieb, Instandhaltung und Sicherheitsüberwachung [6]

Thema	**Vorgeschlagene Maßnahme**
Identifikation der Betriebsanforderungen	Das Sifa-System muss bei Temperaturen zwischen $-25°$ C und $+55°$ C betrieben werden [6] & [70].
Sicherheitsprotokolle	Vor jedem Betriebsbeginn muss ein Systemcheck durchgeführt werden, um sicherzustellen, dass alle Komponenten ordnungsgemäß funktionieren.
Wartungspläne	Das Sifa-System sollte alle sechs Monate einer vollständigen Inspektion unterzogen werden, einschließlich der Überprüfung der elektronischen Komponenten und der Software-Updates.
Schulung des Personals	Wartungstechniker müssen an einem jährlichen Schulungsprogramm teilnehmen, das die neuesten Wartungstechniken und Sicherheitsvorschriften abdeckt.
Ersatzteilmanagement	Ein Lagerbestand an kritischen Ersatzteilen, wie z.B. Sensoren und Steuerplatinen, muss jederzeit verfügbar sein, um bei einem Ausfall schnell reagieren zu können.
Berichterstattung und Dokumentation	Alle Vorfälle und Wartungsarbeiten müssen in einem zentralen System dokumentiert werden, um eine lückenlose Nachverfolgung zu gewährleisten.
Notfallmaßnahmen	Im Falle eines Systemausfalls muss ein Notfallplan aktiviert werden, der die sofortige Benachrichtigung des Wartungsteams und die Umleitung des Zugverkehrs umfasst.
Audit und Inspektionen	Jährliche Audits durch eine externe Prüfstelle sollten durchgeführt werden, um die Einhaltung der Sicherheitsstandards zu überprüfen und Verbesserungspotenziale zu identifizieren.
Feedback-Mechanismen	Ein digitales Feedback-Formular sollte für das Betriebspersonal bereitgestellt werden, um Probleme oder Verbesserungsvorschläge direkt an das Wartungsteam zu übermitteln.

SRAC für Stilllegung und Entsorgung:
In der folgenden Tabelle 3.17 werden die sicherheitsbezogenen Anwendungsbedingungen für die Stilllegung und Entsorgung dargestellt.

Tabelle 3.17: SRACs für Stilllegung und Entsorgung [6]

Thema	**Vorgeschlagene Maßnahme**
Identifikation der Komponenten	Es sollen alle Teile des Sifa-Systems erfasst werden, die entsorgt werden müssen, einschließlich elektronischer, mechanischer und softwarebasierter Komponenten.
Regulatorische Anforderungen	Es müssen die gesetzlichen Vorschriften und Normen, die für die Entsorgung von sicherheitsrelevanten Systemen gelten erfasst werden, um sicherzustellen, dass alle rechtlichen Anforderungen erfüllt werden.
Risikoanalyse	Es sollen die potenziellen Risiken bewertet werden, die mit der Stilllegung und Entsorgung verbunden sind, wie z.B. Umweltauswirkungen, Sicherheitsrisiken für das Personal und mögliche Datenverluste.
Sicherheitsmaßnahmen	Es sollen Maßnahmen zur Risikominderung entwickelt werden, wie z.B. sichere Demontageverfahren, Schulung des Personals und geeignete Entsorgungsmethoden für gefährliche Materialien.
Dokumentation	Es sollen eine umfassende Dokumentation des Stilllegungs- und Entsorgungsprozesses erstellt werden, einschließlich der durchgeführten Risikoanalysen und der umgesetzten Sicherheitsmaßnahmen.
Überwachung und Kontrolle	Es soll ein System zur Überwachung des Stilllegungsprozesses implementiert werden, um sicherzustellen, dass alle Schritte gemäß den festgelegten Sicherheitsanforderungen durchgeführt werden.
Notfallpläne	Es sollen Notfallpläne für den Fall unvorhergesehener Ereignisse während der Stilllegung und Entsorgung entwickelt werden, um schnell und effektiv reagieren zu können.

Die sicherheitsbezogenen Anwendungsbedingungen (SRAC) für Betrieb, Instandhaltung und Sicherheitsüberwachung sowie die SRAC für Stilllegung und Entsorgung sind dem Unterkapitel 5.2 im Zusammenhang mit dem Qualitätsmanagementprozess der Norm DIN EN 50129 [6] entnommen. In den Tabellen 3.16 und 3.17 werden relevante Themen vorgestellt und beispielhaft Maßnahmen vorgeschlagen, die veranschaulichen sollen, wie solche Maßnahmen beschrieben sein könnten.

4 Design und Konstruktion

In diesem Kapitel wird der Entwurf der Sicherheitsfahrschaltung detailliert behandelt, beginnend mit dem Hardware-Design, das die Auswahl und Konfiguration der Komponenten umfasst. Es folgt das Software-Design, das die Entwicklung der notwendigen Steuerungslogik und Algorithmen beinhaltet. Die Simulation des Systems ermöglicht es, das Verhalten der Schaltung unter verschiedenen Bedingungen zu testen und frühzeitig Fehler zu identifizieren. Abschließend wird die Verifizierung der Sicherheitsanforderungen beschrieben, um sicherzustellen, dass das System alle relevanten Sicherheitsstandards erfüllt. Dieses Kapitel bietet einen umfassenden Überblick über die technischen und sicherheitstechnischen Aspekte des Schaltungsentwurfs.

4.1 Hardware-Design

In diesem Unterkapitel wird das Hardware-Design der Sicherheitsfahrschaltung, welches eine zentrale Rolle für die Funktionalität und Zuverlässigkeit des gesamten Systems spielt, vorgestellt. Das Hardware-Design gliedert sich in zwei wesentliche Bereiche: Zum einen die Auswahl der Komponenten mittels einer Marktrecherche für das Sifa-System, der Eingangs-, Ausgangs- und Überwachungsschnittstelle und zum anderen der Erstellung des Schaltplans.

4.1.1 Marktrecherche und Komponentenauswahl - Sifa System

Dieses Unterkapitel behandelt die Marktrecherche und Auswahl der elektronischen Komponenten für das Hardware-Design des Sifa-Systems. Ziel ist es, eine Auswahl der Bauteile zu treffen, die für die Entwicklung und Funktionalität des Systems entscheidend sind. Im Fokus stehen die Analyse und Bewertung von Mikrocontrollern, Komponenten für die galvanische Trennung, Schaltern, Tastern, Relais, LEDs und einem Buzzer. Diese Komponenten sind essenziell, um die geforderten Leistungsmerkmale und Sicherheitsstandards zu erfüllen. Die Auswahl basiert auf den Kriterien der Norm DIN EN 50129 [6], die sicherstellen, dass die Komponenten die Zuverlässigkeit und Funktionalität des Systems gewährleisten.

Mikrocontroller:

Für die Implementierung der Sicherheitsfahrschaltung ist der Einsatz einer Mikrocontroller-Platine erforderlich. Die Anforderungsanalyse gemäß TSI [17] und UIC 641 [18] beschreibt bzw. spezifiziert nicht, welcher Mikrocontroller zu verwenden ist. In der folgenden Tabelle 4.1 sind die auf dem Markt verfügbaren Mikrocontroller dargestellt.

Tabelle 4.1: Marktrecherche - Mikrocontroller

Board	Prozessor	Takt	Speicher	Merkmal	Preis
Arduino UNO R3 [23]	ATMega328P	16 MHz	16 kB ISP Flash / 512 B EEPROM / 512 B SRAM	I/O 20 Digital, P für Energiespar-modi	20,99 € [19]
Arduino Nano [24]	ATMega328	16 MHz	32 kB Flash / 1 kB EEPROM / 2 kB SRAM	I/O 20 Digital	25,70 € [20]
Raspberry Pi [25]	ARM Cortex-A72 CPU	1,5 GHz	2 GB RAM	I/O 40 pin GPIO	54,99 € [21]
ESP32 [26]	ESP32-WROVER-IE	240 MHz	512 kB RAM / Dual Core	I/O 17 Digital	20,99 € [22]

Obwohl die Sifa selbst nur eine begrenzte Anzahl von I/O-Anschlüssen benötigt, erfordert die umfassende Überwachung des Systems eine Mikrocontroller-Platine, die ausreichend I/O-Anschlüsse bereitstellt. Diese Anschlüsse sind notwendig, um alle relevanten Signale und Zustände zu erfassen sowie ein LCD-Display zu integrieren, der der Anzeige von Systeminformationen dient. Die Anzeige ermöglicht es die richtige Funktion bzw. den aktuellen Zustand des Systems zu verifizieren. Es werden die Mikrocontroller Arduino UNO R3 und Arduino Nano eingesetzt. Obwohl diese nicht die Anforderungen des Sicherheitsintegritätslevel SIL-3 erfüllen, eignen sie sich aus verschiedenen Gründen zur Prototypentwicklung. Dazu zählen

ihre Einfachheit und Benutzerfreundlichkeit, die Unterstützung durch eine große Community sowie umfangreiche Open-Source-Ressourcen. Zudem ermöglichen sie eine kosteneffiziente und schnelle Prototypentwicklung und sind mit einer Vielzahl von Sensoren und Aktuatoren kompatibel.

In der folgenden Abbildung 4.1 werden die Mikrocontroller-Platinen Arduino Nano (links) und Arduino UNO R3 (rechts) dargestellt.

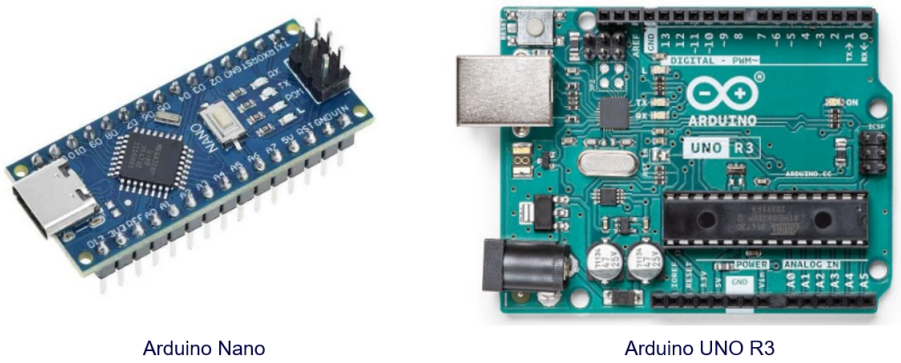


Abbildung 4.1: Mikrocontroller- Arduino Nano [24] und Arduino UNO R3 [23]

Komponenten für die galvanische Trennung:

Im Rahmen einer Marktrecherche wird eine geeignete Lösung zur galvanischen Trennung zwischen den beiden Mikrocontrollern ermittelt. Abhängig von den spezifischen Anforderungen und dem Anwendungsfall stehen verschiedene Komponenten zur Verfügung. Es gibt mehrere Lösungen und Bauteile, die je nach Anwendungsfall und Anforderungen ausgewählt werden können.

In der folgenden Tabelle 4.2 werden die verschiedenen Bauteile bzw. Technologien dargestellt, die auf dem Markt verfügbar sind.

Tabelle 4.2: Marktrecherche - Galvanische Trennung

Komponent	**Empfehlung**	**Vorteile**	**Nachteile**	**Preis**
Optokoppler [29]	Einfache digitale Signale und Anwendungen, Datenrate nicht extrem hoch.	Kostengünstig, einfach zu implementieren, weit verbreitet.	Begrenzte Datenrate und Lebensdauer, insbesondere bei hohen Frequenzen.	0,15€ [34] bis 12,90€ [35]
Digital Isolator [30]	Höhere Datenraten oder wenn kompaktere Lösung erforderlich.	Höhere Datenraten, kompakte Bauweise, gute Leistung.	In der Regel teurer als Optokoppler.	2,99€ [36]
Isolierte DC-DC-Wandler [[31]& [38]]	Signale und Isolierung Stromversorgung.	Signal und Stromversorgungsisolation.	Größer und teurer, hauptsächlich für Stromversorgungsanwendungen.	1,99€ [37]
Transformator (Übertrager) [32]	Analoge Signale oder spezielle Anwendungen.	Effektiv für analoge Signale und Stromversorgung.	Nicht geeignet für digitale Hochgeschwindigkeitssignale.	5,65€ [39]
Relais [33]	Für hohe Spannungen oder Ströme und niedrige Schaltfrequenz.	Hohe Spannungs- und Stromkapazität, vollständige Isolation und Robustheit	Langsame Schaltgeschwindigkeit, Größe, Stromverbrauch	3,45€ [40]

Dabei ist sicherzustellen, dass die gewählte Lösung den Systemanforderungen entspricht. Für die galvanische Trennung wird ein Optokoppler eingesetzt, da dieser eine elektrische Isolation zwischen Ein- und Ausgangsschaltkreisen gewährleistet, was ihn geeignet zur Vermeidung von Erdschleifen und zur Sicherstellung der Signalreinheit macht.

Optokoppler sind in der Regel kleiner und leichter als Relais [33] oder Übertrager, weshalb sie sich für platzbeschränkte Anwendungen eignen. Zudem sind sie energieeffizienter als Relais, da sie keine Spulen haben, die kontinuierlich mit Strom versorgt werden müssen. Da Optokoppler keine beweglichen Teile haben, sind sie in der Regel zuverlässiger und haben eine längere Lebensdauer als mechanische Relais. Sie sind einfach in der Schaltung zu implementieren und erfordern keine komplexen Schaltungsdesigns, wie es bei DC-DC-Wandlern [31] oder Übertragern der Fall sein könnte. Während DC-DC-Wandler und Übertrager primär zur Leistungsübertragung genutzt werden, dient der Optokoppler speziell der Signaltrennung.

Relais hingegen eignen sich für Anwendungen, die eine physische Trennung und höhere Stromkapazitäten erfordern [29]. Auf Basis der durchgeführten Marktrecherche wurde der Optokoppler als optimale Lösung ausgewählt. Die folgende Abbildung 4.2 zeigt den gewählten Optokoppler.

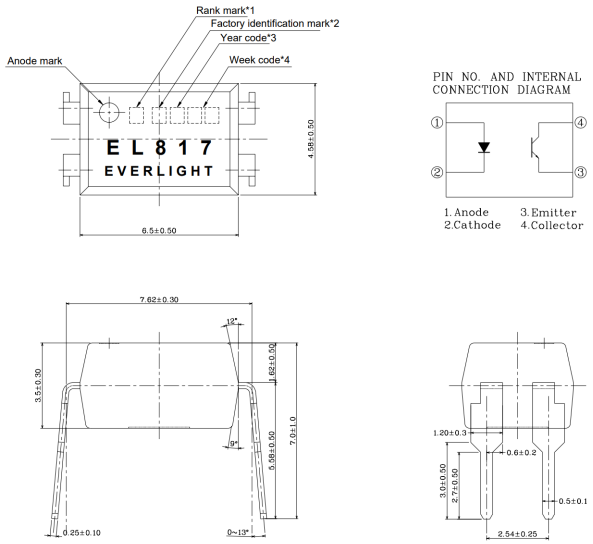


Abbildung 4.2: Optokoppler [34]

Die Leuchtdiode (LED) an der Eingangsseite des Optokopplers sollte mit einem Widerstand von $380\,\Omega$ betrieben werden, da die LED laut Datenblatt [80] eine Vorwärtsspannung von $1{,}2\,\mathrm{V}$ hat und ein sicherer Betriebsstrom von $10\,\mathrm{mA}$ empfohlen wird. Die Signale des Arduino-Mikrocontrollers liefern $5\,\mathrm{V}$. Für den Vorwiderstand wird daher ein $390\,\Omega$ Widerstand aus der E12-Reihe verwendet. Für die Pull-Up- bzw. Pull-Down-Ausgänge wird ein Widerstand von $10\,\mathrm{k}\Omega$ verwendet.

4.1.2 Marktrecherche und Komponentenauswahl - Eingangsschnittstelle

In diesem Unterabschnitt werden die Sensoren und Aktoren behandelt, die als wesentliche Komponenten in der Sicherheitsfahrschaltung fungieren. Sensoren sind für die kontinuierliche Erfassung von Betriebszuständen und Umgebungsdaten verantwortlich, was für die präzise Steuerung und Überwachung des Systems unerlässlich ist. Aktoren setzen die durch Sensoren erfassten Daten und die Verarbeitungsergebnisse des Mikrocontrollers in physische Aktionen um.

Schalter für die Sifa Aktivierung und die Mindestgeschwindigkeit:

Für die ordnungsgemäße Funktion der Sicherheitsfahrschaltung sind zwei spezifische Schalter erforderlich. Der erste Schalter dient der Aktivierung der Sifa, indem er sicherstellt, dass das System in den Betriebsmodus wechselt, sobald die Bedingungen für die Überwachung der Triebfahrzeugführeraktivität erfüllt sind. Der zweite Schalter dient der Überwachung der Mindestgeschwindigkeit. Diese beiden Schalter sind entscheidend, um die Sicherheit und Zuverlässigkeit des Systems zu gewährleisten, indem sie sicherstellen, dass die Sifa nur unter den vorgesehenen Betriebsbedingungen aktiv ist. In der folgenden Tabelle 4.3 sind die Alternativen für die Schalter dargestellt.

Tabelle 4.3: Marktrecherche - Schalter

Name	**Marke**	**Informationen**	**Preis**
Kippschalter 2x Ein-Ein [41]	Reichelt Elektronik	20 V/0, 4 VA	4,90 € [42]
Mini Kippschalter [43]	Taiss	125 V 6 A EIN/EIN 6 Terminals 2 Position DPDT	1,00 € [43]
Kippschalter [44]	Mouser Electronics E-Switch	5 A28 VDC	2,86 € [45]

Da alle zweikanaligen Kippschalter ähnliche Eigenschaften aufweisen und alle drei für den Rapid-Prototyping-Prozess geeignet sind, wurde aus wirtschaftlichen Gründen der Mini-Kippschalter des Herstellers Taiss [43] ausgewählt.

Drücktaster für Sifa:

Die Drücktaste für die Sicherheitsfahrschaltung ist ein zentrales Bedienelement, das die kontinuierliche Aufmerksamkeit des Triebfahrzeugführers sicherstellt. Sie muss regelmäßig betätigt werden, um dem System zu signalisieren, dass der Fahrer aktiv und aufmerksam ist. Diese Taste sollte ergonomisch gestaltet und leicht zugänglich sein, um eine intuitive Bedienung zu ermöglichen. Für die Eingangsschnittstelle wird ein Taster verwendet, da er für die Sifa geeignet und einfach zu bedienen ist. Andere technische Lösungen, wie ein Pedal, wären ebenfalls möglich, sind jedoch schwieriger im Rapid-Prototyping umzusetzen.

In der folgenden Tabelle 4.4 sind die Alternativen für den Drucktaster dargestellt.

Tabelle 4.4: Marktrecherche - Drucktaster

Name	**Marke**	**Informationen**	**Preis**
Drucktaster 2 Pol [46]	Apem - Reichelt Elektronik	$4\,\mathrm{A} - 30\,\mathrm{VDC}$, 2x (Ein), Printstifte; Lebensdauert: 30000 Zyklen; Arbeitstemperatur: $-40°$ C- $+85°$ C	8,20 € [47]
Druckschalter 2 pol [48]	Cliff Switches	Rating:AC $125\,\mathrm{V}$ $4\,\mathrm{A}$, $250\,\mathrm{V}$ $2\,\mathrm{A}$, Lebensdauert: 50000 Zyklen; Arbeitstemperatur: $-20°$ C- $+65°$ C	5,40 € [49]
Geschützter Drucktaster [50]	TRU Components	$250\,\mathrm{V/AC}$ $3\,\mathrm{A}$ 2x Ein/(Ein) tastend Lebensdauert: 50000 Zyklen; Arbeitstemperatur: $-20°$ C- $+70°$ C	16,12 € [51]

Für diese Arbeit wurde der zweipolige Drucktaster der Marke Apem, Serie 8442 (siehe Datenblatt [46]), ausgewählt. Der Taster erfüllt alle in der Anforderungsanalyse festgelegten Eigenschaften. Zudem entspricht die Ein-(Ein)-Logik der gewählten Serie der Logik der Sifa was den Anforderungen der TSI [17] und UIC 641 [18] entspricht. Außerdem hat der gewählte Drucktaster eine elektrische Lebensdauer von 30.000 Zyklen. Zudem hat dieser einen Betriebstemperaturbereich von $-40°$ C bis $+85°$ C, was die Anforderungen an die Sicherheitsintegrität bezüglich der Umweltbedingungen für das System in einem Temperaturbereich T3 im Fahrzeugabteil gemäß der Norm DIN EN 50125 [70] erfüllt. In der folgenden der Abbildung 4.3 wird der Drucktaster für die Sifa dargestellt.

Abbildung 4.3: Drucktaster Apem Serie 8442 Ein - (Ein) [46]

4.1.3 Marktrecherche und Komponentenauswahl - Ausgangsschnittstelle

Relais:

Relais sind elektromechanische Schalter, die es ermöglichen, mit einem kleinen Steuersignal einen größeren Laststromkreis zu steuern. Sie werden häufig in verschiedenen elektronischen und elektromechanischen Systemen eingesetzt, um Geräte zu steuern, die höhere Spannungen oder Ströme benötigen. In der folgenden Tabelle 4.5 werden die Alternativen für das Relais dargestellt.

Tabelle 4.5: Marktrecherche - Relais

Name	Marke	Informationen	Preis
Relais KY-019RM [53]	Joy-It	50 V AC/28 V 5 A DC	3,80 € [54]
KF-301 1-Relais [55]	AZ-Delivery	50 V AC/30 V 5 A DC	5,99 € [56]
Two-pole Relais G5V-2 [57]	Omrom Electronics	5 VDC /2 A	4,15 € [58]

Bei der Auswahl eines geeigneten Relais für das System fiel die Entscheidung auf das kosteneffizienteste Modell. Ausschlaggebend hierfür war, dass alle geprüften Relais die spezifizierten Anforderungen an Spannung und Leistung gemäß der Systemdefinition vollständig erfüllen. Durch die Wahl einer wirtschaftlichen Lösung werden die Kosten optimiert, ohne die Funktionalität oder Zuverlässigkeit des Systems zu beeinträchtigen. Die folgende Abbildung 4.4 zeigt das verwendete Relais.

Abbildung 4.4: Relais KY-019RM JOY-IT [54]

LEDs:

LEDs, oder Leuchtdioden, sind energieeffiziente Lichtquellen, die sich durch Langlebigkeit und geringen Energieverbrauch auszeichnen. Sie sind in verschiedenen Farben und Helligkeiten verfügbar, was sie für eine Vielzahl von Anwendungen geeignet macht. In der folgenden Tabelle 4.6 werden die Alternativen für die LEDs dargestellt.

Tabelle 4.6: Marktrecherche - LEDs

Name	Marke	Informationen	Preis
LED bedrahtet [59]	Kingbright	$5\,\mathrm{mm},\ 2,10\,\mathrm{V},\ 2\,\mathrm{mA}$	0,14 € [60]
Oval LED [61]	Cree LED	$5\,\mathrm{mm},\ 2,10\,\mathrm{V},\ 20\,\mathrm{mA}$	0,19 € [62]

Da beide Optionen vergleichbare Eigenschaften aufweisen und LEDs als allgemein verfügbare Standardbauteile gelten, wurde aus wirtschaftlichen Gründen die kostengünstigste Variante gewählt. Die LEDs übernehmen keine sicherheitskritische Funktion in der Schaltung. Das System ist in der Lage potenzielle Defekte zu erkennen und entsprechend darauf zu reagieren.

Buzzer:

Der Buzzer, der einen Dauerton erzeugt, ist ein wesentliches Warnsignal in der Sicherheitsfahrschaltung. Er wird aktiviert, um den Triebfahrzeugführer auf eine ausbleibende Reaktion oder Inaktivität aufmerksam zu machen. Der durchdringende Ton dient als letzte Aufforderung zur Handlung, bevor das System eine automatische Zwangsbremsung einleitet. Diese akustische Warnung trägt maßgeblich zur Sicherheit im Zugbetrieb bei, indem sie potenzielle Gefahren durch Unaufmerksamkeit reduziert. In der folgenden Tabelle 4.7 sind zwei Alternativen für den Buzzer dargestellt.

Tabelle 4.7: Marktrecherche - Buzzer

Name	Marke	Informationen	Preis
Buzzer [63]	CUI Devices	$85\,\mathrm{dB},\ 2300\,\mathrm{Hz},\ 5\,\mathrm{V}$	1,40 € [64]
Miniatur Summer Geräusch-Entwicklung [65]	TRU Components	$85\,\mathrm{dB}$ Spannung: $5\,\mathrm{V/DC}$	0,93 € [66]

Es wird die kostengünstigste Version des Miniatur-Summers aus der Geräusch-Entwicklungsreihe [65] ausgewählt.

4.1.4 Komponentenauswahl - Überwachungsschnittstelle

Die Überwachungsschnittstelle für die Entwicklung des Sifa-Systems ist nicht Bestandteil der Anforderungsanalyse gemäß TSI [17] und UIC 641 [18]. Dennoch werden bestimmte Komponenten eingesetzt, um die Korrektheit sowohl der Software als auch der Hardware während der Verifizierung zu überwachen. Zur Bestätigung aller Funktionalitäten wird auf einem LCD-Bildschirm der aktuelle Zustand der Software angezeigt. Für die Wahl der Komponenten ist es, anders als für die Hauptteile, nicht notwendig eine Marktrecherche durchzuführen.

LCD Display:

Das LCD-Display 1602A ist ein Anzeigemodul, das über 16 Zeichen und 2 Zeilen verfügt, auf denen Textinformationen dargestellt werden können. Dieses Display eignet sich für Projekte, bei denen Informationen wie Sensordaten, Menüs oder andere Statusmeldungen anzeigt werden sollen. In der folgenden Abbildung 4.5 wird das LCD-Display 1602A dargestellt.

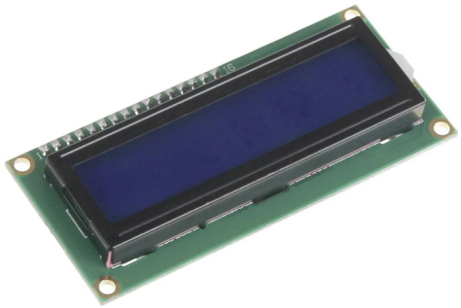


Abbildung 4.5: LCD-Display 1602A [68]

Potentiometer:

Der Zweck des Drehpotentiometers besteht darin, den Kontrast des LCD-Displays zu regulieren. Es wird der Dreh-Potentiometer 1-Gang Mono $0.200\,\mathrm{W}$, $50\,\mathrm{k\Omega}$ verwendet. Das Datenblatt dieses Bauteiles ist im Dokument [69] zu sehen.

4.1.5 Schaltplan

Nach der Auswahl der Komponenten wird der Schaltplan entwickelt, der detailliert die Verdrahtung und Anordnung der Komponenten aufzeigt. Dieser Plan ist essenziell für den Aufbau und die spätere Fehlersuche im System.

Auswahl der Software für die Entwicklung von Leiterplatten:

Bei der Auswahl einer CAD-/PCB-Entwurfssoftware für das Sifa-System spielen Kosten und Funktionalität eine zentrale Rolle. EAGLE ist ein etabliertes Tool und bietet bietet umfangreiche Funktionen, ist jedoch mit 500 Euro pro Jahr kostenintensiv und damit außerhalb des Budgets dieses Projektes [74]. KiCad hingegen ist eine kostenlose Open-Source-Software, die alle relevanten Funktionen für den Leiterplattenentwurf abdeckt. Es umfasst die Stromlaufplan-Verwaltung, das PCB-Routing und die 3D-Modellerstellung. Diese Funktionen decken alle Anforderungen für das Sifa-System ab [74]. DesignSpark, eine weitere elektronische CAO-Software, bietet keine direkte Unterstützung für den PCB-Entwurf und ist daher für dieses Projekt weniger geeignet [74]. Aufgrund der umfassenden Funktionen und der Kostenfreiheit wurde KiCad für das Projekt gewählt. Beim Schaltungsdesign werden die Systemgrenzen und Schnittstellen aus Kapitel 3.3.2 berücksichtigt. Es entstehen drei Zeichnungen: für die Eingangs- und Ausgangsschnittstellen sowie das Sifa-System selbst.

Schaltplan Eingangsschnittstelle:

In der folgenden Tabelle 4.8 wird die Signalliste der Eingangsschnittstelle dargestellt.

Tabelle 4.8: Signalliste der Eingangsschnittstelle

Bauteil	Signalname	In/Out	Erklärung	Signalstatus
SW1	push1a und push2a	Output	Signal des Drucktasters zu SW4 und SW5	LOW/NC
SW2	sifa_Aktiv1 und sifa_Aktiv2	Output	Signal des Schalters für die Aktivierung der Sifa	LOW/NC
SW3	geschwindigkeit1 und geschwindigkeit2	Output	Signal der Schnittstelle der Mindestgeschwindigkeit	LOW/NC
SW4 & SW5	push1 und push2	Output	Signale zum Mikrocontroller 1 und 2	LOW/NC
J1	Terminals	Input	Spannungsversorgung VVC1, VCC2 und VCC3	5 V

In der folgenden Abbildung 4.6 wird der Schaltplan für die Eingangsschnittstelle dargestellt.

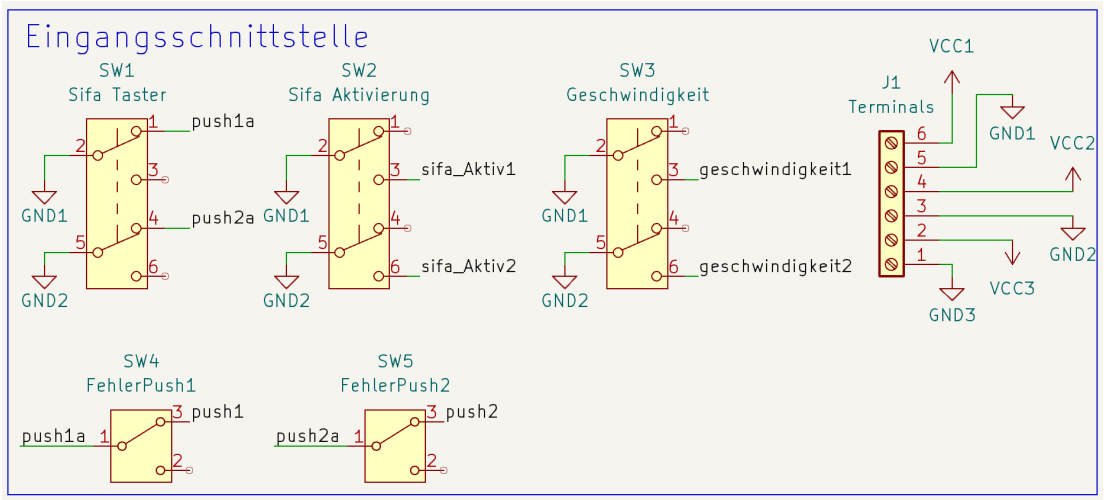


Abbildung 4.6: Schaltplan Eingangsschnittstelle

Die Eingangsschnittstelle umfasst sechs wesentliche Bauteile, die in der folgenden Liste erläutert werden:

- Taster 1 (SW1): Doppelkanaliger Taster zur Erfassung der Aktivität des Triebfahrzeugführers.
- Schalter 1 (SW2): Zur Aktivierung der Sifa.
- Schalter 2 (SW3): Zur Bestätigung, dass eine Geschwindigkeit von $20\,\mathrm{km/h}$ erreicht wurde [18].
- Schalter 3 (SW4): Zur Simulation eines Fehlers im Sifa-Drucktaster bzw. in der Leitung des Kanals 1 (push1).
- Schalter 4 (SW5): Zur Simulation eines Fehlers im Sifa-Drucktaster bzw. in der Leitung des Kanals 2 (push2).
- Terminals (J1): Fungieren als Eingänge für die Spannungsquellen.

Sowohl der Taster SW1 als auch der Schalter SW2 werden direkt vom Triebfahrzeugführer bedient. Der Schalter SW3 simuliert ein Signal vom Teilsystem zur Überwachung der Mindestgeschwindigkeit der Lokomotive. Die Schalter SW4 und SW5 dienen der gezielten Simulation von Leitungs- oder Sifa-Drucktasterfehlern zu Schulungs- und Demonstrationszwecken.

Schaltplan Sifa-System:

In der folgenden Tabelle 4.9 wird die Signalliste des Sifa-Systems dargestellt.

Tabelle 4.9: Signalliste des Sifa-Systems

Anschluss	Signalname	In/Out	Erklärung	Signalstatus
D13-UNO	notbremse_1a	Output	Notbremsesignal des Mikrocontrollers zu Schalter SW8	LOW/HIGH
D12-UNO	notbremse2_ Ueberwachung	Input	Überwachung des Notbremssignals	LOW/HIGH
D11-UNO	push1	Input	Signal 1 vom Sifa Taster	LOW/NC
D10-UNO	push2_ Ueberwachung	Input	Überwachung Signal 2 vom Sifa Taster	LOW/HIGH
D9-UNO	tonMelder_1	Output	Tonmelder Signal zu Relais Speaker 1	LOW/HIGH
D8-UNO	lichtMelder_1	Output	Lichtmelder 1 zu Relais Licht 1	LOW/HIGH
D7-UNO	fehlerMelder_1	Output	Fehlermelder 1 zu Relais Fehler 1	LOW/HIGH
D6-UNO	sifa_Aktiv1	Input	Sifa ist aktiv 1	LOW/NC
D5-UNO	geschwindigkeit1	Input	Geschwindigkeit von x km/h erreicht	LOW/NC
D13-NANO	notbremse_2a	Output	Notbremsesignal des Mikrocontrollers zu Schalter SW9	LOW/HIGH
D12-NANO	notbremse1_ Ueberwachung	Input	Überwachung des Notbremssignals	LOW/HIGH
D11-NANO	push2	Input	Signal 2 vom Sifa Taster	LOW/NC
D10-NANO	push1_ Ueberwachung	Input	Überwachung Signal 1 vom Sifa Taster	LOW/HIGH
D9-NANO	tonMelder_2	Output	Ton Melder Signal zu Relais Speaker 2	LOW/HIGH
D8-NANO	lichtMelder_2	Output	LichtMelder 2 zu Relais Licht 2	LOW/HIGH
D7-NANO	fehlerMelder_2	Output	Fehlermelder 2 zu Relais Fehler 2	LOW/HIGH
D6-NANO	sifa_Aktiv2	Input	Sifa ist aktiv 2	LOW/NC
D5-NANO	geschwindigkeit2	Input	Geschwindigkeit von x km/h erreicht	LOW/NC

In der folgenden Abbildung 4.7 wird der Schaltplan für die Sifa Schnittstelle dargestellt.

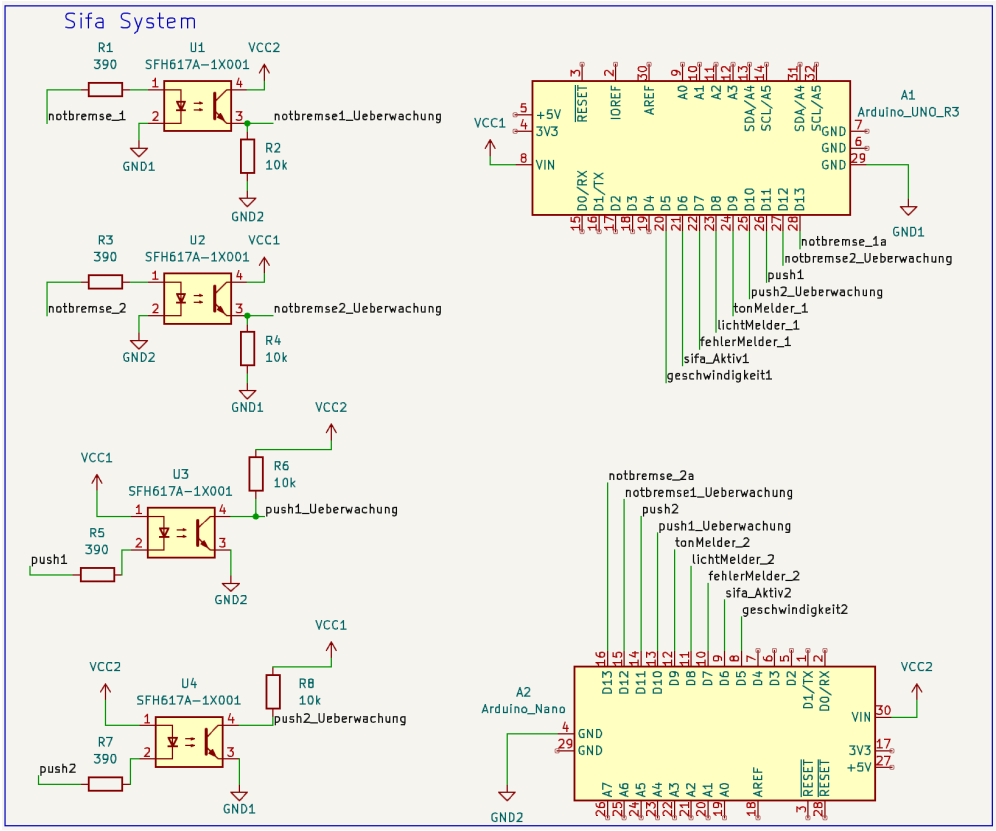


Abbildung 4.7: Schaltplan Sifa-System

Das Sifa-System verwendet zwei Mikrocontroller zur Gewährleistung der Systemredundanz sowie vier Optokoppler zur galvanischen Trennung. Die zentralen Komponenten sind:

- Optokoppler (U1-U4): Gewährleisten die galvanische Trennung zwischen den beiden Systemen. Es ist zu beachten, dass die Trennung zwischen den Notbremssignalen (Optokoppler U1 und U2) und deren Überwachungssignalen eine Pull-Down-Schaltung verwendet, während für den Sifa-Drucktaster (Optokoppler U3 und U4) eine Pull-Up-Konfiguration implementiert ist.
- Arduino UNO R3: Mikrocontroller-Plattform, die als Steuerungseinheit dient und die Verarbeitung der Eingangssignale übernimmt.
- Arduino Nano: Kompakte Mikrocontroller-Plattform, die zur Systemredundanz beiträgt und ausreichend Leistung für die Steuerungsaufgaben bietet.

Schaltplan Ausgangsschnittstelle:

Die Ausgangsschnittstelle verfügt über insgesamt vier Ausgangssignale. Das wichtigste Signal für die Sicherheit ist das Notbremssignal, das durch eine LED simuliert wird. In der folgenden Tabelle 4.10 wird die Signalliste der Ausgangsschnittstelle dargestellt.

Tabelle 4.10: Signalliste der Ausgangsschnittstelle

Anschluss	Signalname	In/Out	Erklärung	Signalstatus
K1 Relay Speaker 1	tonMelder_1	Input	Signal vom Ton Melder des ersten Mikrocontrollers	LOW/HIGH
K1 Relay Speaker 2	tonMelder_2	Input	Signal vom Ton Melder des zweiten Mikrocontrollers	LOW/HIGH
LS1 Speaker	Signal VCC	Input	Relay K1 Speaker 1 UND Relay K2 Speaker 2	5 V
K3 Relay Licht 1	lichtMelder_1	Input	Signal vom Licht Melder des ersten Mikrocontrollers	LOW/HIGH
K4 Relay Licht 2	lichtMelder_2	Input	Signal vom Licht Melder des zweiten Mikrocontrollers	LOW/HIGH
D1 LED LichtMelder	Signal VCC	Input	Relay K3 Licht 1 UND Relay K4 Licht 2	5 V
K5 Relay Notbremse 1	notbremse_1	Input	Notbremssignal des Arduino UNO Mikrocontrollers zu Relay, aus Schalter SW8.	LOW/HIGH
K6 Relay Notbremse 2	notbremse_2	Input	Notbremssignal des Arduino Nano Mikrocontrollers zu Relay, aus Schalter SW9.	LOW/HIGH
D2 LED Notbremse	Signal VCC	Input	Relay K5 Notbremse 1 UND Relay K6 Notbremse 2	5 V
K7 Relay Fehler 1	fehlerMelder_1	Input	Signal vom Fehler Melder des ersten Mikrocontrollers	LOW/HIGH
K8 Relay Fehler 2	fehlerMelder_2	Input	Signal vom Fehler Melder des zweiten Mikrocontrollers	LOW/HIGH
D3 LED Fehler	Signal VCC	Input	Relay K7 Fehler 1 UND Relay K8 Fehler 2	5 V

In der folgenden Abbildung 4.8 wird der Schaltplan für die Ausgangsschnittstelle dargestellt.

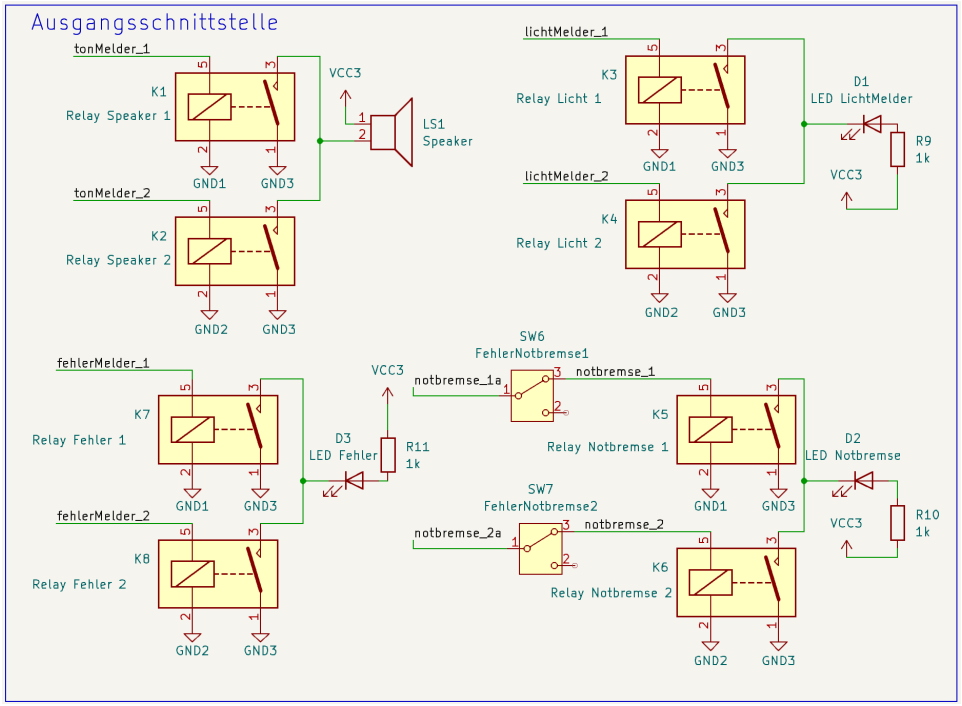


Abbildung 4.8: Schaltplan Ausgangsschnittstelle

Die Komponenten werden in der folgenden Liste erläutert:

- LS1: Tonmelder.
- D1: Weiße LED für den Lichtmelder.
- D2: Rote LED für das Notbremssignal.
- D3: Gelbe LED für den Fehlermelder.
- K1-K18: Relais für die elektrische Isolation des Sifa-Systems.
- Schalter 5 und 6 (SW6-SW7): Zur Simulation eines Fehlers im Notbremssignal des Arduino UNO bzw. Nano.

Alle Ausgänge der Mikrocontroller sind mit den Relais verbunden und parallel geschaltet, um die Redundanz des Systems zu berücksichtigen. Durch die Parallelschaltung bleibt das Sifa-System auch bei einem Ausfall eines der Kanäle funktionsfähig.

4.2 Software-Design

In diesem Abschnitt wird das Software-Design der Sicherheitsfahrschaltung detailliert beschrieben, wobei der Fokus auf der Implementierung als Zustandsautomat liegt, wie in Unterkapitel 3.3.4 „Anforderungen an den Entwurf der Software“ definiert. Im ersten Teil wird ein Zustandsdiagramm (UML) präsentiert, das die Übergänge zwischen den definierten Zuständen visualisiert, und die Logik hinter den Zustandswechseln verdeutlicht. Der zweite Teil definiert die verschiedenen Zustände, die das System durchlaufen kann, um die Funktionalität und Sicherheit zu gewährleisten. Im dritten Teil wird die Arduino-Programmierung vorgestellt, wobei die wichtigsten Codeabschnitte hervorgehoben werden, um die praktische Umsetzung des Zustandsautomaten zu veranschaulichen.

4.2.1 UML-Zustandsautomat

Das UML-Diagramm des Zustandsautomaten bietet eine visuelle Darstellung der verschiedenen Betriebszustände der Sicherheitsfahrschaltung. Es dient als Werkzeug, um die Logik und das Verhalten des Systems zu modellieren, indem es die Bedingungen und Ereignisse aufzeigt, die einen Zustandswechsel auslösen. In der folgenden Abbildung 4.9 wird das UML-Diagramm des Zustandsautomaten dargestellt.

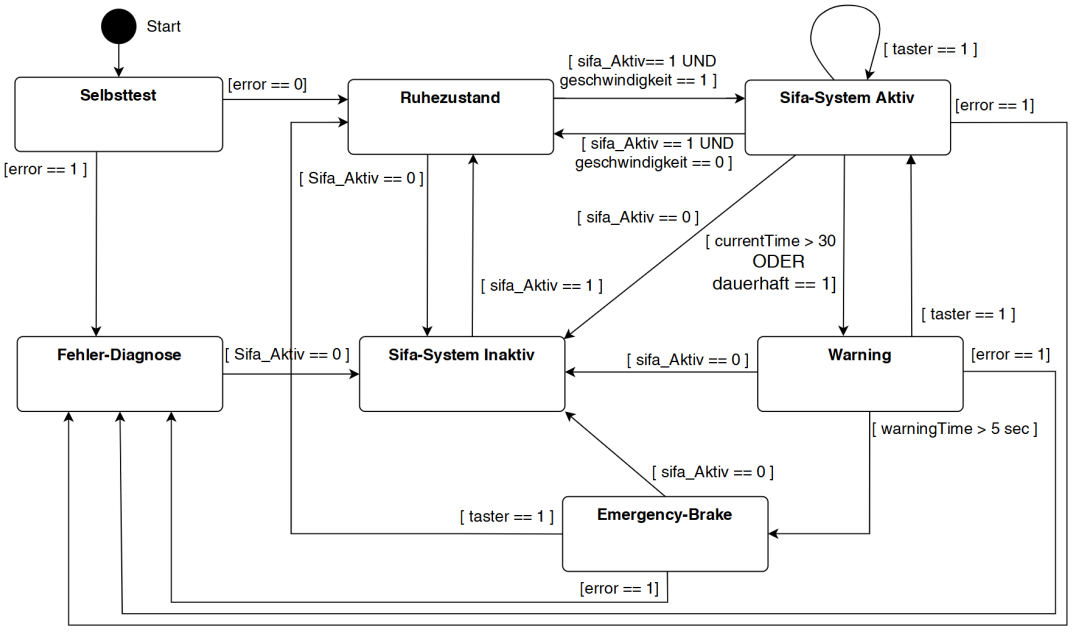


Abbildung 4.9: UML-Diagramm des Zustandsautomats

4.2.2 Definition der Zustände

Zur Definition der Zustände ist die Tabelle 3.14, die die funktionalen Anforderungen detailliert beschreibt, zu berücksichtigen.

Selbsttest-Zustand:

Ein automatischer Selbsttest für eine Sicherheitsfahrschaltung (Sifa) stellt sicher, dass alle wesentlichen Komponenten und Funktionen ordnungsgemäß arbeiten, bevor das System in den Normalbetrieb übergeht.

- Taster-Test: Überprüft wird, ob der Drucktaster ordnungsgemäß funktioniert, indem sein Zustand gelesen und sichergestellt wird, dass dieser auf Betätigung reagiert. Der Benutzer soll den Sifa-Taster einmal manuell loslassen. Wenn die Signale push1 und push2 erkannt werden, kann der Test fortgesetzt werden. Andernfalls wird „error“ auf 1 gesetzt und der Zustand wechselt in den „Fehlerdiagnose“-Zustand.
- LED- und Buzzer-Test: Zur Sicherstellung ihrer Funktionalität werden alle LEDs nacheinander ein- und ausgeschaltet. Die Signale tonMelder_1 und tonMelder_2 sowie lichtMelder_1 und lichtMelder_2 werden von den Mikrocontrollern für eine Sekunde aktiviert und anschließend deaktiviert. Diese Signalgebung ermöglicht eine klare visuelle und akustische Wahrnehmung durch den Triebfahrzeugführer.
- Fehlererkennung des Notbremssignals: Überprüft, ob alle Notbremssignale (notbremse_1 und notbremse_2 mit notbremse1_Ueberwachung und notbremse2_Ueberwachung) erfolgreich gesendet wurden. Zunächst sendet Mikrocontroller 1 (UNO) das Signal notbremse_1, während Mikrocontroller 2 (Nano) mit notbremse1_Ueberwachung dessen Empfang bestätigt. Anschließend sendet Mikrocontroller 2 (Nano) das Signal notbremse_2, das wiederum von Mikrocontroller 1 (UNO) durch notbremse2_Ueberwachung bestätigt wird. Schlägt der Test fehl, wechselt das System in einen sicheren Zustand („error“ wird auf 1 gesetzt und der Zustand wechselt in „Fehlerdiagnose“). Gleichzeitig wird die Fehlerausgabe (fehlerMelder_1 und fehlerMelder_2) aktiviert.

Ruhezustand:

Nach erfolgreichem Selbsttest wechselt die Sifa in den „Ruhezustand“. In diesem Zustand darf der Ausgang für das Notbremssignal nicht aktiviert sein. Alle Sifa-Ausgänge müssen deaktiviert bleiben. Sind Ruhezustand und sifa_Aktiv deaktiviert, wechselt sie in den Zustand „Sifa-System Inaktiv“. Sind im Ruhezustand sifa_Aktiv und Geschwindigkeit aktiviert, erfolgt ein Wechsel in den Zustand „Sifa-System Aktiv“.

Sifa-System Aktiv-Zustand:

Im Zustand „Sifa-System Aktiv“ wird die Wachsamkeit des Triebfahrzeugführers überwacht, sobald „geschwindigkeit” und „sifa_Aktiv” == LOW (aktivert) sind und sich das System nicht mehr im Ruhezustand befindet. Hierbei wird der Druckaster (Loslassen) überwacht. Wenn der Taster auf GND (push1/push2) losgelassen wird, setzt sich der Timer zurück. Erfolgt innerhalb von 30 Sekunden keine Betätigung des Tasters oder wird dieser länger als 2,5 Sekunden losgelassen, wechselt der Zustand zu „Warning“. Parallel dazu erfolgt eine Fehlerprüfung: Wenn die Überwachungen von push1 und push2 nicht übereinstimmen, d.h. push1 sollte gleich push1_überwachung und push2 gleich push2_überwachung sein, wird „error“ gesetzt und der Zustand wechselt zu „Fehlerdiagnose“. Jeder Mikrocontroller überwacht, was der andere als Tastereingang erhält. In diesem Zustand kann es vorkommen, dass das Signal „sifa_Aktiv“ inaktiv wird, woraufhin sofort in den Zustand „Sifa-System Inaktiv“ gewechselt wird. Die Sifa wechselt in den Ruhezustand, sobald der aktuelle Zustand „Sifa-System Aktiv“ ist und die Geschwindigkeit unter den festgelegten Schwellenwert fällt.

Sifa-System Inaktiv-Zustand:

Die Sifa wechselt in den Zustand „Inaktiv“, sobald sie sich entweder im „Ruhezustand“, im Zustand „Sifa-System Aktiv“ oder „Warning“ befindet und eine externe Deaktivierung (sifa_Aktiv != GND) erkannt wird. Wenn das System sich im Zustand „Sifa-System Inaktiv“ befindet und das Signal sifa_Aktiv wieder aktiviert wird, wechselt es in den „Ruhezustand“.

Warning-Zustand:

Die Sifa wechselt in den Zustand „Warning“, sobald sie sich im Zustand „Sifa-System Aktiv“ befindet und das Wachsamkeitssignal vom externen Drucktaster ausbleibt (d.h., der Taster von push1 und push2 wird nicht innerhalb von 30 Sekunden kurz losgelassen). In diesem Zustand wird ein optisches Signal (lichtMelder_1 und lichtMelder_2) für 2,5 Sekunden (warningTime) angezeigt. Erfolgt keine Reaktion, verbleibt das System im Zustand „Warning“ und ein zusätzliches akustisches Signal (tonMelder_1 und tonMelder_2) wird für weitere 2,5 Sekunden ausgelöst. Überschreitet die warningTime 5 Sekunden, wechselt der Zustand zu „Emergency-Brake“. Befindet sich das System im Zustand „Warning“ und sifa_Aktiv wird deaktiviert, wechselt es in den Zustand „Sifa-System Inaktiv“. Parallel dazu wird der Taster auf Fehler überwacht. Wenn die Überwachungen von push1 und push2 nicht übereinstimmen, d.h. push1 sollte gleich push1_überwachung und push2 gleich push2_überwachung sein, wird „error“ gesetzt und der Zustand wechselt zu „Fehlerdiagnose“. Jeder Mikrocontroller überwacht, was der andere als Tastereingang erhält.

Emergency-Brake-Zustand:

Die Sifa wechselt in den Zustand „Emergency-Brake“, sobald sie sich im Zustand „Warning“ befindet und das Wachsamkeitssignal vom externen Taster weiterhin ausbleibt (warningTime überschreitet 5 Sekunden). In diesem Zustand wird das Notbremssignal (notbremse_1 und notbremse_2) aktiviert. Wird der Sifa-Drucktaster auf GND gesetzt (push1 und push2 werden kurz losgelassen), wechselt das System in den Ruhezustand und die Notbremssignale (notbremse_1 und notbremse_2) werden deaktiviert. Parallel dazu sollen in diesem Zustand (Emergency-Breke) auch Fehler erkannt werden. Fehler können in der Überwachung von push1 und push2 oder in der Überwachung von notbremse_1 und notbremse_2 auftreten. Wird ein Fehler erkannt, wird „error“ gesetzt und der Zustand wechselt zu „Fehlerdiagnose“. Befindet sich das System im Zustand „Emergency-Brake“ und sifa_Aktiv wird deaktiviert, wechselt es in den Zustand „Sifa-System Inaktiv“.

Fehlerdiagnose-Zustand:

Die Sifa-Funktion muss über die Fähigkeit zur Fehlerdiagnose verfügen und die entsprechenden Informationen an den Systemgrenzen bereitstellen. Das System muss in der Lage sein, sowohl Hardware- als auch Softwarefehler zu erkennen. Dabei werden die Reaktion des Sifa-Drucktasters und das Notbremssignal überwacht. Fehler können in der Überwachung von push1 und push2 oder in der Überwachung von notbremse_1 und notbremse_2 auftreten. In diesem Zustand sollen fehlerMelder_1 (UNO) und fehlerMelder_2 (NANO) aktiviert sein. Wenn das Signal sifa_Aktiv deaktiviert wird, wechselt das System in den „Sifa-System Inaktiv-Zustand“ und „error“ wird zurückgesetzt.

4.2.3 Arduino-Programmierung

In diesem Unterkapitel wird ein Teil des Codes des Zustandsautomaten für die Sicherheitsfahrschaltung präsentiert, der die wichtigsten Betriebszustände steuert und so die zuverlässige und sichere Funktionalität gewährleistet. Der vollständige Code, der die Implementierung der Zustandsübergänge sowie die Logik zur Überwachung der Triebfahrzeugführeraktivität und zur Auslösung von Warn- und Notbremssignalen zeigt, wird in Anhang B präsentiert.

Struktur des Codes:

Die folgende Tabelle 4.11 stellt den ersten Teil der Codestruktur samt zugehöriger Erklärungen vor. Die vollständigen Listings sind in den aufgeführten Kapitelnummern zu finden.

Tabelle 4.11: Struktur des Codes - Teil 1

Listing	**Erklärung**
Pin-Definitionen (10.1)	Die Pins sind für die Steuerung und Überwachung des Notbremssignals, des Sifa-Tasters sowie der Ton- und Lichtsignale zuständig. Zusätzlich wird die Konfiguration für ein LCD-Display definiert, um Systeminformationen anzuzeigen.
Zeit-Konstanten und Variablen (10.2)	Die Zeitkonstanten legen die Dauer für verschiedene Systemzustände fest, darunter die maximale Inaktivitätszeit von 30 Sekunden sowie die 5 Sekunden für LED- und Tonsignale, gemäß UIC 641 [18].
Definition der Zustände (10.3)	Mithilfe eines *enum* werden die verschiedenen Systemzustände festgelegt, darunter selbsttestZustand, ruheZustand, sifaAktivZustand, sifaInaktivZustand, warningZustand, emergencyBrakeZustand und fehlerDiagnoseZustand.
Definition Fehlerverfolgung (10.4)	Die Variablen für die Fehlerverfolgung der Sicherheitsfahrschaltung sind definiert.
Setup (10.5)	Hier werden die Pin-Modi für Eingänge eingestellt. Die Ausgänge werden als OUTPUT definiert und initial auf LOW gesetzt, um sicherzustellen, dass alle Signale zu Beginn deaktiviert sind.
Hauptprogramm (10.6)	Der loop-Code verwendet eine switch-Anweisung, um den aktuellen Zustand des Systems zu überprüfen und die entsprechende Funktion auszuführen, wie „performSelfTest()"für den Selbsttest oder „handleWarningZustand()" für den Warnzustand. Jede Funktion behandelt die spezifischen Anforderungen und Aktionen des jeweiligen Zustands. Am Ende jeder Schleife wird das LCD-Display mit „updateLCD()" aktualisiert, um den aktuellen Systemstatus anzuzeigen.
Taste Entprellung (10.7)	Es wurde eine Funktion entwickelt, die für die Entprellung des Sifa-Drucktaster zuständig ist.

In der folgenden Tabelle 4.12 wird der zweite Teil der Struktur des Codes mit Erklärungen dargestellt.

Tabelle 4.12: Struktur des Codes - Teil 2

Listing	**Erklärung**
Notbremssignal Entprellung (10.8)	Um die Ungenauigkeit bei der Synchronisierung des Notbremssignals der beiden Mikrocontroller auszugleichen, wird diese Funktion berücksichtigt.
Selbsttest-Zustand (10.9)	Die Funktion „performSelfTest()" führt einen Selbsttest für ein System mit Tastern, LEDs, einem Buzzer und einem Notbremssignal durch.
Ruhezustand (10.10)	Die Funktion „handleRuheZustand()" überwacht den Zustand des Sifa-Systems im Ruhezustand.
Sifa-System Aktiv-Zustand (10.11)	Die Funktion „handleSifaAktivZustand()" verwaltet den Zustand des Systems, wenn die Sicherheitsfahrschaltung aktiv ist.
Sifa-System Inaktiv-Zustand (10.12)	Die Funktion „handleSifaInaktivZustand()" überwacht den Zustand des Systems, wenn die Sicherheitsfahrschaltung inaktiv ist.
Warning-Zustand (10.13)	Die Funktion „handleWarningZustand()" verwaltet das System, wenn es sich im Warning-Zustand befindet.
Emergency-Brake-Zustand (10.14)	Die Funktion „handleEmergencyBrakeZustand()" steuert das System, wenn es sich im Emergency-Brake-Zustand befindet.
Fehlerdiagnose-Zustand (10.15)	Die Funktion „handleFehlerDiagnoseZustand()" verwaltet das System, wenn es sich im Fehlerdiagnosezustand befindet.
Funktion Dauerhaft (10.16)	Die Funktion „dauerhaft()" überwacht, ob der Sifa-Druckaster länger als 2,5 Sekunden lossgelassen wird.
Funktion LCD Aktualisierung (10.17)	Die Funktion „updateLCD()" aktualisiert die Anzeige auf einem LCD-Bildschirm basierend auf dem aktuellen Zustand des Systems.

Zur Sicherstellung der korrekten Funktion des doppelkanaligen Sifa-Systems wurden Funktionen entwickelt, die die funktionale Sicherheit gewährleisten und die Vorgaben der Norm DIN EN 50129 [6] umsetzen. Dazu gehören Funktionen zur Entprellung des Sifa-Drucktasters und des Notbremssignals, der Selbsttest-Zustand mit der Funktion „performSelfTest()", der Fehlerdiagnose-Zustand mit der Funktion „handleFehlerDiagnoseZustand()" sowie die Funktion „dauerhaft", die die korrekte Bedienung des Sifa-Drucktasters durch den Triebfahrzeugführer überwacht. Die Funktion „dauerhaft()" wird im folgenden Listing 4.1 vorgestellt. Alle anderen Listings befinden sich in Anhang B.

Funktion zur Erkennung des dauerhaften Drückens des Sifa-Tasters:

Die Funktion „dauerhaft()" überwacht, ob ein Taster (push1) gedrückt gehalten wird. Sie liest den Tasterzustand und prüft, ob er gedrückt ist (LOW). Wenn der Taster gerade neu gedrückt wurde, wird der Zustand „isButtonPressed" auf „true" gesetzt und die aktuelle Zeit gespeichert. Wenn der Taster länger als 2,5 Sekunden gedrückt gehalten wird, wechselt das System in den warningZustand und die Warnzeit wird gespeichert. Sobald der Taster losgelassen wird, wird der Zustand „isButtonPressed" zurückgesetzt. In dem folgenden Listing wird die Funktion zur Erkennung des dauerhaften Drückens des Sifa-Tasters dargestellt.

```
1  void dauerhaft() {
2    int buttonState = digitalRead(push1); // Liest den Zustand des
       Tasters
3
4    if (buttonState == LOW) { // Ueberprueft, ob der Taster gedrueckt
       ist
5      if (!isButtonPressed) { // Wenn der Taster gerade neu gedrueckt
         wurde
6        isButtonPressed = true; // Setzt den Zustand auf "gedrueckt"
7        buttonPressTime = millis(); // Speichert die aktuelle Zeit
8      } else {
9        if (millis() - buttonPressTime > 2500 ) { // Ueberprueft, ob
           der Taster laenger als 2,5 Sekunden gedrueckt ist
10         currentState = warningZustand;
11         warningStartTime = millis();
12        // startSifaAktiv == false;
13       }
14     }
15   } else {
16     isButtonPressed = false; // Setzt den Zustand zurueck, wenn der
         Taster losgelassen wird
17   }
18 }
```

Listing 4.1: Funktion Dauerhaft

Die Funktion wurde entwickelt, um mögliche menschliche Fehler, wie in diesem Fall das dauerhafte Drücken des Sifa-Tasters durch den Triebfahrzeugführer zu vermeiden, wie es in der Norm DIN EN 50129 [6] für SIL-3- und SIL-4-Systeme empfohlen wird.

4.3 Simulation des Systems

In diesem Abschnitt wird die Verifizierung der Hardware und der Software durchgeführt. Zunächst wird ein Simulationswerkzeug gewählt, um die Hardware und Software zu verifizieren.

4.3.1 Auswahl des Simulationswerkzeuges

Vor dem Übergang zum Prototyping des Systems ist es entscheidend, die Hardware und Software umfassend zu simulieren, um potenzielle Fehler und Schwachstellen frühzeitig zu identifizieren und zu beheben, was Zeit und Kosten spart. Es ermöglicht eine Optimierung des Designs und stellt sicher, dass das System den in Unterkapitel 3.3.3 dargestellten Anforderungen entspricht, bevor physische Ressourcen investiert werden. Dadurch wird das Risiko von teuren Nachbesserungen im späteren Entwicklungsprozess minimiert. Die Auswahl eines geeigneten Simulationswerkzeuges spielt dabei eine zentrale Rolle. Die folgende Tabelle 4.13 zeigt die verschiedenen Simulationswerkzeuge, die laut Dinale [12] auf dem Markt verfügbar sind.

Tabelle 4.13: Simulationswerkzeuge für Arduino

Name	**Entwickelt von**	**Open Source**	**Besonderheiten**	**Preis**
Microsoft MakeCode	Microsoft	Nein	Testen verschiedener virtueller Komponenten, einsteigerfreundlich	Kostenlos
Tinkercad Circuits	Autodesk	Nein	Platinen und Schaltpläne können für die Herstellung der Leiterplatte exportiert werden	Kostenlos
Wokwi	Uri Shaked	Ja	Webbasiert, Benutzerfreundlich, geeignet für Fortgeschrittene und Experten.	Kostenlos
PICSimLab	Luis Claudio Gamboa Lopes	Ja	Die Simulationen können integrierte Shape Based Autoroutings als Standard enthalten.	Kostenlos
Proteus VSM	Labcenter Electronics	Nein	Den Simulationen können Abschirmungen hinzugefügt werden.	ab 200 €

Nach sorgfältiger Abwägung der verfügbaren Simulationswerkzeuge, wie in Tabelle 4.13 dargestellt, wurde Wokwi als das bevorzugte Werkzeug für die Simulation der Hardware und Software des Systems ausgewählt. Wokwi bietet eine benutzerfreundliche Oberfläche und unterstützt eine Vielzahl von Arduino-Mikrocontrollern, was es geeignet für die Anforderungen

des Projektes macht. Ein weiterer entscheidender Faktor ist, dass Wokwi als Open-Source-Tool kostenlos verfügbar ist, was es zu einer kosteneffizienten Lösung macht. Die Kombination aus einfacher Bedienbarkeit und umfassender Funktionalität ermöglicht es, realistische Simulationen durchzuführen und verschiedene Szenarien effektiv zu testen, bevor das System in die Prototyping-Phase übergeht.

Die folgende Abbildung 4.10 zeigt links den verwendeten Code in Arduino und rechts die Hardware-Simulation für einen Mikrocontroller.

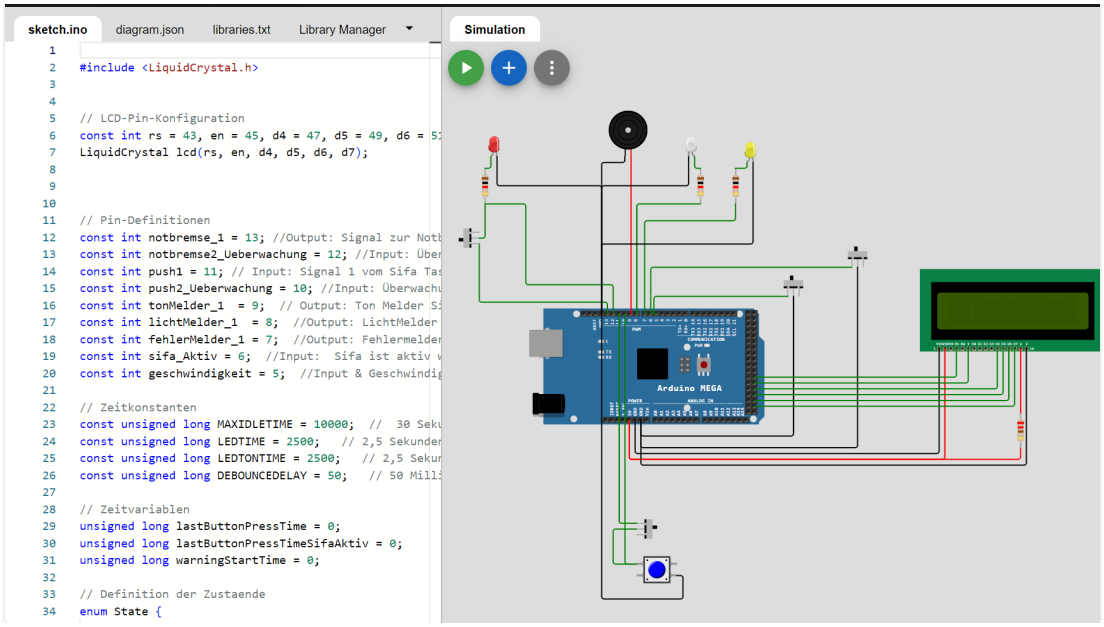


Abbildung 4.10: Simulationswerkzeug

Das digitale Werkzeug ermöglicht es nur einen Mikrocontroller zur Zeit zu überprüfen. Aus diesem Grund wird der Mikrocontroller sich selbstständig überwachen und Fehlersituationen mit Hilfe von Switches simulieren.

4.3.2 Hardware Verifizierung

Im Abschnitt zur Hardware-Verifizierung wird eine Tabelle präsentiert, die die überprüften Komponenten detailliert auflistet. Die Verifizierung stellt sicher, dass alle Hardware-Elemente den erforderlichen Spezifikationen der Datenblätter entsprechen und zuverlässig funktionieren. Die Tabelle 4.14 bietet einen Überblick über die getesteten Komponenten und die Ergebnisse der Überprüfung. Ist das Ergebnis in Ordnung, wird es mit i.O. gekennzeichnet.

Tabelle 4.14: Hardware Verifizierung

Test	Komponente	Testverfahren	Ergebnis
1	Mikrocontroller Arduino UNO	Überprüfung jedes Mikrocontroller-Pins durch Test mit einem LED-Blink-Sketch.	i.O.
2	Mikrocontroller Arduino Nano	Überprüfung jedes Mikrocontroller-Pins durch Test mit einem LED-Blink-Sketch.	i.O.
3	Optokoppler	Der Optokoppler wird getestet, indem die LED-Seite aktiviert und das Ausgangssignal überprüft wird.	i.O.
4	Schalter Sifa Aktivierung/-Mindestgesch.	Der Schalter wird getestet, indem er betätigt und das Ausgangssignal überprüft wird.	i.O.
5	Relais	Das Relais wird getestet, indem es aktiviert und das Schalten des Ausgangskreises überprüft wird.	i.O.
6	LEDs	Die LED wird getestet, indem bei Stromversorgung ein Aufleuchten erfolgt.	i.O.
7	Buzzer / Dauerton	Der Buzzer wird getestet, indem bei Stromversorgung der Dauerton ertönt.	i.O.
8	LCD Display	Das LCD-Display wird getestet, indem es mit einem Mikrocontroller verbunden und ein einfaches „Hello World“ - Programm angezeigt wird.	i.O.
9	Potentiometer	Das Potentiometer wird getestet, indem es an einen Mikrocontroller angeschlossen und die variierende Spannungsausgabe gemessen wird, während der Knopf gedreht wird.	i.O.

Alle Bauteile haben die Testverfahren erfolgreich abgeschlossen. Jede Komponente wurde auf Funktionalität und Übereinstimmung mit den festgelegten Spezifikationen überprüft. Die Ergebnisse bestätigen, dass alle Bauteile den Anforderungen entsprechen und für den Einsatz im System geeignet sind. Die erfolgreiche Verifizierung gewährleistet die zuverlässige Funktion der Hardware und bildet die Grundlage für die nächste Projektphase.

4.3.3 Software Verifizierung

Zur Verifizierung des Designs, der Zustände, der funktionalen Anforderungen und der Sicherheitsfunktionen werden in diesem Abschnitt Simulationen durchgeführt. Die Verifizierung stellt sicher, dass die Software den festgelegten Spezifikationen entspricht und zuverlässig arbeitet. Die Anforderungen an den Entwurf der Software sind in Unterkapitel 3.3.4 beschrieben. Zur Verifizierung der Software im Selbsttest-Zustand wird das Programm mithilfe eines LCD-Bildschirms im Selbsttest-Zustand gehalten und geprüft, ob die in Kapitel 3 beschriebenen Anforderungen korrekt umgesetzt wurden. In der folgenden Tabelle 4.15 wird die Softwareverifizierung des Selbsttest-Zustands dargestellt.

Tabelle 4.15: Softwareverifizierung des Selbsttest-Zustands

Test	Testverfahren	Ergebnis
1	Taster-Test: Überprüfung der Funktion des Sifa-Drucktasters durch Lesen des Zustandes und Sicherstellung, dass dieser auf Betätigung reagiert. Der Test ist erfolgreich, wenn der Taster von beiden Mikrocontrollern erkannt wird.	i.O.
2	LED- und Buzzer-Test: Überprüfung der Funktionalität durch ein- und ausschalten der Sifa-LED und des Buzzers. Der Test ist bei Aufleuchten der LED und der Erzeugung eines Geräusches durch den Buzzer erfolgreich.	i.O.
3	Fehlererkennung des Notbremssignals: Es ist eine Fehlererkennung implementiert, die überprüft, ob alle Notbremssignale gesendet worden sind. Der Test ist erfolgreich, wenn die rote LED leuchtet und keine Fehlermeldung durch die gelbe LED angezeigt wird.	i.O.
4	Fehler im Sifa-Drucktaster werden mithilfe eines Schalters zur Unterbrechung der Leitung simuliert. Der Test ist erfolgreich, wenn der simulierte Fehler erkannt wird und die gelbe LED leuchtet.	i.O.
5	Fehler des Notbremssiggnals werden mithilfe eines Schalters zur Unterbrechung der Leitung simuliert. Der Test ist erfolgreich, wenn der simulierte Fehler erkannt wird und die gelbe LED leuchtet.	i.O.
6	Ein korrekter Übergang in den Fehlerdiagnose-Zustand erfolgt, wenn ein simulierter Fehler auftritt.	i.O.
7	Ein korrekter Übergang in den Ruhezustand erfolgt, wenn kein Fehler auftritt.	i.O.

Zur Verifizierung der Software im Ruhezustand wird das Programm mithilfe des LCD-Bildschirms im Ruhezustand gehalten. Dabei wird überprüft, ob alle in Kapiteln 3 beschriebenen Anforderungen ordnungsgemäß erfüllt werden. In der folgenden Tabelle 4.16 wird die Softwareverifizierung des Ruhezustands dargestellt.

Tabelle 4.16: Softwareverifizierung des Ruhezustands

Test	Testverfahren	Ergebnis
1	Ein Übergang in den Sifa-System Aktiv-Zustand erfolgt, wenn die Signale sifa_Aktiv und Geschwindigkeit anliegen. Der Test ist erfolgreich, wenn beide Switches aktiviert werden und das Zustandsautomaten-Programm in den Sifa-System Aktiv-Zustand wechselt.	i.O.
2	Ein Übergang in den Sifa-System Inaktiv-Zustand erfolgt, wenn das Signal sifa_Aktiv ausgeschaltet ist. Der Test ist erfolgreich, wenn der Sifa-Aktiv-Switch deaktiviert wird und das Zustandsautomaten-Programm in den Sifa-System Inaktiv-Zustand wechselt. Eine Voraussetzung für diesen Test ist, dass der Switch für die Mindestgeschwindigkeit deaktiviert ist.	i.O.

In der folgenden Tabelle 4.17 wird die Softwareverifizierung des Sifa-System Aktiv-Zustands dargestellt.

Tabelle 4.17: Softwareverifizierung des Sifa-System Aktiv-Zustands

Test	Testverfahren	Ergebnis
1	Ein Übergang in den Ruhezustand erfolgt, wenn das Signal sifa_Aktiv anliegt, aber kein Mindestgeschwindigkeitssignal aktiv ist.	i.O.
2	Ein Übergang in den Sifa-System Inaktiv-Zustand erfolgt, wenn das Signal sifa_Aktiv ausgeschaltet ist.	i.O.
3	Ein Übergang in den Warning-Zustand erfolgt, wenn die Zeit seit dem letzten Loslassen der Druck-Taste mehr als 30 Sekunden beträgt.	i.O.
4	Ein Übergang in den Warning-Zustand erfolgt, wenn der Druck-Taster länger als 2,5 Sekunden losgelassen bleibt.	i.O.
5	Erkennung eines möglichen Fehlers im Druck-Taster: Erkennung des Fehlers und Übergang in den Fehlerdiagnose-Zustand.	i.O.
6	Zurücksetzen der Zeit auf Null, bei Beginn des Sifa-System Aktiv-Zustands.	i.O.
7	Zurücksetzen der Zeit auf Null, wenn der Taster kurzzeitig (weniger als 2,5 Sekunden) losgelassen wird.	i.O.

In der folgenden Tabelle 4.18 wird die Softwareverifizierung des Sifa-System Inaktiv-Zustands dargestellt.

Tabelle 4.18: Softwareverifizierung des Sifa-System Inaktiv-Zustands

Test	Testverfahren	Ergebnis
1	Ein Übergang in den Ruhezustand erfolgt, wenn das Signal sifa_Aktiv eingeschaltet ist. Der Test ist erfolgreich, wenn der Sifa_Aktiv-Switch aktiviert wird und der LCD-Bildschirm den Zustandswechsel anzeigt. Eine Voraussetzung für diesen Test ist, dass die Mindestgeschwindigkeit deaktiviert bleibt, damit der Zustand im Ruhezustand bleibt und nicht direkt in den Sifa-System Aktiv-Zustand wechselt.	i.O.
2	Der Zustand bleibt stabil, wenn der Schalter Sifa_Aktiv ausgeschaltet ist. In diesem Fall sollte das System keine unerwarteten Zustandsänderungen vornehmen und alle anderen Funktionen weiterhin arbeiten. Zudem ist sicherzustellen, dass keine Fehlermeldungen auftreten, solange der Schalter in dieser Position bleibt.	i.O.

In der folgenden Tabelle 4.19 wird die Softwareverifizierung des Warning-Zustands dargestellt.

Tabelle 4.19: Softwareverifizierung des Warning-Zustands

Test	Testverfahren	Ergebnis
1	Ein Übergang in den Sifa-System Inaktiv-Zustand erfolgt, wenn das Signal sifa_Aktiv nicht eingeschaltet ist.	i.O.
2	Ein Übergang in den Emergency-Brake-Zustand erfolgt, wenn die Warnzeit mehr als 5 Sekunden beträgt und der Druck-Taster nicht losgelassen wurde.	i.O.
3	Ein Übergang in den Sifa-System Aktiv-Zustand erfolgt, wenn der Sifa-Druck-Taster losgelassen wird.	i.O.
4	Ein Übergang in den Fehlerdiagnose-Zustand erfolgt, wenn ein simulierter Fehler im Taster erkannt wird.	i.O.
5	Warnsignale: Der Test ist erfolgreich, wenn die Ausgangssignale für Licht (2,5 Sekunden) und Licht-/ Tonmelder (2,5 Sekunden) aktiviert sind.	i.O.

In der folgenden Tabelle 4.20 wird die Softwareverifizierung des Emergency-Brake-Zustands dargestellt.

Tabelle 4.20: Softwareverifizierung des Emergency-Brake-Zustands

Test	Testverfahren	Ergebnis
1	Ein Übergang in den „Ruhezustand“ erfolgt, wenn der Taster losgelassen wird.	i.O.
2	Ein Übergang in den „Fehlerdiagnose“-Zustand erfolgt, wenn ein simulierter Fehler im Taster oder im Notbremssignal erkannt wird.	i.O.
3	Ein Übergang in den ’Sifa-System Inaktiv’-Zustand erfolgt, wenn eine externe Inaktivierung (sifa_Aktiv!= GND) erkannt wird.	i.O.
4	Das Notbremssignal ist korrekt aktiviert, wenn die rote LED leuchtet.	i.O.

In der folgenden Tabelle 4.21 wird die Softwareverifizierung des Fehler-Diagnose-Zustands dargestellt.

Tabelle 4.21: Softwareverifizierung des Fehler-Diagnose-Zustands

Test	Testverfahren	Ergebnis
1	Fehlersignal: Bei Simulation eines Fehlers wird das Fehlersignal korrekt angezeigt, wenn die gelbe LED leuchtet.	i.O.
2	Der Zustand kann den Ursprung eines simulierten Fehlers erkennen.	i.O.
3	Notbremssignal: Wenn das System in den Fehlerdiagnose-Zustand wechselt, wird das Notbremssignal aktiviert.	i.O.
4	Der Test ist erfolgreich wenn ein Übergang in den „Sifa-System Inaktiv“-Zustand erfolgt, wenn das Signal sifa_Aktiv deaktiviert ist.	i.O.

Anhand der Verifizierung kann festgestellt werden, dass die Funktionalität des Sifa-Systems den in der Anforderungsanalyse definierten Spezifikationen entspricht. Die Simulationstests basierten maßgeblich auf den Sicherheitsanforderungen aus Unterkapitel 3.2 sowie der Systemarchitekturspezifikation aus Unterkapitel 3.3, mit besonderem Fokus auf die Softwareentwurfsanforderungen in Unterkapitel 3.3.4. Da alle Funktionalitäten erfolgreich im Entwurf umgesetzt und simuliert wurden, kann nun die nächste Phase des Projekts, das Prototyping, eingeleitet werden.

5 Prototyping

Zur Veranschaulichung der Entwicklung und Optimierung des Systems, wird in diesem Kapitel der Prozess des Prototypings dargestellt. Der erste Abschnitt widmet sich dem Aufbau des Prototyps. Dort werden die grundlegende Struktur und die Implementierung der Komponenten beschrieben. Darauf folgt die Überprüfung der Funktionalität des Prototyps, bei der die einzelnen Funktionen getestet und auf ihre Leistungsfähigkeit hin bewertet werden. Im nächsten Abschnitt wird der Prototype unter Fehlerbedingungen getestet, um die Robustheit und Fehlertoleranz des Systems zu überprüfen. Abschließend erfolgt die Verifizierung der Sicherheitsanforderungen, um sicherzustellen, dass der Prototype alle relevanten Sicherheitsstandards erfüllt und zuverlässig arbeitet. Dieses Kapitel bietet einen detaillierten Einblick in die iterative Entwicklung und Verfeinerung des Systems.

5.1 Aufbau des Prototyps

In diesem Abschnitt wird der Aufbau des Systems detailliert beschrieben, beginnend mit der Entwicklung eines Rapid Prototyps. Dieser erste Schritt ermöglicht es, die grundlegende Funktionalität des Systems schnell zu testen und Anpassungen vorzunehmen. Im nächsten Schritt wird das System auf einer Leiterplatte mithilfe von KiCad, wie im Schaltplan des Unterkapitels 4.1.5 definiert, implementiert, um eine Lösung zu entwickeln, die für die physische Fertigung vorbereitet werden kann. Diese Fertigung liegt jedoch außerhalb des Umfangs dieser Arbeit.

5.1.1 Rapid Prototype

Alle Komponenten werden mit Hilfe eines Steckbretts zusammengebaut. Ein Taster führt zu den beiden Mikrocontrollern. Zur Gewährleistung einer Galvanischen Trennung, überwachen sich die beiden Mikrocontroller mit Hilfe von Optokopplern gegenseitig. Jeder Mikrocontroller erhält zwei Signale von zwei doppel kanaligen Schaltern: eines für die Mindestgeschwindigkeit und eines für die Aktivierung der Sifa. Jeder Mikrocontroller verfügt über vier Ausgänge: Lichtmelder, Tonmelder, Fehlermelder und Notbremssignal. Die Mikrocontroller überwachen,

ob ein Fehler im Taster oder beim Notbremssignal-Ausgang vorliegt. Alle Ausgänge sind parallel mit Relais geschaltet. Für den Rapid-Prototyping-Prozess wird eine Überwachungsschnittstelle mit einem LCD-Bildschirm in einen der Mikrocontroller integriert. Um die erforderliche Anzahl an Ausgängen bereitzustellen, wird der Arduino Nano durch einen Arduino Mega ersetzt. Diese zusätzliche Schnittstelle ermöglicht eine verbesserte Überprüfung der Systemfunktionen. Der Austausch des Arduino zur Anzeige auf einem LCD-Bildschirm hat keine relevante Auswirkung auf das Sifa-System. Der Code läuft auf beiden Arduinos identisch. Das fertige Sifa-System benötigt keinen LCD-Bildschirm. Der Austausch erfolgt lediglich aus akademischen Gründen für den Prototypentest.

Die folgende Abbildung 5.1 zeigt den Rapid-Prototype.

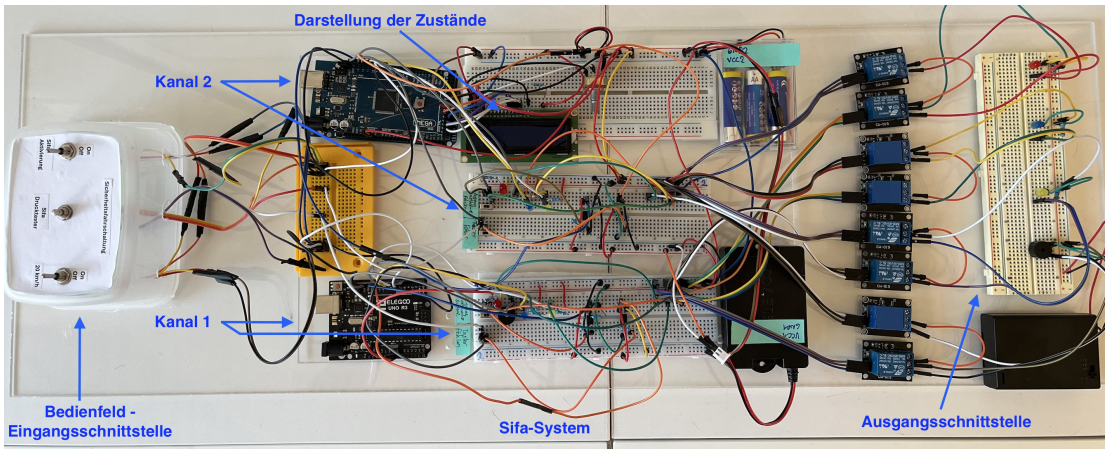


Abbildung 5.1: Rapid-Prototype

Nachdem sichergestellt wurde, dass alle Komponenten korrekt zusammengebaut sind, erfolgt die Überprüfung der Programmierung der Mikrocontroller. Anschließend ist zu prüfen, ob der Optokoppler die verschiedenen Signale korrekt überträgt. Mit der parallelen Anordnung aller Komponenten werden sämtliche Software- und Hardwaretests erneut durchgeführt, um sicherzustellen, dass alle Komponenten wie gefordert funktionieren. Bei vollständig erfüllten Anforderungen wird eine Leiterplatte entworfen. Diese Maßnahme verfolgt das Ziel, die Schaltung nicht nur professioneller zu gestalten, sondern auch den Einsatz von Kabeln zu reduzieren. Durch die Integration der Komponenten auf einer Leiterplatte wird zudem die Zuverlässigkeit und Wartungsfreundlichkeit des Systems verbessert.

5.1.2 Fertigung der Platine

Die Entwicklung wird im nächsten Schritt auf einer Platine umgesetzt. Die Schaltpläne, die in den Abbildungen 4.6, 4.7 und 4.8 dargestellt sind, dienen als Grundlage für das Platinenlayout. Zur Erstellung eines 3D-Modells der Platine wird das Software-Tool KiCAD verwendet. Auf der Platine sind alle Komponenten sowie deren Verbindungen integriert. Die folgende Abbildung 5.2 zeigt die fertiggestellte Platine.

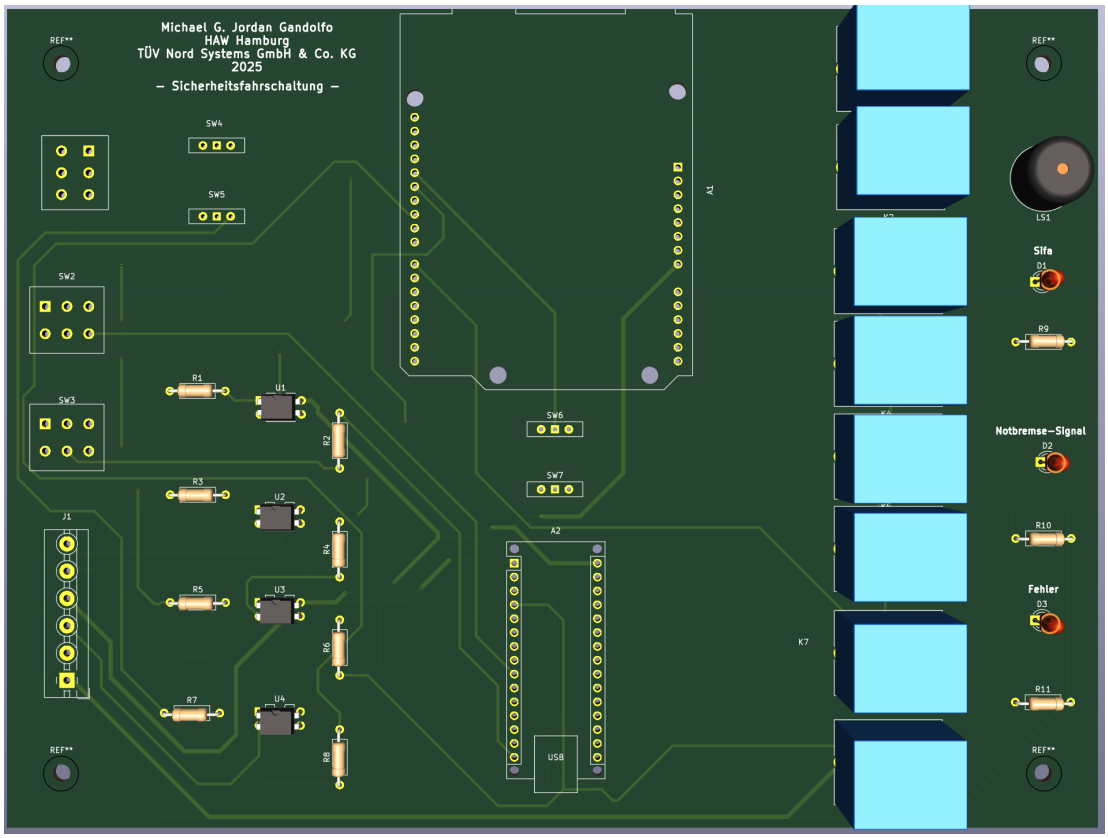


Abbildung 5.2: Sifa-Leiterplatte

Abbildung 5.2 zeigt auf der linken Seite die Eingangsschnittstelle mit dem Sifa-Taster und zwei Schaltern, in der Mitte das Sifa-System und auf der rechten Seite die Ausgangsschnittstelle mit den vier Ausgängen für das Notbremssignal, das Warnsignal, den Tonmelder und den Fehlermelder. Zusätzliche Zeichnungen sind im Anhang C zu finden.

5.2 Überprüfung der Funktionalität des Prototyps

Die Funktionalität des Prototyps wird durch eine Überprüfung der Software und Hardware sichergestellt, wobei beide korrekt und fehlerfrei arbeiten müssen. Für die Hardware werden alle Komponenten getestet, während für die Software alle definierten Zustände kontrolliert werden. Die Ergebnisse dieser Funktionsprüfung sind in Tabelle 5.1 dargestellt. Ist das Ergebnis in Ordnung, wird es mit i.O. gekennzeichnet.

Tabelle 5.1: Überprüfung der Funktionalität des Prototyps

Test	Beschreibung	Ergebnis
1	Software: Selbsttest-Zustand, laut Verifizierung Tabelle 4.15	i.O.
2	Software: Ruhezustand, laut Verifizierung Tabelle 4.16	i.O.
3	Software: Sifa-System Aktiv-Zustand, laut Verifizierung Tabelle 4.17	i.O.
4	Software: Sifa-System Inaktiv-Zustand, laut Verifizierung Tabelle 4.18	i.O.
5	Software: Warning-Zustand, laut Verifizierung Tabelle 4.19	i.O.
6	Software: Emergency-Brake-Zustand, laut Verifizierung Tabelle 4.20	i.O.
7	Software: Fehler-Diagnose-Zustand, laut Verifizierung Tabelle 4.21	i.O.
8	Hardware: Mikrocontroller - Der Test wurde wie in Tabelle 4.14 Hardware Verifizierung dargestellt durchgeführt.	i.O.
9	Hardware: Optokoppler - Der Test wurde wie in Tabelle 4.14 Hardware Verifizierung dargestellt durchgeführt.	i.O.
10	Hardware: Schalter - Sifa Aktivierung/Mindestgeschw. Der Test wurde wie in Tabelle 4.14 Hardware Verifizierung dargestellt durchgeführt.	i.O.
11	Hardware: Relais - Der Test wurde wie in Tabelle 4.14 Hardware Verifizierung dargestellt durchgeführt.	i.O.
12	Hardware: LEDs - Der Test wurde wie in Tabelle 4.14 Hardware Verifizierung dargestellt durchgeführt.	i.O.
13	Hardware: Buzzer / Dauerton - Der Test wurde wie in Tabelle 4.14 Hardware Verifizierung dargestellt durchgeführt.	i.O.

Die Überprüfung der Funktionalität des Prototyps zeigt, dass sowohl die Hardware als auch die Software den festgelegten Anforderungen entsprechen. Alle getesteten Komponenten und Zustände haben die Prüfungen erfolgreich bestanden, was die Zuverlässigkeit und Leistungsfähigkeit des Systems bestätigt.

5.3 Test des Prototyps im Fehlerfall

Das Sifa-System muss die Fähigkeit besitzen, sowohl Software als auch Hardware effektiv zu überwachen und Fehler zu erkennen. Diese Überwachungsfunktion ist entscheidend, um die Sicherheit und Zuverlässigkeit des Systems zu gewährleisten, indem potenzielle Fehlfunktionen frühzeitig identifiziert und behoben werden. In der folgenden Tabelle 5.2 werden die Ergebnisse der durchgeführten Prüfungen vorgestellt. Ist die Prüfung erfolgreich wird das Ergebnis als in Ordnung mit der Abkürzung i.O. gekennzeichnet.

Tabelle 5.2: Test des Prototyps im Fehlerfall

Test	Beschreibung	Ergebnis
1	Im Aktiv-Zustand prüft das Sifa-System auf Defekte am Drucktaster oder der Verbindung zum Mikrocontroller, indem die Leitung unterbrochen wird. Der Test ist erfolgreich, wenn das System den Fehler erkennt und in den Fehlerdiagnose-Zustand wechselt.	i.O.
2	Sifa-System-Aktiv: Erkennung von dauerhaftem Drücken oder Loslassen. Das Sifa-System muss reagieren, wenn der Drucktaster kontinuierlich losgelassen oder gedrückt wird. Der Test gilt als erfolgreich abgeschlossen, wenn das System den Fehler identifiziert und in den Warnzustand wechselt.	i.O.
3	Im Warning-Zustand prüft das Sifa-System auf Defekte am Drucktaster oder der Verbindung zum Mikrocontroller, indem die Leitung unterbrochen wird. Der Test ist erfolgreich, wenn das System den Fehler erkennt und in den Fehlerdiagnose-Zustand wechselt.	i.O.
4	Befindet sich das Sifa-System im Warning-Zustand und wird die Warnzeit nicht erkannt, gilt der Test als erfolgreich abgeschlossen, wenn die Software den Fehler identifiziert und in den Fehlerdiagnose-Zustand übergeht.	i.O.
5	Im Emergency-Brake-Zustand prüft das Sifa-System auf Defekte am Drucktaster oder der Verbindung zum Mikrocontroller durch Unterbrechung der Leitung. Der Test ist erfolgreich, wenn das System den Fehler erkennt und in den Fehlerdiagnose-Zustand wechselt.	i.O.
6	Befindet sich das Sifa-System im Emergency-Brake-Zustand, wird überprüft, ob ein Defekt am Notbremssignal oder an der Verbindung zwischen Mikrocontroller und Relais vorliegt.	i.O.

Die Tests des Prototyps im Fehlerfall haben gezeigt, dass das Sifa-System zuverlässig in der Lage ist, sowohl Software- als auch Hardwarefehler zu erkennen und angemessen darauf zu reagieren. Alle getesteten Szenarien wurden erfolgreich durchlaufen, was die Robustheit und Fehlertoleranz des Systems unterstreicht. Um sicherzustellen, dass keine relevanten Fehlerzustände übersehen wurden, wurden mehrere Ansätze verfolgt. Die umfassende Anforderungsanalyse, wie in Kapitel 3 beschrieben, identifizierte alle potenziellen Fehlerzustände

und bildete die Grundlage für die Entwicklung der Testszenarien. Die Testabdeckung wurde so gestaltet, dass alle Systemfunktionen und -zustände umfassend abgedeckt werden. Vor der physischen Implementierung wurden Simulationen und Modellierungen durchgeführt, um das Systemverhalten unter verschiedenen Bedingungen zu analysieren und potenzielle Fehlerzustände zu erkennen. Für kritische Funktionen, wie ein Defekt im Drucktaster, wurden redundante Tests implementiert, die die Zuverlässigkeit der Fehlererkennung erhöhen.

5.4 Verifizierung der Sicherheitsanforderungen

In diesem Abschnitt wird durch umfassende Tests und Prüfungen verifiziert, dass alle sicherheitskritischen Funktionen den Anforderungen aus Kapitel 3 entsprechen.

5.4.1 Verifizierung der Anforderungen an die Sicherheitsfunktionen

In der folgenden Tabelle 5.3 wird die Verifizierung der Anforderungen an die Sicherheitsfunktionen dargestellt, gemäß TSI [17] und UIC641[18]. Ist die Prüfung erfolgreich wird das Ergebnis als in Ordnung mit der Abkürzung i.O. gekennzeichnet.

Tabelle 5.3: Verifizierung der Anforderungen an die Sicherheitsfunktionen

Test	Beschreibung	Ergebnis
1	**Aktivitätserkennung:** Das System muss die Aktivität des Triebfahrzeugführers kontinuierlich überwachen [17] & [18].	i.O.
2	**Warnsignal:** Bei Inaktivität des Triebfahrzeugführers über einen Zeitraum von 30 Sekunden muss innerhalb von weiteren 2,5 ein optisches Signal ausgelöst werden [18].	i.O.
3	**Notbremssignal:** Wenn innerhalb von 2,5 Sekunden nach dem Warnsignal keine Aktivität festgestellt wird, muss ein optisches und akustisches Signal ausgelöst werden und das System das Notbremssignal aussenden, sobald die Zeit abläuft [18].	i.O.
4	**Manuelle Übersteuerung:** Das System muss eine Schnittstelle für die manuelle Übersteuerung durch den Triebfahrzeugführer bieten, um das Warnsignal zurückzusetzen oder die Notbremsung zu stoppen.	i.O.
5	**Benutzerschnittstelle:** Das System muss eine klare und intuitive Benutzerschnittstelle haben, die es dem Triebfahrzeugführer ermöglicht, schnell und effektiv auf Warnsignale zu reagieren und das System bei Bedarf zu übersteuern [18].	i.O.

5.4.2 Verifizierung der Anforderungen an die Sicherheitsintegrität

In der folgenden Tabelle 5.4 wird die Verifizierung der Anforderungen an die Sicherheitsintegrität aus Kapitel 3 dargestellt.

Tabelle 5.4: Verifizierung der Anforderungen an die Sicherheitsintegrität

Test	Beschreibung	Ergebnis
1	**Zuverlässigkeit:** Die Funktionalität der Sifa entspricht der Sicherheitsanforderungsstufe SIL3 gemäß den CENELEC-Normen [6]. Das System muss gewährleisten, dass im Zustand „Aktiv“ eine Zwangsbremsung ausgelöst wird, falls das Wachsamkeitssignal über den festgelegten Zeitraum ausbleibt. Die Wahrscheinlichkeit, dass die Signalisierung der Zwangsbremsung ausbleibt, muss geringer als $1 \cdot 10^{-7} \frac{1}{h}$ sein, wie in der Tabelle 9.2 zu sehen ist [6].	i.O.
2	**Reaktionszeit:** Die Reaktionszeit für die Auslösung des Warnsignals und die Aktivierung des Notbremssignals darf maximal 5,0 Sekunden betragen [18].	i.O.
3	**Umweltbedingungen und Höhe:** Das System funktioniert in einem Temperaturbereich T3 im Fahrzeugabteil von -25° C bis $+55^{\circ}$ C und bei einer relativen Luftfeuchtigkeit mit einem Jahresmittelwert von $75\,\%$. Die Höhenlage überschreitet die Klasse A3 - 1 200 m über dem Meeresspiegel - nicht [6] & [70].	i.O.
4	**Mechanische Bedingungen:** Das Sytem muss eine Vibrations- und Stoßfestigkeit, eine Temperaturbeständigkeit, einen Feuchtigkeits- und Korrosionsschutz sowie eine Montage- und Wartungsfreundlichkeit aufweisen [6].	i.O.

5.4.3 Verifizierung der Integrität gegen systematische Fehler

In der folgenden Tabelle 5.5 wird die Verifizierung der Integrität gegen systematische Fehler dargestellt.

Tabelle 5.5: Verifizierung der Integrität gegen systematische Fehler

Test	Beschreibung	Ergebnis
1	**Fail-Safe-Mechanismen:** Das System muss in einem sicheren Zustand verbleiben, auch bei Ausfall von zwei Komponenten, aufgrund der Unabhängigkeit zwischen den Betrachtungseinheiten [6].	i.O.
2	**Permanente Tastenbetätigung:** Das System ist darauf ausgelegt, eine kontinuierliche Betätigung der Taste zu erkennen und unverzüglich darauf zu reagieren [6] .	i.O.
3	**Einhaltung von Normen:** Das System muss den Sicherheitsnormen gemäß UIC 641 [18] und anderen relevanten Eisenbahnstandards wie DIN EN 50129 [6] und TSI [17] entsprechen.	i.O.
4	**Aktion nach Offenbarung:** Für SIL 3 und SIL 4 muss das System, Subsystem oder die Einrichtung nach der Offenbarung eines ersten Ausfalls einen sicheren Zustand einnehmen oder darin verbleiben [6].	i.O.

Die Anforderung im „Fail-Safety“-Fall mit mindestens zwei Betrachtungseinheiten besagt, dass ein erster Ausfall schnell erkannt und ein sicherer Zustand erzwungen werden muss, um das Risiko eines zweiten Ausfalls unter dem spezifizierten Zielwert zu halten. Im „Fail-Safety“-Fall durch eine sicherheitsgerichtete Ausfallreaktion darf die Zeit für die Erkennung und die Reaktion nicht die festgelegte Grenze für die Dauer eines potenziell gefährlichen Zustands überschreiten [6]. Für diese Arbeit wurden die Techniken und Maßnahmen für die Vermeidung von systematischen Fehlern, des Anhangs E, der Norm DIN EN 50129 [6] betrachtet.

5.4.4 Verifizierung der Integrität gegen zufällige Ausfälle

In der folgenden Tabelle 5.6 wird die Verifizierung der Integrität gegen zufällige Ausfälle dargestellt.

Tabelle 5.6: Verifizierung der Integrität gegen zufällige Ausfälle

Test	Beschreibung	Ergebnis
1	**Redundanz:** Um die Integrität gegen zufällige Ausfälle zu gewährleisten, muss das System redundante Komponenten verwenden, insbesondere in kritischen Bereichen wie der Signalverarbeitung und der Energieversorgung [6].	i.O.
2	**Common-Cause-Failure:** Um Common-Cause-Failures zu verhindern, ist der Einsatz einer zweikanaligen, diversitären Mikrocontrollerarchitektur erforderlich. Sämtliche Eingänge und Ausgänge müssen dabei von beiden Kanälen evaluiert werden [6].	i.O.
3	**Selbsttest:** Das System sollte einen Selbsttest am Anfang der Aktivierung des Systems durchführen, um sicherzustellen, dass alle Komponenten und Funktionen ordnungsgemäß arbeiten [6].	i.O.
4	**Fehlererkennung und -management:** Das System muss in der Lage sein, Fehler zu erkennen und entsprechende Maßnahmen zu ergreifen, um die Sicherheit zu gewährleisten. Der Ausgangszustand „Fehler“ muss von beiden Kanälen unabhängig lesbar sein, um eine Deaktivierung der Sifa zuverlässig anzuzeigen [6].	i.O.
5	**Dokumentation und Protokollierung:** Alle Vorfälle und Systemzustände sollten dokumentiert und protokolliert werden, um eine nachträgliche Analyse und kontinuierliche Verbesserung des Systems zu ermöglichen [6].	i.O.
6	**Software:** Die Software muss angemessene Mechanismen implementieren, um die Überwachung des Programmablaufs sicherzustellen [5].	i.O.
7	**Galvanische Trennung:** Um die Demonstration der Unabhängigkeit der beiden Kanäle zu vereinfachen, wird eine galvanische Trennung zwischen den Kanälen durchgeführt [6].	i.O.

6 Sicherheitsnachweis

In diesem Kapitel erfolgt die Dokumentation des Sicherheitsnachweises für das Sifa-System. Es orientiert sich in seinem Aufbau an der in Unterkapitel 2.4.2 vorgestellten Struktur des Sicherheitsnachweises (siehe Abb. 2.3). Der technische Sicherheitsbericht bildet die Grundlage, indem er die Implementierung und Wirksamkeit der sicherheitsrelevanten Funktionen detailliert beschreibt. Ergänzend dazu wird der Qualitätsmanagementbericht vorgestellt, der die Einhaltung der festgelegten Qualitätsstandards während des gesamten Entwicklungsprozesses sicherstellt. Die Validierung der funktionalen Sicherheitsprüfung bestätigt, dass alle sicherheitskritischen Funktionen korrekt implementiert und getestet wurden. Darüber hinaus wird die Validierung der Systemprüfung behandelt, um die Gesamtleistung und Zuverlässigkeit des Systems zu gewährleisten. Abschließend wird die Erfüllung der Anforderungen an die Sicherheitsintegritätsstufe SIL 3 nachgewiesen, was die Eignung für den Einsatz in sicherheitskritischen Anwendungen bestätigt. Dieses Kapitel bietet somit einen Überblick über die Maßnahmen und Prüfungen, die zur Sicherstellung der Systemintegrität und -sicherheit durchgeführt werden müssen.

6.1 Definition des Systems

Die Definition des Systems bildet den ersten Teil des Sicherheitsnachweises (siehe Abb. 2.3) und erfolgt im Rahmen der Systemarchitekturspezifikation in Unterkapitel 3.3.

6.2 Qualitätsmanagementbericht

Der Qualitätsmanagementbericht bildet den zweiten Teil des Sicherheitsnachweises (siehe Abb. 2.3). Gemäß der Norm DIN EN 50129 [6] muss die Qualität eines Sifa-Systems über dessen gesamte Lebensdauer hinweg durch ein leistungsfähiges Qualitätsmanagementsystem sichergestellt werden, das den Anforderungen der DIN EN ISO 9001 [77] entspricht. Dieses System optimiert die Prozesseffizienz und trägt zur Reduzierung menschlicher und systematischer Fehler bei. Die konsequente Einhaltung dieser Normen gewährleistet die Zuverlässigkeit und Sicherheit des Systems und stärkt das Vertrauen in seine Funktionalität.

Die Aspekte, die im Rahmen des Qualitätsmanagementsystems überwacht und im Qualitätsmanagementbericht aufgenommen werden sollen, werden in der folgenden Tabelle dargestellt.

Tabelle 6.1: Aspekte des Qualitätsmanagementsystems

Aspekt	**Beschrieben in**
Organisationsstruktur	Die Rollen (DIN EN 50129, Kapitel 5.3.4.2 [6]) wurden vom Autor übernommen. Näher behandelt in Kapitel 6.3.2 Sicherheitsorganisation.
Qualitätsplanung und -verfahren	Es wurden die relevanten Normen aus Tabelle 2.1 berücksichtigt.
Spezifikation der Anforderungen	In Kapitel 3 behandelt.
Überwachung des Entwurfs	Die Rollen (DIN EN 50129, Kapitel 5.3.4.2 [6]) wurden vom Autor übernommen. In Kapitel 6.3.2 Sicherheitsorganisation behandelt.
Verifizierung und Prüfung des Entwurfs	In Unterkapitel 4.3 Simulation des Systems und Kapitel 5 Prototyping behandelt.
Entwicklung der Anwendung	In Kapitel 5 Prototyping behandelt.
Beschaffung und Herstellung	In Kapitel 5 Prototyping behandelt.
Identifikation und Verfolgbarkeit des Produkts	In Kapitel 3 Anforderungsanalyse behandelt.
Handhabung und Lagerung	In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen behandelt.
Inspektion und Prüfung	In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen behandelt.
Nicht-Konformität und korrigierende Maßnahmen	Alle Nicht-Konformitäten wurden in Kapitel 4 korrigiert.
Verpackung und Lieferung	Nicht anwendbar in dieser Arbeit.
Installation und Inbetriebsetzung	In Kapitel 5 Prototyping behandelt.
Qualitätsüberwachung und - meldungen	Durch die Betreuer dieser Arbeit.
Dokumentation und Aufzeichnungen	Der Entwicklungsprozess ist in allen geschriebenen Kapiteln dokumentiert.
Konfigurationsmanagement und Änderungsüberwachung	Änderungen in der Entwicklung wurden intern vom Autor dokumentiert.
Kompetenz und Schulung des Personals	Nicht anwendbar in dieser Arbeit.
Qualitätsaudits und ihre Nachverfolgung	Behandelt In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen.
Stilllegung und Entsorgung	Behandelt in Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen, SRACs für Stilllegung und Entsorgung

6.3 Sicherheitsmanagementbericht

Der Sicherheitsmanagementbericht bildet den dritten Teil des Sicherheitsnachweises (siehe Abb. 2.3). Eine Bedingung für die Sicherheitsanerkennung ist, dass die Sicherheit des Sifa-Systems gemäß dem in DIN EN 50126-1 [3] und DIN EN 50126-2 [4] beschriebenen RAMS-Managementprozess gewährleistet wurde und weiterhin im Rahmen eines effektiven Sicherheitsmanagementprozesses gewährleistet bleibt. In der folgenden Tabelle 6.2 werden relevante Punkte des Sicherheitsmanagementprozess vorgestellt.

Tabelle 6.2: Der Sicherheitsmanagementprozess

Thema	**Beschrieben in**
Richtlinie für die Strukturierung der Dokumentation	Die vollständige Struktur dieser Arbeit ist im Inhaltsverzeichnis aufgeführt.
Sicherheitslebenszyklus	In Unterkapitel 6.3.1 Sicherheitslebenszyklus behandelt.
Sicherheitsorganisation	In Unterkapitel 6.3.2 Sicherheitsorganisation behandelt.
Sicherheitsplan	Teilweise behandelt in Unterkapitel 3.2 Sicherheitsanforderungen.
Gefährdungslogbuch	Teilweise behandelt in Unterkapitel 3.1.3 Gefährdungsanalyse und Risikobewertung der Sifa.
Sicherheitsanforderungsspezifikation	Behandelt in Unterkapitel 3.2 Sicherheitsanforderungen.
Systementwurf für Sicherheit	Behandelt in Kapitel 4.
Betriebs- und Instandhaltungsplan für Sicherheit	In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen behandelt.
Sicherheitsverifizierung	In Unterkapitel 3.2 Sicherheitsanforderungen definiert und in Unterkapitel 5.4 Verifizierung der Sicherheitsanforderungen behandelt.
Sicherheitsvalidierung	In Kapitel 6.5 Validierung der funktionalen Sicherheitsprüfung behandelt.
Sicherheitserprobung	In Unterkapitel 5.4 Verifizierung der Sicherheitsanforderungen behandelt.
Management der sicherheitsbezogenen Anwendungsbedingungen	In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen behandelt.
Sicherheitsbegründung	In Kapitel 6 Sicherheitsnachweis behandelt.
Unabhängige Sicherheitsbegutachtung	Nicht anwendbar für diese Arbeit.

6.3.1 Sicherheitslebenszyklus

Die Struktur dieser Arbeit orientiert sich am Sicherheitslebenszyklus, der als Referenzmodell dient. In Abbildung 6.1 wird dieser als V-Modell dargestellt [6].

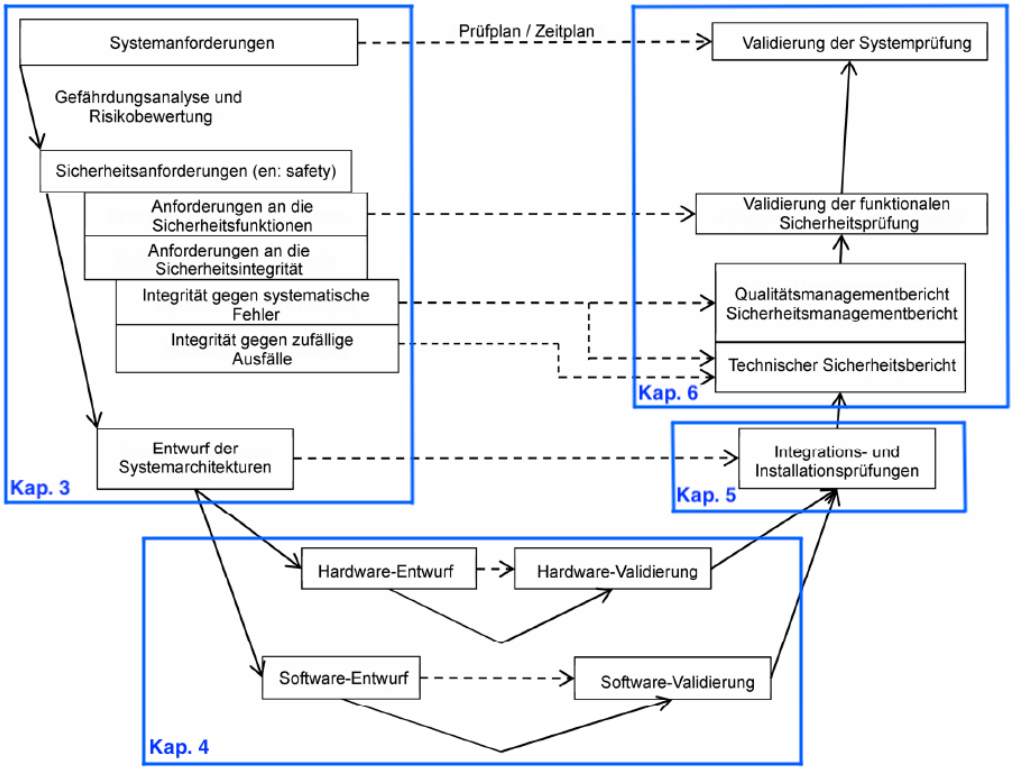


Abbildung 6.1: Sicherheitslebenszyklus [6]

Wie im Bild 6.1 ersichtlich, wird in jedem Kapitel ein Teil des Sicherheitslebenszyklus behandelt. Kapitel 3 befasst sich mit den System- und Sicherheitsanforderungen und der Systemarchitekturspezifikation,. In Kapitel 4 werden das Hardware- und Softwaredesign sowie die Simulation des Systems zur Verifizierung von Hardware und Software behandelt. Kapitel 5 widmet sich dem Prototyping, einschließlich des Aufbaus des Prototyps, der Überprüfung seiner Funktionalität, der Tests im Fehlerfall und der Verifizierung der Sicherheitsanforderungen. Kapitel 6 behandelt den Sicherheitsnachweis, in dem die Entwicklung des Sifa-Systems validiert wird.

6.3.2 Sicherheitsorganisation

Der Sicherheitsmanagementprozess, laut Abschnitt 5.3.4 der Norm DIN EN 50129 [6], erfordert die Überwachung durch eine geeignete Organisation. Das ISA (Independent Safety Assessment) im Eisenbahnbereich ist eine unabhängige Prüfung, ob ein sicherheitsrelevantes System die geltenden Normen und Anforderungen erfüllt. Fachkundiges Personal mit anerkannten Kompetenzen, einschließlich technischer Qualifikationen und Erfahrung, ist für eine solche Prüfung notwendig [76]. Ein Verzeichnis der zugewiesenen Rollen bei Systementwicklungen oder -änderungen muss geführt werden. Die Unabhängigkeit zwischen den Rollen ist sicherzustellen. Diese Regelungen gelten für alle Lebenszyklusphasen, angepasst an den geforderten Sicherheitsintegritätsgrad. In der folgenden Abbildung 6.2 ist die Unabhängigkeit der Rollen für unterschiedliche SILs dargestellt.

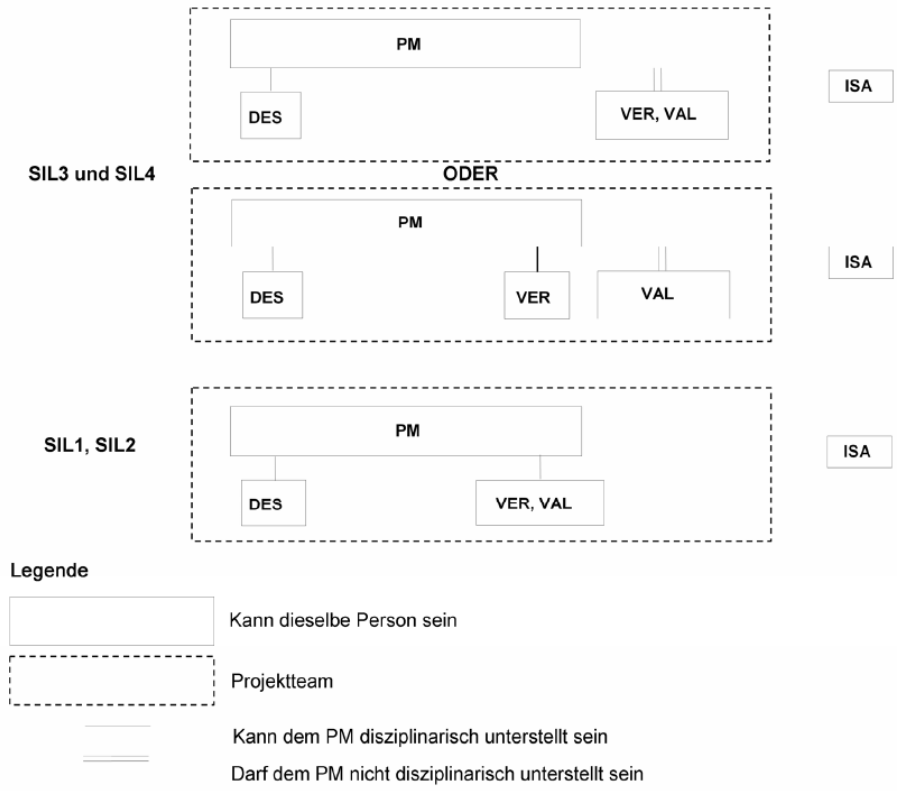


Abbildung 6.2: Unabhängigkeit der Rollen für unterschiedliche SILs [7]

Für diese Arbeit übernimmt der Autor alle Rollen: Projektmanager (PM), Designer (DES), Verifizierer (VER) und Validierer (VAL).

6.4 Technischer Sicherheitsbericht

Der technische Sicherheitsbericht bildet den vierten Teil des Sicherheitsnachweises (siehe Abb. 2.3). Er dokumentiert den Nachweis der Entwurfssicherheit und bildet einen wesentlichen Bestandteil des Sicherheitsnachweises. Der Aufbau dieses Unterkapitels orientiert sich an der in Unterkapitel 2.4.2 vorgestellten Struktur des technischen Sicherheitsberichtes in Abbildung 2.4.

6.4.1 Abschnitt 1: Einleitung

In diesem Abschnitt wird der Entwurf des Sifa-Systems beleuchtet, mit besonderem Augenmerk auf die technischen Sicherheitsprinzipien, die für die Gewährleistung der Systemsicherheit entscheidend sind.

6.4.2 Abschnitt 2: Nachweis des korrekten funktionalen Verhaltens

In diesem Abschnitt wird nachgewiesen, dass das Sifa-System unter normalen Betriebsbedingungen und ohne Störungen den festgelegten Betriebs- und Sicherheitsanforderungen entsprechend einwandfrei funktioniert [6]. Die folgenden Aspekte der untenstehenden Tabelle 6.3 sind zu berücksichtigen.

Tabelle 6.3: Nachweis des korrekten funktionalen Verhaltens

Aspekt	**Behandelt in**
Beschreibung der Systemarchitektur	In Unterkapitel 3.3 wird die Systemarchitekturspezifikation behandelt.
Definition der Schnittstellen	In Unterkapitel 3.3.2 werden die Systemgrenze und die Schnittstellen behandelt.
Erfüllung der Systemanforderungsspezifikation	In Unterkapitel 5.2 wird die Überprüfung der Funktionalität des Prototyps dargestellt.
Erfüllung der Sicherheitsanforderungsspezifikation	In Unterkapitel 5.3 wird der Test des Prototyps im Fehlerfall dargestellt und in Unterkapitel 5.4 die Verifizierung der Sicherheitsanforderungen behandelt.
Nachweis der korrekten Hardwarefunktionalität	In Kapitel 4.3.2 wird die Verifizierung der Hardware behandelt. Im Unterkapitel 5.2 wird die Überprüfung der Funktionalität des Prototyps dargestellt.
Nachweis der korrekten Softwarefunktionalität	In Unterkapitel 4.3.3 wird die Verifizierung der Software behandelt und in Unterkapitel 5.2 die Überprüfung der Funktionalität des Prototyps dargestellt.

6.4.3 Abschnitt 3: Ausfallauswirkungen

In diesem Abschnitt ist nachzuweisen, dass das System auch im Falle zufälliger Hardwareausfälle weiterhin die spezifizierten Sicherheitsanforderungen und das quantifizierte Sicherheitsziel erfüllt. Zudem wird aufgezeigt, welche technischen Schritte unternommen wurden, um das resultierende Risiko auf ein akzeptables Maß zu reduzieren. Die in Tabelle 6.4 aufgeführten Überschriften sollten in diesem Abschnitt berücksichtigt werden, wie im Anhang B.3 der der Norm DIN EN 50129 [6] dargelegt.

Tabelle 6.4: Ausfallauswirkungen

Thema	**Behandelt in**
Auswirkungen von Einzelausfällen	In Tabelle 3.15 des Unterkapitels 3.4.1 Fehlermöglichkeits- und Einflussanalyse (FMEA) dargestellt. „Fail-safety“ wird in Kapitel 5.4 verifiziert.
Unabhängigkeit von Betrachtungseinheiten	Das Sifa-System ist so konzipiert, dass die Unabhängigkeit durch mindestens zwei Betrachtungseinheiten und durch eine „fail-safety“ sicherheitsgerichtete Ausfallreaktion bewiesen ist. In Unterkapitel 3.2 werden die Sicherheitsanforderungen behandelt.
Offenbarung von Einzelausfällen	In Unterkapitel 3.4.1 wird die Fehlermöglichkeits- und Einflussanalyse (FMEA) und in Unterkapitel 3.4.2 die Fehlerbaumanalyse behandelt.
Aktion nach der Offenbarung	In Unterkapitel 3.2 werden die Sicherheitsanforderungen analysiert und in Abschnitt 4.3 Simulation des Systems und 5.4 Verifizierung der Sicherheitsanforderungen bestätigt.
Auswirkungen von Mehrfachausfällen	Werden in der Tabelle 3.15 des Unterkapitels 3.4.1 Fehlermöglichkeits- und Einflussanalyse (FMEA) und des Unterkapitels 4.1.5 Fehlerbaumanalyse (FTA) dargestellt. „Fail-safety“ wird in Kapitel 5.4 verifiziert.
Schutz gegen systematische Fehler	In Unterkapitel 5.4.3 Verifizierung der Integrität gegen systematische Fehler behandelt.

Daraus lässt sich schlussfolgern, dass alle Aspekte des dritten Abschnitts des technischen Sicherheitsberichtes erfüllt und während des Lebenszyklus des Systems berücksichtigt werden.

6.4.4 Abschnitt 4: Betrieb mit externen Einflüssen

In diesem Abschnitt ist darzulegen, dass das System auch unter externen Einflüssen, wie in der Systemanforderungsspezifikation in Unterkapitel 3.3 festgelegt, sowohl seine definierten betrieblichen als auch seine festgelegten Sicherheitsanforderungen erfüllt [6]. Die relevanten Einflüsse werden in der folgenden Tabelle 6.5 beschrieben.

Tabelle 6.5: Betrieb mit externen Einflüssen

Externer Einfluss	**Behandelt in**
Klimatische Bedingungen	In Unterkapitel 3.2.2 Anforderungen an die Sicherheitsintegrität definiert und in Kapitel 5.4.2 Verifizierung der Anforderungen an die Sicherheitsintegrität verifiziert. (Siehe Tabelle 5.4)
Mechanische Bedingungen	In Unterkapitel 3.2.2 Anforderungen an die Sicherheitsintegrität definiert und in Kapitel 5.4.2 Verifizierung der Anforderungen an die Sicherheitsintegrität verifiziert (Siehe Tabelle 5.4).
Höhe	In Unterkapitel 3.2.2 Anforderungen an die Sicherheitsintegrität definiert und in Kapitel 5.4.2 Verifizierung der Anforderungen an die Sicherheitsintegrität verifiziert (Siehe Tabelle 5.4).
Elektrische Bedingungen	In Unterkapitel 3.2.4 Integrität gegen zufällige Ausfälle definiert und in Unterkapitel 5.4.4 Verifizierung der Integrität gegen zufällige Ausfälle verifiziert.
Schutz vor unberechtigtem Zugriff	Nicht behandelt. Das Sifa-System wird nicht im realen Betrieb eingesetzt. Es wird davon ausgegangen, dass der Benutzer das Sifa-System zu akademischen Zwecken verwendet.
Erschwerte Bedingungen	Nicht erforderlich. Sifa-System für akademische Zwecke.

Daraus lässt sich schlussfolgern, dass alle erforderlichen Aspekte des vierten Abschnitts des technischen Sicherheitsberichtes erfüllt und während des Lebenszyklus des Systems berücksichtigt werden.

6.4.5 Abschnitt 5: Sicherheitsbezogene Anwendungsbedingungen

In diesem Abschnitt des technischen Sicherheitsberichtes sind die Regeln, Bedingungen und Einschränkungen zu definieren, die für die funktionale Sicherheit wichtig sind und bei der Nutzung des Systems eingehalten werden müssen [6]. In der folgenden Tabelle 6.6 werden die sicherheitsbezogenen Anwendungsbedingungen dargestellt.

Tabelle 6.6: Sicherheitsbezogene Anwendungsbedingungen

Anwendungsbedingungen	**Behandelt in**
Systemprojektierung und -aufbau	In Kapitel 3, 4 und 5 behandelt.
SRAC für Betrieb, Instandhaltung und Sicherheitsüberwachung	In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen behandelt. (Siehe Tabelle 3.16)
SRACs für Stilllegung und Entsorgung	In Unterkapitel 3.4.3 Sicherheitsbezogene Anwendungsbedingungen behandelt. (Siehe Tabelle 3.17)

6.4.6 Abschnitt 6: Ergebnisse der Sicherheitserprobung

In Unterkapitel 5.4 Verifizierung der Sicherheitsanforderungen wurden die Sicherheitstests im Normalbetrieb erfolgreich durchgeführt und abgeschlossen, wie es in Unterkapitel 5.3.12 Sicherheitserprobung der Norm DIN EN 50129 [6] erklärt wird.

6.5 Validierung der funktionalen Sicherheitsprüfung

Die Validierung der funktionalen Sicherheitsprüfung folgt denselben Schritten wie die Verifizierung in Kapitel 5.4. Im Unterschied zur Verifizierung muss diese allerdings unabhängig durchgeführt werden, wie in Kapitel 5.3.4.2 der Norm DIN EN 50129 [6] Unabhängigkeit der Rollen gefordert ist. Die validierende Person darf nicht dem Projektmanager unterstellt sein und nicht dem Projektteam angehören. Aus diesen und aus Gründen des Umfangs dieser Arbeit wird die Validierung der funktionalen Sicherheitsprüfung nicht durchgeführt.

6.6 Validierung der Systemprüfung

Dieses Unterkapitel beschäftigt sich mit der Validierung der Systemprüfung, wobei der Fokus auf den Vergleich der erzielten Ergebnisse mit den Anforderungen der TSI [17] und der UIC 641 [18] gelegt wird. Die durchgeführten Systemtests zeigen, dass das System die festgelegten Standards und Spezifikationen erfüllt. Die Validierung bestätigt die Konformität des Systems mit den relevanten Sicherheits- und Betriebsanforderungen.

6.6.1 Validierung der Systemanforderungen gemäß TSI

In diesem Abschnitt erfolgt die Validierung der in den TSI festgelegten Systemanforderungen. Der Fokus liegt hierbei auf dem Nachweis der bereits in Kapitel 3.1.1 vorgestellten Inspektionsanforderungen. Jede Anforderungstabelle verfügt dabei über eine Nachweisspalte, in der die jeweilige Quelle des Nachweises zur Erfüllung der Anforderung dokumentiert ist.

In der folgenden Tabelle 6.7 wird der erste Nachweis der Inspektionsanforderung für die Kontrolle der Wachsamkeit des Triebfahrzeugführers vorgestellt.

Tabelle 6.7: Nachweis - Kontrolle der Wachsamkeit des Triebfahrzeugführers [17]

Punkt	Inspektionsanforderung	Nachweis
(1)	Der Führerraum ist mit einer Vorrichtung auszustatten, mit der die Aktivität des Triebfahrzeugführers überwacht und der Zug automatisch angehalten werden kann, wenn eine fehlende Aktivität des Triebfahrzeugführers erkannt wird. Mit dieser fahrzeugseitigen technischen Vorrichtung kann das Eisenbahnunternehmen die Anforderung des Abschnitts 4.2.2.9 der TSI OPE erfüllen.	3.3.1 System Definition: Zeit-Sifa

In der folgenden Tabelle 6.8 werden die Nachweise des zweiten Punktes der Inspektionsanforderung, die Spezifikationen für die Vorrichtungen zur Überwachung der Aktivität des Triebfahrzeugführers, vorgestellt.

Tabelle 6.8: Nachweis - Spezifikationen für die Vorrichtungen zur Überwachung der Aktivität [17]

Punkt	Inspektionsanforderung	Nachweis
(2)	Spezifikationen für die Vorrichtungen zur Überwachung der Aktivität (und zur Erkennung einer fehlenden Aktivität) des Triebfahrzeugführers:	
	Die Aktivität des Triebfahrzeugführers ist zu überwachen, sofern sich der Zug in Fahrkonfiguration im Zustand „Fahren“ befindet. (Kriterium für die Bewegungserkennung ist eine niedrige Geschwindigkeitsschwelle.) Diese Überwachung hat über die Kontrolle der Aktivität des Triebfahrzeugführers in Bezug auf anerkannte Schnittstellen zwischen dem Triebfahrzeugführer und dem Fahrzeug wie z. B. bestimmte Vorrichtungen (Pedal, Druckknöpfe, Sensoren usw.) und/oder anerkannte Schnittstellen zwischen dem Triebfahrzeugführer und der Leit- und Steuerungselektronik zu erfolgen.	In Kapitel 3.3 Systemarchitekturspezifikation, unter 3.3.2 Systemgrenze und Schnittstellen nachgewiesen.
	Wird an den anerkannten Schnittstellen zwischen Triebfahrzeugführer und Fahrzeug während eines Zeitraums von mehr als X Sekunden keine Aktivität beobachtet, wird eine fehlende Aktivität des Triebfahrzeugführers festgestellt.	Verifiziert und nachgewiesen in Kapitel 5.2 Überprüfung der Funktionalität des Prototyps.
	Das System muss (in der Werkstatt im Rahmen der Instandhaltung) eine Anpassung der Zeit X innerhalb einer Spanne von 5 bis 60 Sekunden ermöglichen.	In Kapitel 5.2 nachgewiesen.
	Wird die gleiche Aktivität fortlaufend über einen Zeitraum von mehr als maximal 60 Sekunden ohne weitere Aktivitäten an einer anerkannten Schnittstelle zwischen Triebfahrzeugführer und Fahrzeug beobachtet, stellt das System ebenfalls eine fehlende Aktivität des Triebfahrzeugführers fest.	In Kapitel 5.2 nachgewiesen.
	Vor dem Feststellen einer fehlenden Aktivität des Triebfahrzeugführers erfolgt eine entsprechende Warnung an den Triebfahrzeugführer, damit dieser reagieren und das System zurücksetzen kann.	In Kapitel 5.2 nachgewiesen.
	Dem System soll die Information „Fehlende Aktivität des Triebfahrzeugführers erkannt“ zur Übermittlung an andere Systeme (z. B. das Funksystem) zur Verfügung stehen.	In Kapitel 5.2 nachgewiesen.

In der folgenden Tabelle 6.9 wird der Nachweis des dritten Punktes der Inspektionsanforderung für die Kontrolle der Wachsamkeit des Triebfahrzeugführers vorgestellt.

Tabelle 6.9: Nachweis - TSI Kontrolle der Wachsamkeit des Triebfahrzeugführer -zusätzliche Anforderung [17]

Punkt	**Inspektionsanforderung**	**Nachweis**
(3)	Zusätzliche Anforderung:	
	Die Funktion zur Erkennung einer fehlenden Aktivität des Triebfahrzeugführers ist einer Zuverlässigkeitsuntersuchung zu unterziehen, in der Fehlermodi der betreffenden Komponenten ebenso zu berücksichtigen sind wie Redundanzen, die eingesetzte Software, regelmäßige Prüfungen und sonstige Vorschriften. Die geschätzte Ausfallquote der Funktion (d. h. die Wahrscheinlichkeit, dass eine fehlende Aktivität des Triebfahrzeugführers im oben beschriebenen Sinne nicht erkannt wird) ist in Abschnitt 4.2.12 in der technischen Dokumentation anzugeben.	In Kapitel 4, unter 4.2 Software-Design, wird der Entwurf beschrieben. In Unterkapitel 4.3.3 die Software-Verifizierung und in Punkt 5.4 Verifizierung der Sicherheitsanforderungen nachgewiesen.

In der folgenden Tabelle 6.10 wird der Nachweis des vierten Punktes der Inspektionsanforderung zur Anzeige von Aktivitäten für die Wachsamkeitskontrolle über den Triebfahrzeugführer vorgestellt.

Tabelle 6.10: Nachweis - TSI Spezifikationen zur Anzeige von Aktivitäten [17]

Punkt	**Inspektionsanforderung**	**Nachweis**
(4)	Spezifikationen zur Anzeige von Aktivitäten auf Zugebene, wenn eine fehlende Aktivität des Triebfahrzeugführers erkannt wird:	
	Bei fehlender Aktivität des Triebfahrzeugführers in einem Zug, der sich in Fahrkonfiguration im Zustand „Fahren“ befindet (Kriterium für die Bewegungserkennung ist eine niedrige Geschwindigkeitsschwelle), muss eine Vollbremsung erfolgen.	In Kapitel 4.3 Simulation des Systems und 5.2 Überprüfung der Funktionalität des Prototyps nachgewiesen.

6.6.2 Validierung der Bedingungen der Sifa gemäß UIC 641

Die Validierung der Anforderungen des internationalen Eisenbahnverbandes an eine Sicherheitsfahrschaltung erfolgt in tabellarischer Form. Dabei wurde bereits bei der Vorstellung der Anforderungen in Kapitel 3.1.2 jede Tabelle mit einer Nachweisspalte versehen, in der die jeweilige Quelle des Nachweises zur Erfüllung der Anforderung im Rahmen des Validierungsprozesses dokumentiert werden kann. In der folgenden Tabelle 6.11 werden die Nachweise der UIC 641 Anforderungen 1 bis 3 vorgestellt.

Tabelle 6.11: Nachweis - UIC 641 Anforderungen 1-3 [18]

	Inspektionsanforderung	**Nachweis**
1	Aufgabe	
	Die Sicherheitsfahrschaltung überwacht die Dienstfähigkeit des Triebfahrzeugführers vom Fahrzeug aus. Sie wirkt unabhängig von ortsfesten Einrichtungen. Bei nicht ordnungsgemäßer Bedienung durch den Triebfahrzeugführer veranlasst sie die Abschaltung der Antriebskraft des Triebfahrzeugs und eine Zwangsbremsung.	In Kapitel 5 Prototyping, unter Punkt 5.2 Überprüfung der Funktionalität des Prototyps überprüft und nachgewiesen.
2	Einrichtung auf dem Führerraum	
	Die Führerraumeinrichtungen umfassen: 1. Betätigungseinrichtungen wie zum Beispiel Handtaster, Fußtaster, Kniehebel, 2. eine akustische Signaleinrichtung wie zum Beispiel Summer, Hupe, Wecker. Dieses Signal muss unter allen Betriebsbedingungen hörbar sein, 3. es können zusätzliche optische Signaleinrichtungen vorgesehen werden.	In Kapitel 4 Design und Konstruktion definiert und entworfen und in Kapitel 5 Prototyping verifiziert.
3	Bereitschaftsstellung	
3.1.	Die Sicherheitsfahrschaltung schaltet sich spätestens selbsttätig ein, wenn die Geschwindigkeit von $20\,\mathrm{km/h}$ erreicht ist, und bleibt eingeschaltet, solange die Geschwindigkeit diesen Wert überschreitet.	Als Schalter simuliert. In Unterkapitel 4.1 Systemarchitekturspezifikation nachgewiesen.
3.2.	Einzelne Bahnen können im gegenseitigen Einvernehmen eine Sicherheitsfahrschaltung verwenden, die vor dem Anfahren vom Triebfahrzeugführer einzuschalten ist.	In Kapitel 4 Design und Konstruktion nachgewiesen.

In der folgenden Tabelle 6.12 werden die Nachweise über die Erfüllung der UIC 641 Anforderungen 4 vorgestellt.

Tabelle 6.12: Nachweis - UIC 641 Anforderungen 4 [18]

	Inspektionsanforderung	**Nachweis**
4	Eingriffsstellung	
4.1.	Wenn in Bereitschaftsstellung: 1. keine der Betätigungseinrichtungen betätigt wird oder 2. die Betätigungseinrichtungen ohne Unterbrechung länger als t = 30 sek. betätigt werden, a. ertönt spätestens nach 2,5 sek. ein akustisches Signal, b. wird nach spätestens weiteren 2,5 sek. die Antriebskraft abgeschaltet und eine Zwangsbremsung eingeleitet. Die angegebenen Zeiten können mit Toleranzen von 15 % behaftet sein.	In Kapitel 5 Prototyping, unter Punkt 5.2 Überprüfung der Funktionalität des Prototyps nachgewiesen.
4.2.	An Stelle der Zeiten nach Punkt 4.1 - Seite 5 der [18] kann die Sicherheitsfahrschaltung auch nach bestimmten Wegen eingreifen, die so festgelegt werden, dass sich bei Fahrgeschwindigkeiten von 100 km/h die Zeiten nach Punkt 4.1 ergeben.	Nicht Teil der Systemgrenze. Es ist möglich, mehrere Input Signale hinzufügen.
4.3.	An Stelle der Unterbrechung der Betätigung der Betätigungseinrichtungen kann die Betätigung eines anderen Steuerorgans treten, wenn das im Schema der Sicherheitsfahrschaltung vorgesehen ist und dadurch die gleiche Wirkung hervorgerufen wird wie durch das Loslassen.	Nicht Teil der Systemgrenze. Es ist aber möglich, mehrere Input Signale hinzufügen.
4.4.	Ein Ausfall der zum Betrieb der Sicherheitsfahrschaltung nötigen Versorgungsspannung führt zur Abschaltung der Antriebszugkraft und zur Zwangsbremsung.	Im Kapitel 5 Prototyping, unter Punkt 5.2 Überprüfung der Funktionalität des Prototyps nachgewiesen.
4.5.	Bei Einleitung der Zwangsbremsung durch die Sicherheitsfahrschaltung muss die Entlüftung der Hauptluftleitung in einer Zeit erfolgen, die nicht größer ist als bei Einleitung einer Schnellbremsung durch das Führerbremsventil ist. Die bei Entlüftung entweichende Luftmenge per Zeiteinheit muss merklich größer als die durch die Bremseinrichtung in Füllstellung des Führerbremsventils nachgespeiste Luftmenge sein, um ein sicheres Ansprechen der Bremsen des Zuges zu gewährleisten.	Nicht Teil der Systemgrenze. Es wird ein Notbremssignal gesendet und durch LEDs simuliert.

In der folgenden Tabelle 6.13 werden die Nachweise über die Erfüllung der UIC 641 Anforderungen 5 vorgestellt.

Tabelle 6.13: Nachweis - UIC 641 Anforderungen 5 [18]

	Inspektionsanforderung	**Nachweis**
5	Aufhebung des Eingriffes	
5.1.	Vor Eintreten der Zwangsbremsung kann das Eingreifen der Sicherheitsfahrschaltung aufgehoben werden, indem bei Ansprechen: eine der Betätigungseinrichtungen nach Punkt 2, Absatz 1 betätigt wird, die Betätigung der Betätigungseinrichtungen kurzzeitig unterbrochen wird.	Definiert in Punkt 3.3.4 Definition der Zustände und in Punkt 5.2 Überprüfung der Funktionalität des Prototyps nachgewiesen.
5.2.	Nach Abschalten der Antriebskraft und Eintreten der Zwangsbremsung kann das Eingreifen der Sicherheitsfahrschaltung nur aufgehoben werden, wenn zusätzlich zu den unter Punkt 5.1 genannten Betätigungshandlungen vom Triebfahrzeugführer mindestens eine weitere Tätigkeit ausgeführt wird, zum Beispiel Auslösen der Bremse oder Wiederherstellung der Antriebskraft.	Definiert in Unterkapitel 3.3.4 Anforderungen an den Entwurf der Software und in Punkt 5.2 Überprüfung der Funktionalität des Prototyps nachgewiesen.

6.7 Erfüllung des SIL 3

Zu bewerten ist die Erfüllung des SIL 3 des Sifa-Systems. Durch redundante Mikrocontroller und galvanisch getrennte Überwachungssignale wird eine hohe Fehlertoleranz und Zuverlässigkeit gewährleistet. Zusätzlich minimieren strenge Qualitätsmanagementprozesse systematische Fehler und unterstützen die SIL 3-Zertifizierung. Zur Nachvollziehbarkeit der SIL-Berechnung ist der Rechenweg in Anhang A, Punkt 9.2, dargestellt.

6.7.1 Identifikation der Komponenten und Ermittlung der Ausfallraten

Zunächst werden die Komponenten und deren Ausfallraten anhand ihrer Datenblätter analysiert. Die relevanten Komponenten innerhalb der Sifa-Systemgrenze sind die zwei Mikrocontroller, die Relais, die Optokoppler und der Taster. Es müssen nicht alle Komponenten SIL3 erreichen, sondern die Sicherheitsfunktion der Sifa im Gesamten. Die Komponente, die

ursächlich für das Versagen der Sicherheitsfunktion der Sifa sein könnte, ist der gleichzeitige Ausfall beider Mikrocontroller bzw. der Relais, die in Reihe zu den Mikrocontrollern geschaltet sind.

In der folgenden Tabelle 9.1 wird die Komponentenliste dargestellt.

Tabelle 6.14: Komponenten und ihre Ausfallraten

Nr.	**Komponent**	**MTTF (hours)**	**Ausfallraten λ (1/h)**	SIL
1	Drucktaster Serie 8442 Ein-(Ein) [46]	833,00	$1,2 \cdot 10^{-3}$	-
2	Arduino UNO R3 [23]	876.000,00	$1,14 \cdot 10^{-6}$	1
3	Arduino Nano[24]	876.000,00	$1.14 \cdot 10^{-6}$	1
4	Optokoppler Al-Zard [29]	833,00	$1,2 \cdot 10^{-3}$	-
5	Relais Siemens [79]	10.000.001,00	$0{,}9999999 \cdot 10^{-7}$	3
5	Relais KY-019RM JOY-IT [54]	Keine Information	Keine Information	-

Die folgende Liste befasst sich mit der Sicherheit jeder Komponente.

- Obwohl der **Sifa-Taster** eine wichtige Rolle für die korrekte Funktionsweise der Sifa spielt, wird dieser in der Berechnung nicht berücksigtig, weil das entwickelte Sifa-System in der Lage ist, beim Selbsttest bzw. bei Ungenauigkeiten in den Taster-Signalen diese Fehler zu bemerken und das System in den Fail-Safe-Modus zu versetzen.
- **Arduino UNO R3 bzw. Arduino Nano:** Arduino gibt keine Ausfallraten für seine Produkte an. Es wird die Ausfallrate des Mikrochip ATmega328 [78], der im Mikrocontroller installiert ist, verwendet. Die Ergebnisse der Zuverlässigkeitsqualifikation zeigen, dass die prognostizierte Ausfallrate für die Datenspeicherung bei weniger als 1 PPM über 20 Jahre bei $85°$C oder 100 Jahre bei $25°$C liegt. Das Versagen aller anderen Peripheriekomponenten wird indirekt durch den anderen Mikrocontroller überwacht. Diese Information ist auf Seite 8 im Datenblatt des ATmega328 [78] zu finden.
- Die **Optokoppler** ermöglichen die galvanische Trennung zwischen den parallelen Kanälen. Versagt ein Kanal, ist das Sifa-System spätestens nach 30 Sekunden im Fail-Safe-Modus.
- **Relais:** Das Datenblatt des im Rapid Prototyping verwendeten Relais zeigt keine Ausfallrate. Zur Berechnung wird die Ausfallrate eines Relais der Marke Siemens [79] verwendet. Im Datenblatt wird ein SIL von 3 angegeben, jedoch keine Ausfallrate. Die Ausfallrate wird konservativ berechnet, wobei der schlechteste MTTF-Wert für SIL 3 von 10.000.001 Stunden gemäß der SIL-Übersetzungstabelle 9.2 verwendet wird. Das Relais von Siemens wurde aus finanziellen Gründen nicht im Rapid Prototype verwendet.

6.7.2 Berechnung der Systemfehlerrate

Für die Berechnung der Systemfehlerrate wird die im Anhang A dargestellte Bestimmung des SILs einer Sicherheitsfunktion verwendet. In der folgenden Abbildung 6.3 wird die Fehlerbaumanalyse - Ausfall der Sifa-Sicherheitsfunktion - dargestellt [6].

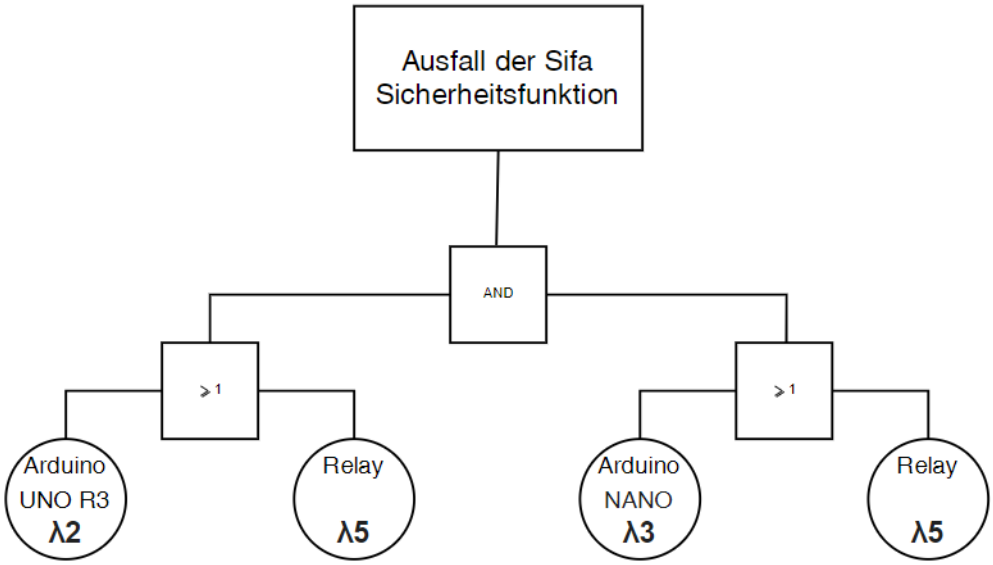


Abbildung 6.3: Fehlerbaumanalyse - Aufall des Sifa-Systems

Die gesamte Zuverlässigkeitszahl ist wie folgt berechnet:

$$R(t) = e^{-(\lambda_2+\lambda_5)t} + e^{-(\lambda_3+\lambda_5)t} - e^{-(\lambda_2+\lambda_3+2\cdot\lambda_5)t} \tag{6.1}$$

$$MTTF_{gesamt} = \int_0^\infty R(t) \cdot \, dx = \frac{1}{\lambda_2+\lambda_5} + \frac{1}{\lambda_3+\lambda_5} - \frac{1}{\lambda_2+\lambda_3+2\cdot\lambda_5} \tag{6.2}$$

Daraus folgt die Mean Time To Failure (MTTF) in Stunden:

$$MTTF_{gesamt} = 1.209.677,43\,h \tag{6.3}$$

Daraus folgt die Tolerable Functional Failure Rate (TFFR) :

$$TFFR = \frac{1}{MTTF_{gesamt}} = \frac{1}{1.313.830,25} = 8,267 \cdot 10^{-7}\,h^{-1} \tag{6.4}$$

Mit den dargestellten Bauteilen wird SIL 2 erreicht, wie in der Tabelle 9.2 zu sehen ist.

6.7.3 SIL3 - Nicht-quantitative Maßnahmen

Um das Safety Integrity Level 3 für eine Sicherheitsfahrschaltung zu erreichen, sind nicht-quantitative Maßnahmen ebenso wichtig wie quantitative Analysen. Diese Maßnahmen konzentrieren sich auf organisatorische, prozessuale und technische Aspekte, die die Zuverlässigkeit und Sicherheit des Systems erhöhen. In der folgenden Tabelle 6.15 werden die berücksichtigten, nicht-quantitativen Maßnahmen dargestellt [6].

Tabelle 6.15: SIL3 - Nicht-quantitative Maßnahmen

Nr.	Beschreibung
1	**Fail-Safe-Mechanismen:** Das System verbleibt in einem sicheren Zustand auch bei Ausfall einer Komponente [6].
2	**Permanente Tastenbetätigung:** Das System ist darauf ausgelegt, eine kontinuierliche Betätigung der Taste zu erkennen und unverzüglich darauf zu reagieren [6].
3	**Einhaltung von Normen:** Das System muss den Sicherheitsnormen gemäß UIC 641 und anderen relevanten Eisenbahnstandards wie der DIN EN 50129 [6] und den TSI [17] entsprechen.
4	**Redundanz:** Das System hat eine redundante Konfiguration, insbesondere in kritischen Bereichen wie der Signalverarbeitung und der Energieversorgung [6].
5	**Common-Cause-Failure:** Der Einsatz einer zweikanaligen, diversitären Mikrocontrollerarchitektur ist erforderlich. Sämtliche Eingänge und Ausgänge müssen dabei von beiden Kanälen evaluiert werden [6].
6	**Selbsttest:** Das System führt einen Selbsttest bei Aktivierung durch, um sicherzustellen, dass alle Komponenten und Funktionen ordnungsgemäß arbeiten. Diese Tests helfen, potenzielle Ausfälle frühzeitig zu erkennen und zu beheben [6].
7	**Fehlererkennung und -management:** Das System ist in der Lage, Fehler zu erkennen und entsprechende Maßnahmen zu ergreifen. Der Ausgangszustand „Fehler“ ist von beiden Kanälen unabhängig lesbar [6].
8	**Dokumentation und Protokollierung:** Alle Vorfälle und Systemzustände sind dokumentiert und protokolliert, um eine nachträgliche Analyse und kontinuierliche Verbesserung des Systems zu ermöglichen [6].
9	**Software:** Die Software hat angemessene Mechanismen implementiert, um die Überwachung des Programmablaufs sicherzustellen [5].
10	**Galvanische Trennung:** Es ist eine galvanische Trennung zwischen den Kanälen durchgeführt, um die Unabhängigkeit der beiden Kanäle sicherzustellen [6].

7 Bewertung und Diskussion

Im siebten Kapitel dieser Arbeit werden die Ergebnisse der Entwicklung und Validierung der Sicherheitsfahrschaltung zusammengefasst und kritisch reflektiert. Abschnitt 7.1 beleuchtet die Herausforderungen, die während des Projekts auftraten, und die Lösungen, die zur Erfüllung der Sicherheitsanforderungen des SIL 3 implementiert wurden. In Abschnitt 7.2 wird ein Ausblick auf zukünftige Entwicklungen und mögliche Erweiterungen des Systems gegeben, um die kontinuierliche Verbesserung und Anpassung an neue technologische und regulatorische Anforderungen zu gewährleisten.

7.1 Herausforderungen und Lösungen

Während der Entwicklung des Sifa-Systems traten mehrere technische und organisatorische Herausforderungen auf, die eine sorgfältige Analyse und innovative Lösungsansätze erforderten. Eine der größten Herausforderungen bestand in der Gewährleistung der Systemzuverlässigkeit unter den strengen Anforderungen der Sicherheitsintegritätsstufe SIL 3.

Um dies zu erreichen, wurde ein redundantes Systemdesign implementiert, das auf zwei parallel arbeitenden Mikrocontrollern basiert. Diese Architektur stellte sicher, dass ein Ausfall eines Mikrocontrollers nicht zu einem vollständigen Systemversagen führte. Es wurden Fail-Safe-Mechanismen verwendet, damit das System in einem sicheren Zustand verbleibt, auch bei Ausfall einer Komponente oder Leitung.

Ein weiteres Problem war die Integration der verschiedenen Überwachungssignale, die durch galvanische Trennung mittels Optokopplern realisiert wurden. Diese Maßnahme minimierte das Risiko von Signalstörungen und erhöhte die Systemstabilität.

Zudem erforderte die Einhaltung der relevanten Normen, insbesondere der DIN EN 50129 [6], eine umfassende Dokumentation und Validierung der Sicherheitsfunktionen. Hierbei halfen systematische Testverfahren und Simulationen, die die Funktionalität und Sicherheit des Systems unter verschiedenen Betriebsbedingungen überprüfen.

Eine Herausforderung bei der Entwicklung des Sifa-Systems bestand darin, Bauteile mit einer möglichst geringen Ausfallrate zu identifizieren und zu integrieren. Die Auswahl solcher

Komponenten ist entscheidend, um die hohen Zuverlässigkeitsanforderungen der Sicherheitsintegritätsstufe SIL 3 zu erfüllen.

Dabei wurden bevorzugt Bauteile eingesetzt, die sich durch eine nachweislich niedrige Ausfallrate und eine hohe Betriebsstabilität auszeichnen. Diese Auswahl trug maßgeblich dazu bei, die Gesamtzuverlässigkeit des Systems zu erhöhen und das Risiko von Systemausfällen signifikant zu reduzieren. Beim Einsatz der Arduino Uno R3 und Arduino Nano mit dem Chip ATmega328 konnte nur SIL 2 erreicht werden. Es wird empfohlen, andere professionellere Mikrocontroller mit einer niedrigeren Ausfallrate zu verwenden.

Durch die Kombination dieser technischen Lösungen und die Unterstützung von den Kollegen des TÜV Nord Systems GmbH & Co. KG konnten die Herausforderungen erfolgreich gemeistert und ein robustes, zuverlässiges Sifa-System entwickelt werden.

7.2 Ausblick

Diese Arbeit hat sich erfolgreich mit der Entwicklung und dem Sicherheitsnachweis eines Sifa-Systems befasst, das die Anforderungen der Sicherheitsintegritätsstufe SIL 3 erfüllt. Durch die Kombination von theoretischer Konzeption und praktischer Implementierung wurde ein umfassender Einblick in die Entwicklung bahntechnischer Sicherheitssysteme geboten. Die wichtigsten Ergebnisse umfassen die erfolgreiche Integration redundanter Mikrocontroller und die Einhaltung relevanter Normen, was die Zuverlässigkeit und Sicherheit des Systems erheblich verbessert.

Der Beitrag dieser Arbeit zur funktionalen Sicherheit in der Bahntechnik liegt in der Schaffung einer Referenzentwicklung, die als Grundlage für zukünftige Projekte dienen kann. Die gewonnenen Erkenntnisse und entwickelten Methoden bieten wertvolle Ansätze zur weiteren Optimierung und Anpassung an neue technologische und regulatorische Anforderungen. Zukünftige Arbeiten könnten sich darauf konzentrieren, die Systemarchitektur weiter zu verfeinern und die Integration neuer Technologien zu erforschen, um die Sicherheit und Effizienz von Bahnsystemen weiter zu steigern.

8 Abkürzungsverzeichnis

CEN Europäisches Komitee für Normung

CENELEC Europäisches Komitee für Elektrotechnische Normung

CSM Common Safety Method

CSM-RA Common Safety Method for Risk Evaluation and Assessmen

DFMEA Design Fehlermöglichkeits- und Einflussanalyse

EBU Eisenbahnunternehmen

EC Europäische Kommission

ERA European Railway Agency

FMEA Fehlermöglichkeits- und Einflussanalyse

FTA Fehlerbaumanalyse

HR High Recommended

ISA Independent Safety Assessment

MTBR Mean Time Between Failures

MTTF Mean Time to Failure

MTTR Mean Time To Repair

NR Not Recommended

PFD Probability of Failure on Demand

PFMEA Prozess Fehlermöglichkeits- und Einflussanalyse

PM Projektmanager

PPM Parts Per Million

R Recommended

RAMS Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (en: Reliability, availability, maintainability and safety)

RFU Recommendation for Use

RPZ Risikopriorität szahl

SFF Safe Failure Fraction

Sifa Sicherheitsfahrschaltung

SIRF Sicherheitsregelung Fahrzeug

SRAC Safety-Related Application Condition

TFFR Tolerable Functional Failure Rate

TNG TÜV Nord Group

TSI Technische Spezifikationen für die Interoperabilität

UIC Internationaler Eisenbahnverband

UML Unified Modeling Language

USB Unabhängiger Sicherheitsbegutachter

VAL Validierer

VER Verifizierer

9 Anhang A: SIL Berechnung

9.1 Kenngrößen der Risiko- und Zuverlässigkeitsanalyse

Die in den Unterkapiteln von Kapitel 9.1 beschriebenen Kenngrößen basieren auf Börcsöks [2] Ausführungen zur Zuverlässigkeit, Ausfallwahrscheinlichkeit, mittleren Lebensdauer, mittleren Instandsetzungszeit, mittleren Brauchbarkeitsdauer und Verfügbarkeit.

9.1.1 Zuverlässigkeit

Die Zuverlässigkeitsfunktion $R(t)$ beschreibt die Wahrscheinlichkeit, dass die Betriebszeit T länger andauert als ein bestimmter Betrachtungszeitraum $(0...t)$ (Verteilungsfunktion der Betriebszeit T bis zum Ausfall). Sie gibt an, mit welcher Wahrscheinlichkeit eine Betrachtungseinheit innerhalb eines Zeitraums von $(0...t)$ funktionsfähig bleibt.

$$R(t) = W(T > t) \tag{9.1}$$

9.1.2 Ausfallwahrscheinlichkeit

Das Komplement der Zuverlässigkeitsfunktion $R(t)$ bildet die Ausfallwahrscheinlichkeit $F(t)$. Die Ausfallwahrscheinlichkeit $F(t)$ gibt an, mit welcher Wahrscheinlichkeit die Betriebszeiten T bis zum Ausfall den vorgegebenen Zeitraum t nicht überschreiten.

$$F(t) = 1 - R(t) = 1 - W(T > t) \tag{9.2}$$

9.1.3 Mittlere Lebensdauer

Laut Börcsök [2] beziehen sich die Begriffe Lebensdauer oder ausfallfreie Arbeitszeit auf die Zeitspanne, in der Betrachtungseinheiten vom Zeitpunkt ihrer Inbetriebnahme bis zu ihrem Ausfall funktionieren. Der Durchschnitt dieser Lebensdauern über alle Betrachtungseinheiten hinweg wird als mittlere ausfallfreie Arbeitszeit, oder Mean Time To Failure $(MTTF)$, bezeichnet. Diese wird aus der Zuverlässigkeitsfunktion $R(t)$ berechnet.

Für eine stetige Zufallsvariable τ, die durch die Dichtefunktion $f(t)$ definiert ist, wird der Erwartungswert (Mittelwert) wie folgt berechnet:

$$E_\tau = \int_{-\infty}^{+\infty} t \cdot f(t)\, dt \tag{9.3}$$

Für eine positive Zufallsgröße, bei der $t > 0$ ist, vereinfacht sich die genannte Gleichung wie folgt:

$$E_\tau = \int_{0}^{\infty} t \cdot f(t)\, dt \tag{9.4}$$

Daher ergibt sich für eine positive Zufallsvariable folgendes:

$$E_\tau = \int_{0}^{\infty} (1 - F(t))\, dt = \int_{0}^{\infty} R(t)\, dt \tag{9.5}$$

Standardmäßig setzt man $R(0) = 1$ voraus. Der auf diese Weise berechnete Mittelwert entspricht dann dem Mittelwert der ausfallfreien Arbeitszeit, der Mean Time To Failure $(MTTF)$. Die Berechnung erfolgt wie folgt:

$$MTTF = E_\tau = \int_{0}^{\infty} R(t)\, dt \tag{9.6}$$

Diese Gleichung ist sowohl für einzelne Bauelemente als auch für komplette Systeme anwendbar und kann ebenso für reparierbare Betrachtungseinheiten genutzt werden, unter der Voraussetzung, dass das System nach einer Reparatur als neuwertig betrachtet wird. Ausgehend von $R(0) = 1$ ergibt sich folgendes:

$$R(t) = e^{-\int_0^t \lambda(x)\, dx} \tag{9.7}$$

Daraus folgt, dass bei einer konstanten Ausfallrate $\lambda(t) = \lambda$ angenommen wird:

$$R(t) = e^{-\lambda \cdot t} \tag{9.8}$$

In diesem Fall entspricht der Mittelwert der ausfallfreien Arbeitszeit:

$$MTTF = \frac{1}{\lambda} \tag{9.9}$$

9.1.4 Mittlere Instandsetzungszeit

Der Mittelwert der Reparaturzeiten t einer Betrachtungseinheit, auch bekannt als $MTTR$ (Mean Time To Repair), lässt sich wie folgt abschätzen:

$$MTTR = \frac{t_1 + t_2 + ... + t_n}{n} \tag{9.10}$$

Dabei sind t_1 bis t_n als die Reparaturzeiten der Komponente zu betrachten.

Analytisch ergibt sich die $MTTR$ aus der Verteilungsfunktion $G(t)$ der Reparaturzeiten.

$$MTTR = \int_0^\infty (1 - G(t))\, dt \tag{9.11}$$

9.1.5 Mittlere Brauchbarkeitsdauer

Die mittlere Brauchbarkeitsdauer, auch bekannt als MTBF (Mean Time Between Failures), definiert die durchschnittliche Zeitspanne zwischen zwei Ausfällen und wird wie folgt berechnet:

$$MTBF = MTTF + MTTR \tag{9.12}$$

Für den Fall:

Im Falle von $MTTF >> MTTR$ kann die Gleichung 9.12 als sehr gute Näherung folgendermaßen formuliert werden:

$$MTBF = MTTF = \frac{1}{\lambda} \tag{9.13}$$

9.1.6 Verfügbarkeit

Die Verfügbarkeit (availability) beschreibt die Wahrscheinlichkeit, dass eine reparierbare Betrachtungseinheit zu einem bestimmten Zeitpunkt t im Zustand „funktionsfähig“ vorliegt. Die mittlere Verfügbarkeit (point availability) wird wie folgt berechnet:

$$PA = \frac{MTTF}{MTTF + MTTR} \tag{9.14}$$

9.2 Bestimmung des SIL einer Sicherheitsfunktion

9.2.1 Identifikation der Komponenten und Ermittlung der Ausfallraten

Im Folgendem wird ein Beispiel für ein System mit Komponenten vorgestellt, die sowohl in Reihe, als auch parallel geschaltet sind. Das Beispiel ist wichtig, um die in Kapitel 6 vorgestellte Berechnung zur Erfüllung des SILs nachzuvollziehen.

In der folgenden Tabelle 9.1 ist die Komponentenliste als Beispiel dargestellt [6].

Tabelle 9.1: Komponenten und ihre Ausfallraten-Beispiel

Nr.	Komponent	MTTF (hours)	Ausfallraten λ (1/h)
1	Komponent 1	MTTF 1	λ_1
2	Komponent 2	MTTF 2	λ_2
3	Komponent 3	MTTF 3	λ_3
4	Komponent 4	MTTF 4	λ_4

9.2.2 Fehlerbaumanalyse des Ausfalls einer Sicherheitsfunktion

Es wird eine Fehlerbaumanalyse durchgeführt, um die wichtigsten Bauteile und ihre Beziehungen zueinander zu identifizieren, die zu einem Ausfall der Sicherheitsfunktion führen könnten. In der folgenden Abbildung 9.1 wird ein Bespiel für eine Fehlerbaumanalyse des Versagens einer Sicherheitsfunktion [6] vorgestellt.

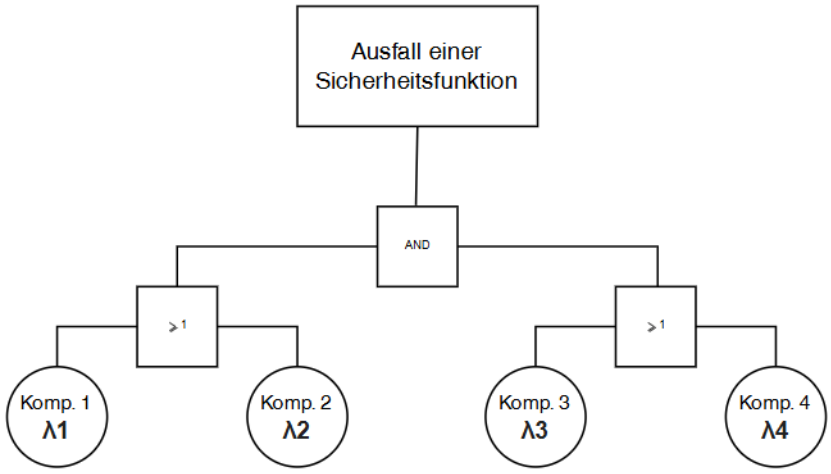


Abbildung 9.1: Fehlerbaumanalyse - Versagen einer Sicherheitsfunktion

9.2.3 Berechnung der gesamten Zuverlässigkeitszahl

Die Formel für die Berechnung der gesamten Zuverlässigkeitszahl $R(t)$ von zwei in Reihe geschalteten Komponenten mit den Ausfallraten λ_1 und λ_2 wird wie folgt kalkuliert:

$$R(t)_{Reihe} = e^{-(\lambda_1+\lambda_2)\cdot t} \tag{9.15}$$

Die Formel für die Berechnung der gesamten Zuverlässigkeitszahl $R(t)$ von zwei parallel geschalteten Komponenten mit den Ausfallraten λ_1 und λ_2 wird wie folgt kalkuliert.

$$R(t)_{Parallel} = e^{-\lambda_1\cdot t} + e^{-\lambda_2\cdot t} - e^{-(\lambda_1+\lambda_2)\cdot t} \tag{9.16}$$

Mit den Gleichungen 9.15 und 9.16 wird die gesamte Zuverlässigkeitszahl der Abbildung 9.1 berechnet.

$$R(t)_{gesamt} = e^{-(\lambda_1+\lambda_2)\cdot t} + e^{-(\lambda_3+\lambda_4)\cdot t} - e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)\cdot t} \tag{9.17}$$

9.2.4 Berechnung MTTF und TFFR

Die Mean Time to Failure wird, wie in der Formel 9.6 dargestelllt ist, berechnet.

$$MTTF_{gesamt} = \int_0^\infty R(t)\cdot\ dx = \frac{1}{\lambda_1+\lambda_2} + \frac{1}{\lambda_3+\lambda_4} - \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_4} \tag{9.18}$$

Daraus folgt die Tolerable Functional Failure Rate (TFFR).

$$TFFR = \frac{1}{MTTF_{gesamt}} \tag{9.19}$$

Ein Gesamtsystem, das in einer SIL-3-Anwendung mit niedrigem Anforderungsmodus verwendet werden soll, muss spezifische Kriterien erfüllen, die in der IEC/EN 61508 [27] festgelegt sind. Die architektonischen Bedingungen sind dabei entscheidend und bestimmen den SIL-Wert des Systems, selbst wenn der berechnete TFFR-Wert einen höheren SIL-Wert nahelegen würde. Diese Bedingungen berücksichtigen die Hardware-Fehlertoleranz sowie das Verhältnis von sicher entdeckbaren zu gefährlich entdeckbaren Fehlern, ausgedrückt durch den SFF-Parameter (Safe Failure Fraction) [2].

In der folgenden Tabelle 9.2 ist die SIL-Einstufung des TFFR-Werts.

Tabelle 9.2: SIL-Einstufung des TFFR-Werts

SIL-Zuordnung	**TFFR** $[h^{^\circ 1}]$
4	$10^{-9} \leq TFFR < 10^{-8}$
3	$10^{-8} \leq TFFR < 10^{-7}$
2	$10^{-7} \leq TFFR < 10^{-6}$
1	$10^{-6} \leq TFFR < 10^{-5}$

Die Safe Failure Fraction (SFF) und die Hardware-Fehlertoleranz sind in der folgenden Tabelle 9.3 dargestellt [2].

Tabelle 9.3: SFF und Hardware-Fehlertoleranz

Safe Failure Fraction (SSF)	0 Fehler	1 Fehler	2 Fehler
$< 60\%$	SIL 1	SIL 2	**SIL 3**
$60\% - < 90\%$	SIL 2	**SIL 3**	SIL 4
$90\% - < 99\%$	**SIL 3**	SIL 4	SIL 4
$> 99\%$	**SIL 3**	SIL 4	SIL 4

10 Anhang B: Arduino-Programmierung

In diesem Teil des Anhangs wird der Code des Zustandsautomaten für die Sicherheitsfahrschaltung vorgestellt. Der Zustandsautomat bildet das Herzstück der Softwarearchitektur und steuert die verschiedenen Betriebszustände der Sifa. Der präsentierte Code zeigt, wie die Zustandsübergänge implementiert sind und welche Logik zur Überwachung der Triebfahrzeugführeraktivität und zur Auslösung von Warn- und Notbremsfunktionen verwendet wird. Diese detaillierte Darstellung bietet Einblicke in die Programmierstruktur und die technischen Überlegungen, die bei der Entwicklung des Systems berücksichtigt werden.

10.1 Pin-Definitionen

In diesem Abschnitt wird der Arduino-Code präsentiert, der die Pin-Definitionen für die Sicherheitsfahrschaltung festlegt. Die Pins sind für die Steuerung und Überwachung des Notbremsssignals, des Sifa-Tasters sowie der Ton- und Lichtsignale zuständig. Zusätzlich wird die Konfiguration für ein LCD-Display definiert, um Systeminformationen anzuzeigen. Diese Struktur ermöglicht eine effiziente Verwaltung der Ein- und Ausgänge des Systems.

```
// Pin-Definitionen
const int notbremse_1 = 13; //Output: Signal zur Notbremse Relay 1
const int notbremse2_Ueberwachung = 12; //Input: Ueberwachung des
    Signals zur Notbremse2 des anderen Mikrocontrollers
const int push1 = 11; // Input: Signal 1 vom Sifa Taster
const int push2_Ueberwachung = 10; //Input: Ueberwachung Signal 2
    vom Sifa Taster
const int tonMelder_1  = 9;  // Output: Tonmelder Signal zu Relay
    Speaker 1
const int lichtMelder_1  = 8;  //Output: Lichtmelder 1 zu Relay
    Licht 1
const int fehlerMelder_1 = 7;  //Output: Fehlermelder 1 zu Relay
    Fehler 1
const int sifa_Aktiv = 6;  //Input:  Sifa ist aktiv wird auf GND
```

```
const int geschwindigkeit = 5;  //Input & Geschwindigket von x km/h
    erreicht, wenn GND
// LCD-Pin-Konfiguration
const int rs = 43, en = 45, d4 = 47, d5 = 49, d6 = 51, d7 = 53;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);
```

Listing 10.1: Pin-Definitionen

10.2 Zeit-Konstanten und Variablen

In diesem Abschnitt wird der Arduino-Code vorgestellt, der die Zeitkonstanten und Zeitvariablen für die Sicherheitsfahrschaltung definiert. Die Zeitkonstanten legen die Dauer für verschiedene Systemzustände fest, darunter die maximale Inaktivitätszeit von 30 Sekunden gemäß UIC641 und die 2,5 Sekunden für LED- und Tonsignale [18]. Die Debounce-Zeit von 50 Millisekunden sorgt für eine zuverlässige Tastererkennung. Die Zeitvariablen lastButtonPressTime, lastButtonPressTimeSifaAktiv und warningStartTime werden verwendet, um die Zeitpunkte der letzten Tasterbetätigung und den Beginn der Warnphase zu speichern.

```
// Zeitkonstanten
const unsigned long MAXIDLETIME = 30000;  // 30 Sekunden UIC-641.
const unsigned long LEDTIME = 2500;   // 2,5 Sekunden
const unsigned long LEDTONTIME = 2500;   // 2,5 Sekunden
const unsigned long DEBOUNCEDELAY = 50;   // 50 Millisekunden
    Debounce-Zeit

// Zeitvariablen
unsigned long lastButtonPressTime = 0;
unsigned long lastButtonPressTimeSifaAktiv = 0;
unsigned long warningStartTime = 0;

// Entprellungsvariablen
unsigned long letzteEntprellZeitPush1 = 0;
unsigned long letzteEntprellZeitNotbremse = 0;
bool letzterPush1Zustand = HIGH;
bool letzterNotbremseZustand = LOW;
```

Listing 10.2: Zeit-Konstanten und Variablen

10.3 Definition der Zustände

In diesem Abschnitt wird der Arduino-Code vorgestellt, der die Zustände der Sicherheitsfahrschaltung definiert. Mithilfe eines *enum* werden die verschiedenen Systemzustände festgelegt, darunter selbsttestZustand, ruheZustand, sifaAktivZustand, sifaInaktivZustand, warningZustand, emergencyBrakeZustand und fehlerDiagnoseZustand. Der initiale Zustand des Systems ist auf selbsttestZustand gesetzt, was den Startpunkt für die Zustandsüberwachung und -steuerung darstellt.

```
// Definition der Zustaende
enum State {
  selbsttestZustand,
  ruheZustand,
  sifaAktivZustand,
  sifaInaktivZustand,
  warningZustand,
  emergencyBrakeZustand,
  fehlerDiagnoseZustand
};
// Initialer Zustand
State currentState = selbsttestZustand;
```

Listing 10.3: Definition der Zustände

10.4 Definition der Variablen für die Fehlerverfolgung

In diesem Abschnitt werden die Variablen für die Fehlerverfolgung der Sicherheitsfahrschaltung definiert. Die Variablen error, errorPush und errorNotbremse überwachen den Fehlerstatus. Hilfsvariablen wie startTest und testFertig steuern Testabläufe. buttonPressTime und isButtonPressed erfassen den Zeitpunkt und Zustand der Tasterbetätigung.

```
// Fehlerstatus
bool error = false;
bool errorPush = false;
bool errorNotbremse = false;
//Hilfsvariablen
bool startTest = false;
bool testFertig = false;


```

```
10 //Zum Fehler Druck dauerhaft
11 unsigned long buttonPressTime = 0; // Zeitpunkt, zu dem der Taster
       gedrueckt wurde
12 bool isButtonPressed = false; // Zustand, ob der Taster gedrueckt
       ist
```

Listing 10.4: Definition Fehlerverfolgung

10.5 Setup

In diesem Abschnitt wird der setup-Code der Sicherheitsfahrschaltung vorgestellt. Hier werden die Pin-Modi für Eingänge definiert. Die Ausgänge werden als OUTPUT definiert und initial auf LOW gesetzt, um sicherzustellen, dass alle Signale zu Beginn deaktiviert sind.

```
1  void setup() {
2    lcd.begin(16, 2);  // Initialisiere das LCD mit 16 Zeichen und 2
         Zeilen
3    lcd.print("System Ready");
4    // Inputs:
5    pinMode(push1, INPUT_PULLUP);
6    pinMode(sifa_Aktiv, INPUT_PULLUP);
7    pinMode(geschwindigkeit, INPUT_PULLUP);
8    pinMode(notbremse2_Ueberwachung, INPUT);
9    pinMode(push2_Ueberwachung, INPUT_PULLUP);
10   // Outputs:
11   pinMode(notbremse_1, OUTPUT);
12   pinMode(tonMelder_1, OUTPUT);
13   pinMode(lichtMelder_1, OUTPUT);
14   pinMode(fehlerMelder_1, OUTPUT);
15   digitalWrite(notbremse_1, LOW);
16   digitalWrite(tonMelder_1, LOW);
17   digitalWrite(lichtMelder_1, LOW);
18   digitalWrite(fehlerMelder_1, LOW);
19 }
```

Listing 10.5: Setup

10.6 Hauptprogramm

In diesem Abschnitt wird das Hauptprogramm der Sicherheitsfahrschaltung vorgestellt. Der loop-Code verwendet eine switch-Anweisung, um den aktuellen Zustand des Systems zu überprüfen und die entsprechende Funktion auszuführen, wie performSelfTest() für den Selbsttest oder handleWarningZustand() für den Warnzustand. Jede Funktion behandelt die spezifischen Anforderungen und Aktionen des jeweiligen Zustands. Am Ende jeder Schleife wird das LCD-Display mit updateLCD() aktualisiert, um den aktuellen Systemstatus anzuzeigen.

```
void loop() {
   entprellenPush1();
   entprellenNotbremse();
  switch (currentState) {
    case selbsttestZustand:
      performSelfTest();
      break;
    case ruheZustand:
      handleRuheZustand();
      break;
    case sifaAktivZustand:
      handleSifaAktivZustand();
      break;
    case sifaInaktivZustand:
      handleSifaInaktivZustand();
      break;
    case warningZustand:
      handleWarningZustand();
      break;
    case emergencyBrakeZustand:
      handleEmergencyBrakeZustand();
      break;
    case fehlerDiagnoseZustand:
      handleFehlerDiagnoseZustand();
      break;
  }
  updateLCD(); // Aktualisiere das LCD
}
```

Listing 10.6: Hauptprogramm

10.7 Entprellung Taster

Entprellen bezieht sich auf eine Technik in der Elektronik und Softwareentwicklung, die dazu dient, unerwünschte Signale oder Störungen zu eliminieren, die durch mechanische Schalter oder Tasten verursacht werden. Wenn ein mechanischer Schalter betätigt wird, kann es zu einem schnellen Hin- und Herwechseln zwischen den Zuständen „ein" und „aus" kommen, bevor sich der Schalter stabilisiert. Dieses Phänomen wird als "Prellen"bezeichnet [75].

```
void entprellenPush1() {
  bool aktuellerPush1Zustand = digitalRead(push1);
  if (aktuellerPush1Zustand != letzterPush1Zustand) {
    letzteEntprellZeitPush1 = millis();
  }
  if ((millis() - letzteEntprellZeitPush1) > DEBOUNCEDELAY) {
    if (aktuellerPush1Zustand == LOW) {
      lastButtonPressTime = millis();
    }
  }
  letzterPush1Zustand = aktuellerPush1Zustand;
}
```

Listing 10.7: Taste Entprellung

10.8 Entprellung Notbremssignal

Um die Ungenauigkeit bei der Synchronisierung der beiden Mikrocontroller auszugleichen, wird ein Entprellungscode für das Notbremssignal entwickelt, das überwacht werden soll.

```
void entprellenNotbremse() {
  bool aktuellerNotbremseZustand = digitalRead(notbremse_1);
  if (aktuellerNotbremseZustand != letzterNotbremseZustand) {
    letzteEntprellZeitNotbremse = millis();
  }
  if ((millis() - letzteEntprellZeitNotbremse) > DEBOUNCEDELAY) {
    //digitalWrite(notbremse_1, HIGH);
    letzterNotbremseZustand = aktuellerNotbremseZustand;
  }
}
```

Listing 10.8: Notbremssignal Entprellung

10.9 Selbsttest-Zustand

Dieser Code führt einen Selbsttest für ein System mit Tastern, LEDs, einem Buzzer und einem Notbremssignal durch. Der Test beginnt, wenn der Taster push1 gedrückt wird. Ein Fehler wird erkannt, wenn die Zustände von push1 und push2_Ueberwachung nicht übereinstimmen. Während des Tests werden der Buzzer und die LEDs für 2000 Millisekunden aktiviert. Das Notbremssignal wird zwischen 2000 und 5000 Millisekunden nach dem Tastendruck aktiviert. Ein Fehler wird erkannt, wenn das Überwachungssignal notbremse2_Ueberwachung nicht HIGH ist, während das Notbremssignal aktiv sein sollte. Nach 5000 Millisekunden wird der Test abgeschlossen. Abhängig vom Fehlerstatus wechselt das System entweder in den ruheZustand oder in den fehlerDiagnoseZustand. Der Code stellt sicher, dass die Komponenten korrekt funktionieren und Fehler während des Tests erkannt werden. In dem folgenden Listing wird der Selbsttest-Zustand dargestellt.

```
1  void performSelfTest(){
2    // Taster-Test
3
4  if (digitalRead(push1) == LOW ){
5    lastButtonPressTime = millis();
6    startTest = true;
7  }
8
9  if ((digitalRead(push1) == HIGH && digitalRead(push2_Ueberwachung)
       == LOW) || (digitalRead(push1) == LOW && digitalRead(
       push2_Ueberwachung) == HIGH)) {
10       errorPush = true;
11       testFertig = true;
12       startTest = false;
13   }
14
15   if ( startTest) {
16     // LED- und Buzzer-Test
17    if(( millis() - lastButtonPressTime   < 2000 )     ){
18     //digitalWrite(tonMelder_1, HIGH);
19     tone(tonMelder_1, 500);
20     digitalWrite(lichtMelder_1, HIGH);
21    }
22   if(( millis() - lastButtonPressTime  > 2000) ){
23     //digitalWrite(tonMelder_1, LOW); //Signal zu Relay K1
```

```
24      noTone(tonMelder_1); //Signal zu Buzzer fuer den Test
25      digitalWrite(lichtMelder_1, LOW);
26      }
27
28      // Fehlererkennung der Notbremssignal
29      if((millis() - lastButtonPressTime   > 2000) &&  (millis() -
            lastButtonPressTime   < 5000)){
30      digitalWrite(notbremse_1, HIGH);
31        }else {
32     digitalWrite(notbremse_1, LOW);
33          }
34
35    if(( millis() - lastButtonPressTime  > 2200) &&  (millis() -
         lastButtonPressTime   < 4800)){
36      if (digitalRead(notbremse2_Ueberwachung) != HIGH) {
37        errorNotbremse = true;
38       testFertig = true;
39      }
40        }
41
42      if((millis() - lastButtonPressTime   > 5000) ){
43      testFertig = true;
44      startTest = false;
45    }
46
47    }
48
49  error = errorPush || errorNotbremse;
50  if(testFertig){
51      if (!error) {
52        currentState = ruheZustand;
53      } else {
54         currentState = fehlerDiagnoseZustand;
55      }
56  }
57
58  }
```

Listing 10.9: Selbsttest-Zustand

10.10 Ruhezustand

Die Funktion handleRuheZustand überwacht den Zustand eines Systems im Ruhezustand. Wenn sowohl sifa_Aktiv als auch geschwindigkeit LOW sind, wechselt das System in den sifaAktivZustand und setzt den Timer zurück, um die Zeitmessung zu starten. Wenn sifa_Aktiv nicht LOW ist, wechselt das System in den sifaInaktivZustand. In dem folgenden Listing wird der Ruhezustand dargestellt.

```
1 void handleRuheZustand() {
2   if (digitalRead(sifa_Aktiv) == LOW && digitalRead(geschwindigkeit)
        == LOW) {
3     currentState = sifaAktivZustand;
4     lastButtonPressTimeSifaAktiv  = millis(); //Damit der Counter
         von 0 Sekunden zu zaehlen anfaengt.
5   } else if (digitalRead(sifa_Aktiv) != LOW) {
6     currentState = sifaInaktivZustand;
7   }
8 }
```

Listing 10.10: Ruhezustand

10.11 Sifa-System Aktiv-Zustand

Die Funktion handleSifaAktivZustand verwaltet den Zustand des Systems, wenn die Sicherheitsfahrschaltung aktiv ist. Wenn der Taster push1 gedrückt wird, wird der Timer zurückgesetzt. Das System wechselt in den warningZustand, wenn die Zeit seit dem letzten Tastendruck die MAXIDLETIME überschreitet. Es kehrt in den ruheZustand zurück, wenn sifa_Aktiv LOW und geschwindigkeit nicht LOW sind. Wenn sifa_Aktiv nicht LOW ist, wechselt das System in den sifaInaktivZustand. Ein Tasterfehler wird erkannt, wenn die Zustände von push1 und push2_Ueberwachung nicht übereinstimmen, was das System in den fehlerDiagnoseZustand versetzt. Die Funktion dauerhaft() wird am Ende aufgerufen, um möglicherweise kontinuierliche Aufgaben auszuführen. In dem folgenden Listing wird der Sifa-System Aktiv-Zustand dargestellt.

```
1 void handleSifaAktivZustand() {
2
3   if (digitalRead(push1) == LOW) {
4     lastButtonPressTimeSifaAktiv  = millis();
5    // startSifaAktiv = true;
```

```
6   }
7
8   //zu Warning
9   if (millis() - lastButtonPressTimeSifaAktiv  > MAXIDLETIME) {
10    currentState = warningZustand;
11    warningStartTime = millis();
12    //startSifaAktiv == false;
13  }
14  //zu Ruhezustand
15  if (digitalRead(sifa_Aktiv) == LOW && digitalRead(geschwindigkeit)
        != LOW) {
16    currentState = ruheZustand;
17   // startSifaAktiv == false;
18  }
19  //Zu Sifa System Inaktiv
20  if (digitalRead(sifa_Aktiv) != LOW) {
21    currentState = sifaInaktivZustand;
22    //startSifaAktiv == false;
23  }
24
25  //Fehler Verfolgung: Taster Fehler
26  if ((digitalRead(push1) == HIGH && digitalRead(push2_Ueberwachung)
        == LOW) || (digitalRead(push1) == LOW && digitalRead(
      push2_Ueberwachung) == HIGH)) {
27      errorPush = true;
28  }
29 error = errorPush;
30  if (error) {
31      currentState = fehlerDiagnoseZustand;
32    //  startSifaAktiv == false;
33
34  }
35 dauerhaft();
36
37 }
```

Listing 10.11: Sifa-System Aktiv-Zustand

10.12 Sifa-System Inaktiv-Zustand

Die Funktion handleSifaInaktivZustand überwacht den Zustand des Systems, wenn die Sicherheitsfahrschaltung inaktiv ist. Wenn das Signal sifa_Aktiv LOW wird, wechselt das System in den ruheZustand. In dem folgenden Listing wird der Sifa-System Inaktiv-Zustand dargestellt.

```
void handleSifaInaktivZustand() {
  if (digitalRead(sifa_Aktiv) == LOW) {
    currentState = ruheZustand;
  }
}
```

Listing 10.12: Sifa-System Inaktiv-Zustand

10.13 Warning-Zustand

Die Funktion handleWarningZustand verwaltet das System, wenn es sich im Warnzustand befindet. Wenn der Taster push1 gedrückt wird, wechselt das System in den sifaAktivZustand, setzt den Timer zurück und deaktiviert den Buzzer und die LEDs. Wenn der Taster nicht gedrückt wird, aktiviert die Funktion die LEDs und den Buzzer in bestimmten Zeitintervallen, basierend auf der verstrichenen Zeit seit warningStartTime. Wenn diese Zeit überschritten wird, wechselt das System in den emergencyBrakeZustand. Falls sifa_Aktiv nicht LOW ist, wird der Buzzer deaktiviert, die LEDs ausgeschaltet, und das System wechselt in den sifaInaktivZustand. Die Funktion überwacht auch mögliche Software- und Tasterfehler. Ein Softwarefehler wird erkannt, wenn die Warnzeit überschritten wird, ohne dass der Zustand gewechselt hat. Ein Tasterfehler wird erkannt, wenn die Zustände von push1 und push2_Ueberwachung nicht übereinstimmen. Bei einem Fehler wechselt das System in den fehlerDiagnoseZustand. In dem folgenden Listing wird der Warning-Zustand dargestellt.

```
void handleWarningZustand() {
 if (digitalRead(push1) == LOW) {
    currentState = sifaAktivZustand;
    lastButtonPressTimeSifaAktiv  = millis(); //Damit der Counter
       von 0 Sekunden zu zaehlen anfaengt.
    //digitalWrite(tonMelder_1, LOW); //Signal zu Relay K1
    noTone(tonMelder_1); //Signal zu Buzzer fuer den Test
    digitalWrite(lichtMelder_1, LOW);
  }else{
     if (millis() - warningStartTime < LEDTIME) {
```

```
10   digitalWrite(lichtMelder_1, HIGH);  }
11      if ((millis() - warningStartTime < LEDTONTIME+LEDTIME)&&(millis
            () - warningStartTime > LEDTIME)) {
12     //digitalWrite(tonMelder_1, HIGH); //Signal zu Relay K1
13     tone(tonMelder_1, 1000);//Signal zu Buzzer fuer den Test
14     digitalWrite(lichtMelder_1, HIGH);  }
15        if (millis() - warningStartTime > LEDTONTIME+LEDTIME) {
16     //digitalWrite(tonMelder_1, LOW); //Signal zu Relay K1
17     noTone(tonMelder_1); //Signal zu Buzzer fuer den Test
18     digitalWrite(lichtMelder_1, LOW);
19     currentState = emergencyBrakeZustand;  }}
20 // Zu Sifa Inaktiv Zustand
21  if (digitalRead(sifa_Aktiv) != LOW) {
22   noTone(tonMelder_1); //Signal zu Buzzer
23     digitalWrite(lichtMelder_1, LOW);
24     currentState = sifaInaktivZustand;  }
25 //Fehler Verfolgung: Software Fehler
26  if ((millis() - warningStartTime > LEDTONTIME+LEDTIME+2000) &&
       currentState == warningZustand ) {
27  noTone(tonMelder_1); //Signal zu Buzzer
28     digitalWrite(lichtMelder_1, LOW);
29  errorWarning =true; }
30 //Fehler Verfolgung: Taster Fehler
31   if ((digitalRead(push1) == HIGH && digitalRead(push2_Ueberwachung)
         == LOW) || (digitalRead(push1) == LOW && digitalRead(
        push2_Ueberwachung) == HIGH)) {
32       errorPush = true;
33     noTone(tonMelder_1); //Signal zu Buzzer
34     digitalWrite(lichtMelder_1, LOW); }
35  error = errorPush || errorWarning;
36   if (error) {
37       currentState = fehlerDiagnoseZustand;
38   } }
```

Listing 10.13: Warning-Zustand

10.14 Emergency-Brake-Zustand

Die Funktion handleEmergencyBrakeZustand steuert das System, wenn es sich im Notbremszustand befindet. Dabei wird das Notbremssignal (notbremse_1) aktiviert. Wenn der Taster push1 gedrückt wird, wird das Notbremssignal deaktiviert und das System wechselt in den ruheZustand. Sollte sifa_Aktiv nicht LOW sein, wird das Notbremssignal ebenfalls deaktiviert und das System wechselt in den sifaInaktivZustand. Die Funktion überwacht auch auf Fehler: Ein Notbremssignalfehler wird erkannt, wenn notbremse_1 HIGH ist, aber notbremse2_Ueberwachung LOW bleibt. Ein Tasterfehler wird erkannt, wenn die Zustände von push1 und push2_Ueberwachung nicht übereinstimmen. Bei einem Fehler wird die Notbremse deaktiviert und das System wechselt in den fehlerDiagnoseZustand. In dem folgenden Listing wird der Emergency-Brake-Zustand dargestellt.

```
1
2  void handleEmergencyBrakeZustand() {
3    digitalWrite(notbremse_1, HIGH);
4     if (digitalRead(push1) == LOW) {
5      digitalWrite(notbremse_1, LOW);
6      currentState = ruheZustand;
7    }
8    // Zu Sifa-System Inaktiv-Zustand
9      if (digitalRead(sifa_Aktiv) != LOW) {
10     digitalWrite(notbremse_1, LOW);
11     currentState = sifaInaktivZustand;
12   }
13   //Fehler Verfolgung: Notbremse Signal Fehler
14     if (digitalRead(notbremse_1)== HIGH && digitalRead(
           notbremse2_Ueberwachung) == LOW && currentState ==
           emergencyBrakeZustand) {
15       errorNotbremse = true;
16     }
17 //Fehler Verfolgung: Sifa-Taster Fehler
18   if ((digitalRead(push1) == HIGH && digitalRead(push2_Ueberwachung)
        == LOW) || (digitalRead(push1) == LOW && digitalRead(
       push2_Ueberwachung) == HIGH)) {
19       errorPush = true;
20   }
21     error = errorNotbremse || errorPush ;
22     if (error) {
```

```
23        digitalWrite(notbremse_1, LOW);
24        currentState = fehlerDiagnoseZustand;
25      }
26  }
```

Listing 10.14: Emergency-Brake-Zustand

10.15 Fehlerdiagnose-Zustand

Die Funktion handleFehlerDiagnoseZustand verwaltet das System, wenn es sich im Fehlerdiagnosezustand befindet. In diesem Zustand werden der Fehleranzeiger (fehlerMelder_1) und das Notbremssignal (notbremse_1) aktiviert. Wenn das Signal sifa_Aktiv nicht LOW ist, werden alle Fehlerindikatoren (error, errorPush, errorNotbremse) sowie die Teststatusvariablen (startTest, testFertig) zurückgesetzt. Das System wechselt dann in den sifaInaktivZustand, und sowohl der Fehleranzeiger als auch das Notbremssignal werden deaktiviert. In dem folgenden Listing wird der Fehlerdiagnose-Zustand dargestellt.

```
1  void handleFehlerDiagnoseZustand() {
2    digitalWrite(fehlerMelder_1, HIGH);
3    digitalWrite(notbremse_1, HIGH);
4
5    if (digitalRead(sifa_Aktiv) != LOW) {
6      error = false;
7      errorPush = false;
8      errorNotbremse =false;
9      startTest =false;
10     testFertig = false;
11     currentState = sifaInaktivZustand;
12     digitalWrite(fehlerMelder_1, LOW);
13     digitalWrite(notbremse_1, LOW);
14   }
15 }
```

Listing 10.15: Fehlerdiagnose-Zustand

10.16 Funktion zur Erkennung des dauerhaften Drückens des Sifa-Tasters

Die Funktion überwacht dauerhaft, ob ein Taster (push1) gedrückt gehalten wird. Sie liest den Tasterzustand und prüft, ob er gedrückt ist (LOW). Wenn der Taster gerade neu gedrückt wurde, wird der Zustand isButtonPressed auf true gesetzt und die aktuelle Zeit gespeichert. Wenn der Taster länger als 2,5 Sekunden gedrückt gehalten wird, wechselt das System in den warningZustand und die Warnzeit wird gespeichert. Sobald der Taster losgelassen wird, wird der Zustand isButtonPressed zurückgesetzt. In dem folgenden Listing wird die Funktion Dauerhaft dargestellt.

```
1  void dauerhaft() {
2    int buttonState = digitalRead(push1); // Liest den Zustand des
       Tasters
3
4    if (buttonState == LOW) { // Ueberprueft, ob der Taster gedrueckt
       ist
5      if (!isButtonPressed) { // Wenn der Taster gerade neu gedrueckt
         wurde
6        isButtonPressed = true; // Setzt den Zustand auf "gedrueckt"
7        buttonPressTime = millis(); // Speichert die aktuelle Zeit
8      } else {
9        if (millis() - buttonPressTime > 2500 ) { // Ueberprueft, ob
           der Taster laenger als 2,5 Sekunden gedrueckt ist
10         currentState = warningZustand;
11         warningStartTime = millis();
12        // startSifaAktiv == false;
13       }
14     }
15   } else {
16     isButtonPressed = false; // Setzt den Zustand zurueck, wenn der
         Taster losgelassen wird
17
18   }
19 }
```

Listing 10.16: Funktion Dauerhaft

10.17 Funktion zur Aktualisierung des LCD-Bildschirms

Die Funktion updateLCD aktualisiert die Anzeige auf einem LCD-Bildschirm basierend auf dem aktuellen Zustand des Systems. Zuerst wird das Display gelöscht und der Cursor auf die erste Zeile gesetzt. Abhängig vom currentState wird eine entsprechende Nachricht auf der ersten Zeile angezeigt, die den aktuellen Systemzustand beschreibt, wie z.B. selbsttest, Ruhe-Zustand oder Emergency-Brake. In der zweiten Zeile werden zusätzliche Informationen angezeigt, die ebenfalls vom currentState abhängen. Zum Beispiel wird die verstrichene Zeit in Sekunden seit einem bestimmten Ereignis angezeigt, wenn das System im selbsttestZustand, sifaAktivZustand oder warningZustand ist. Im emergencyBrakeZustand wird die Nachricht „Drueck Taste" angezeigt, um den Benutzer zur Aktion aufzufordern. Im fehlerDiagnoseZustand wird eine spezifische Fehlermeldung angezeigt, wie „Taste Defekt" oder „Notbremssignal", je nachdem, welcher Fehler erkannt wurde. Im folgenden Listing wird die Funktion zur Aktualisierung des LCD-Bildschirms dargestellt.

```
1
2  void updateLCD() {
3    lcd.clear();
4    lcd.setCursor(0, 0);
5  switch (currentState) {
6      case selbsttestZustand:
7         lcd.print("selbsttest");
8        break;
9      case ruheZustand:
10        lcd.print("Ruhe Zustand");
11       break;
12     case sifaAktivZustand:
13      lcd.print("sifa Aktiv");
14       break;
15     case sifaInaktivZustand:
16      lcd.print("sifa Inaktiv");
17       break;
18     case warningZustand:
19      lcd.print("warning");
20       break;
21     case emergencyBrakeZustand:
22     lcd.print("Emergency Brake");
23       break;
24     case fehlerDiagnoseZustand:
```

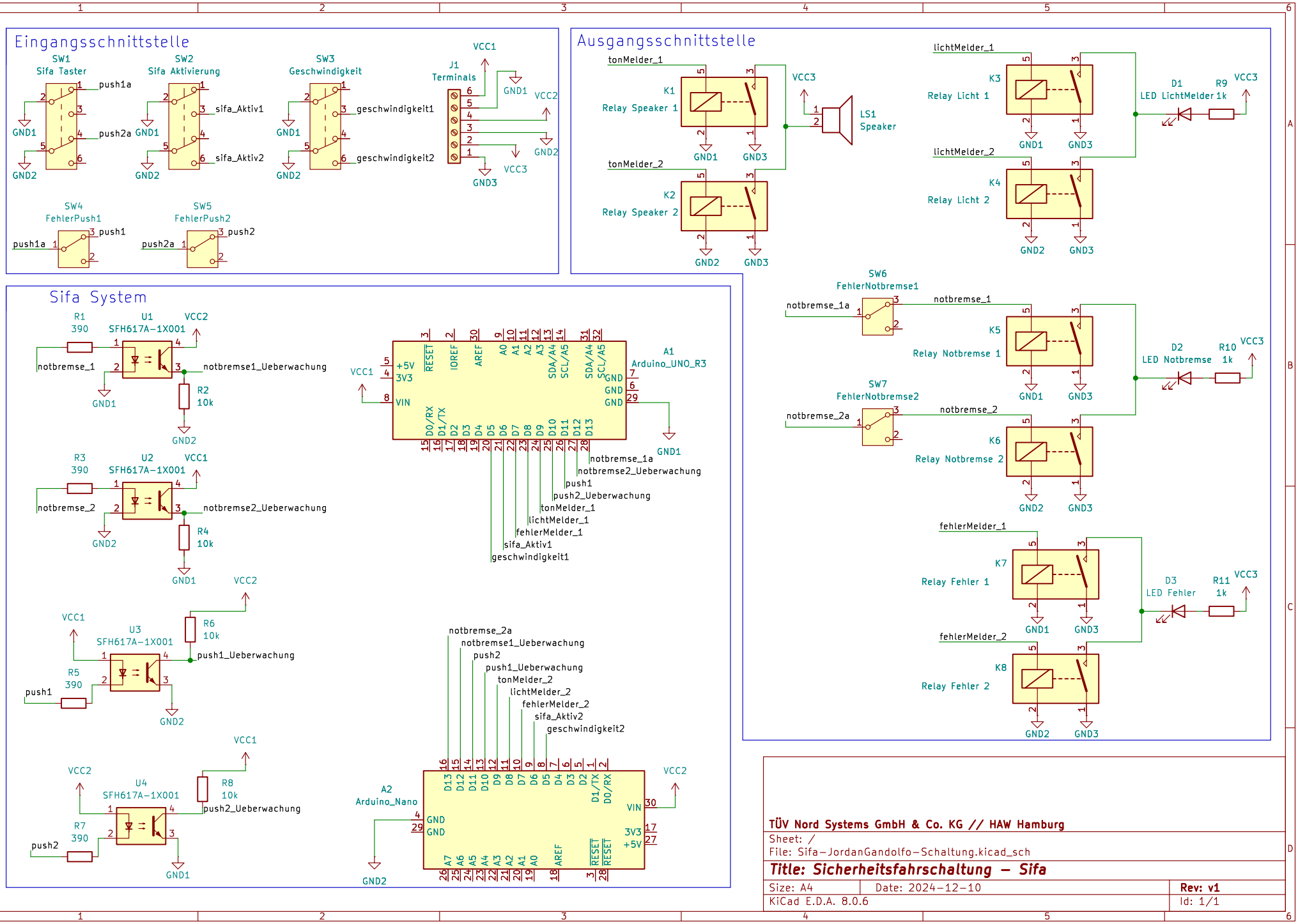
```
25      lcd.print("Fehler Diagnose");
26        break;
27    }
28    lcd.setCursor(0, 1);
29  switch (currentState) {
30      case selbsttestZustand:
31         lcd.print("Time: ");
32         lcd.print((millis() - lastButtonPressTime) / 1000);
33         lcd.print(" sec");
34        break;
35      case ruheZustand:
36         lcd.print("Ruhe");
37        break;
38      case sifaAktivZustand:
39          lcd.print("Time: ");
40         lcd.print((millis() - lastButtonPressTimeSifaAktiv) / 1000);
41         lcd.print(" sec");
42        break;
43      case sifaInaktivZustand:
44        lcd.print("Sifa Inaktiv ");
45        break;
46      case warningZustand:
47         lcd.print("Time: ");
48         lcd.print((millis() - warningStartTime) / 1000);
49         lcd.print(" sec");
50        break;
51      case emergencyBrakeZustand:
52        lcd.print("Drueck Taste  ");
53        break;
54      case fehlerDiagnoseZustand:
55       if(errorPush){lcd.print("Taste Defekt");}
56       else if (errorNotbremse){lcd.print("Notbremssignal");}
57        break;
58    }
59  }
```

Listing 10.17: Funktion LCD Aktualisierung

11 Anhang C: Sicherheitschaltung Zeichnung

In Anhang C werden die Zeichnungen der Sicherheitsfahrschaltung dargestellt.

- Zeichnung des Schaltkreises der Eingangsschnittsstelle, des Sifa-Systems und der Ausgangsschnittstelle.
- Zeichnung der Verbindungen auf der Platine
- 3D Darstellung der Platine


Eingangsschnittstelle
SW1
Sifa Taster
push1a
push2a
GND1
GND2
SW2
Sifa Aktivierung
sifa_Aktiv1
sifa_Aktiv2
SW3
Geschwindigkeit
geschwindigkeit1
geschwindigkeit2
J1
Terminals
VCC1
VCC2
VCC3
GND3
SW4
FehlerPush1
push1
SW5
FehlerPush2
push2
Ausgangsschnittstelle
tonMelder_1
tonMelder_2
K1
Relay Speaker 1
K2
Relay Speaker 2
LS1
Speaker
GND3
lichtMelder_1
lichtMelder_2
K3
Relay Licht 1
K4
Relay Licht 2
D1
LED LichtMelder
R9
1k
SW6
FehlerNotbremse1
notbremse_1a
notbremse_1
K5
Relay Notbremse 1
D2
LED Notbremse
R10
SW7
FehlerNotbremse2
notbremse_2a
notbremse_2
K6
Relay Notbremse 2
fehlerMelder_1
fehlerMelder_2
K7
Relay Fehler 1
K8
Relay Fehler 2
D3
LED Fehler
R11
Sifa System
R1
390
U1
SFH617A-1X001
notbremse_1
notbremse1_Ueberwachung
R2
10k
R3
U2
notbremse_2
notbremse2_Ueberwachung
R4
R5
push1
push1_Ueberwachung
R6
U3
U4
R7
push2
push2_Ueberwachung
R8
A1
Arduino_UNO_R3
A2
Arduino_Nano
TÜV Nord Systems GmbH & Co. KG // HAW Hamburg
Sheet: /
File: Sifa-JordanGandolfo-Schaltung.kicad_sch
Title: Sicherheitsfahrschaltung – Sifa
Size: A4
Date: 2024-12-10
Rev: v1
KiCad E.D.A. 8.0.6
Id: 1/1

In der folgenden Abbildung 11.1 wird die in KiCad Platine-Verbindungen dargestellt.

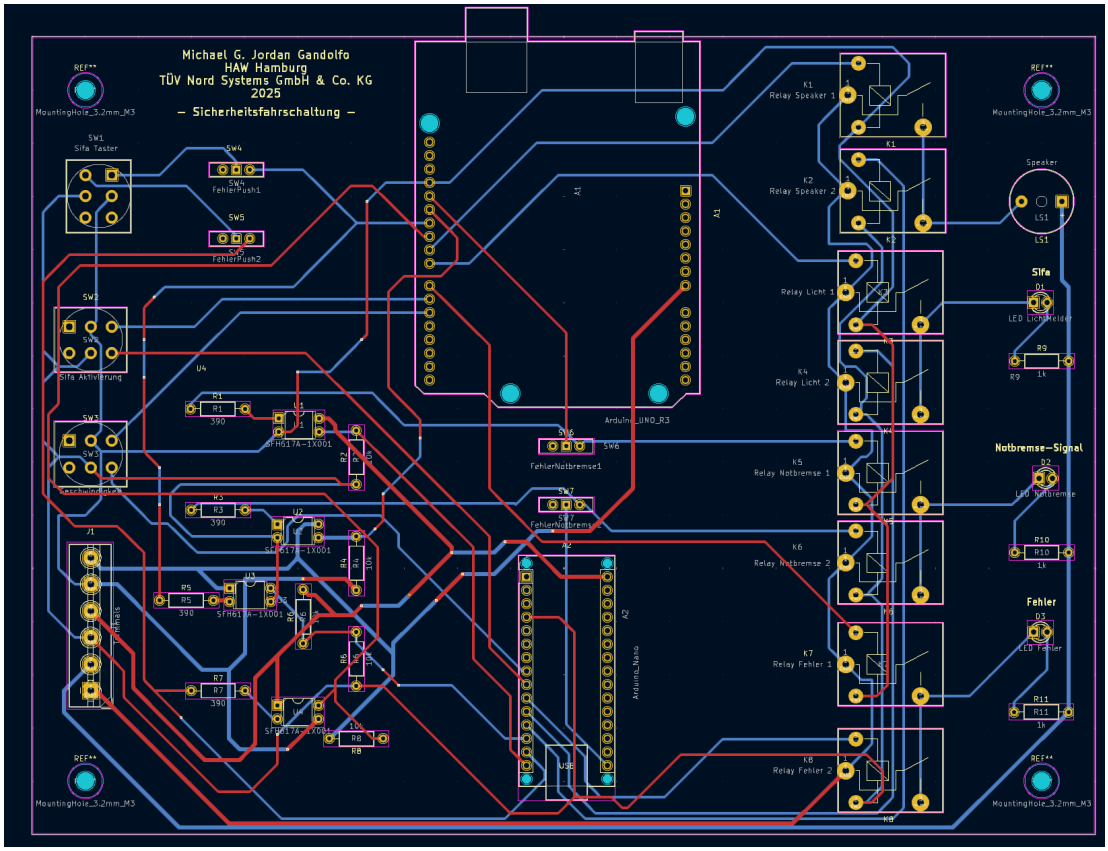


Abbildung 11.1: Platine-Verbindungen

In KiCad werden Verbindungen im Schaltplan-Editor (Eeschema) erstellt, indem zunächst Bauteile platziert werden. Mit dem „Wire“-Werkzeug können Verbindungen zwischen den Anschlüssen der Bauteile gezogen werden. Zur besseren Übersicht können Verbindungen mit dem „Net Label“-Werkzeug benannt werden. Ein „Electrical Rules Check“ (ERC) stellt sicher, dass alle Verbindungen korrekt sind. Abschließend wird eine Netzliste generiert, die im PCB-Layout-Editor für die physische Umsetzung der Verbindungen genutzt wird.

Nach der Verifizierung der korrekten Anschlüsse aller Verbindungen wird in KiCad das 3D-Modell der Platine generiert. Die Platine ist damit bereit für die Fertigung. In der folgenden Abbildung 11.2 wird das in KiCad 3D Modell der Platine dargestellt.

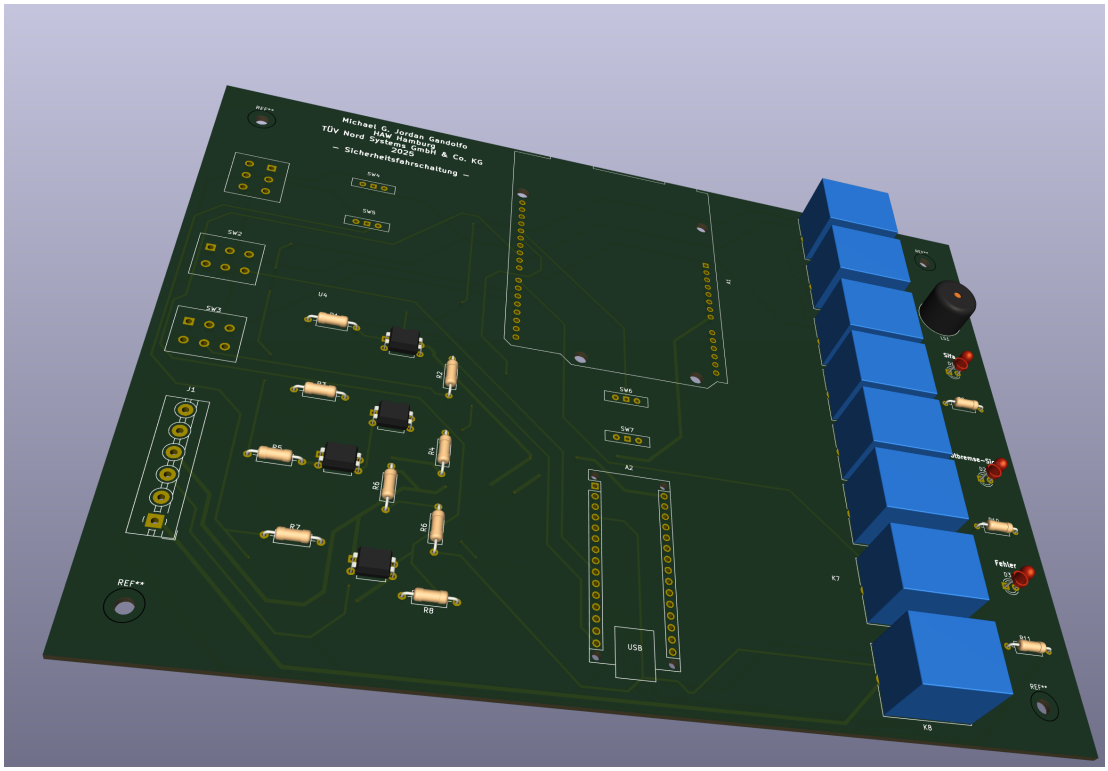


Abbildung 11.2: Platine 3D Darstellung

Literaturverzeichnis

[1] Balzert, H., *Lehrbuch der Softwaretechnik: Basiskonzepte und Requirements Engineering.* Deutschland: Spektrum Akademischer Verlag, 2008

[2] Börcsök, J., *Funktionale Sicherheit Grundzüge sicherheitstechnischer Systeme.* 3., überarbeitete Auflage, Seiten 70-75. Berlin, Deutschland: VDE-Verlag, 2011

[3] DIN EN 50126-1 2018, *Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS-Prozess.* Oktober 2018

[4] DIN EN 50126-2 2018, *Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 2: Systembezogene Sicherheitsmethodik.* Oktober 2018

[5] DIN EN 50128 2020, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme.* 2020

[6] DIN EN 50129 2018, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsbezogene elektronische Systeme für Signaltechnik.* November 2018

[7] DIN EN 50159 2010, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in Übertragungssystemen.* April 2010

[8] Eisenbahnfreunde-Berlin,*Sifa – Die Sicherheitsfahrschaltung.* Dezember 2022 https://www.eisenbahnfreunde-berlin.net/sifa/,
Zugriff: 19.12.2024 um 10:00 Uhr.

[9] Halang, W.A., *Funktionale Sicherheit Echtzeit 2013.* Hagen, Deutschland: Springer Vieweg, 2013

[10] Hanser, E., *Software-Engineering*. Deutschland: Carl Hanser Verlag, 2012

[11] Justram, M., *Safety Integrity Level (SIL): Essentiell für die funktionale Sicherheit*. Oktober 2024. https://www.se-trends.de/safety-integrity-level-sil/,
Zugriff: 10.12.2024 um 16:00 Uhr.

[12] Dinale, L., *Die besten Arduino-Simulatoren (Online & Offline)*. Dezember 2023. https://all3dp.com/de/2/bester-arduino-simulator-online-offline/,
Zugriff: 23.12.2024 um 09:00 Uhr.

[13] Pöting, Dr. S., *Methode zum Festlegen und Nachweisen sicherheitsbezogener Anforderungen und Bewertung der Risiken im Rahmen der Umsetzung der CSM-RA und der EN 50126*. November 2021. https://www.eba.bund.de/SharedDocs/Downloads/DE/Fahrzeuge/Fahrzeugtechnik/Funktionale_Sicherheit/31_SIRF_Sicherheitsregelgung_Fahrzeuge.pdf;jsessionid=CA491E628886976D554F5C965D4FDE6F.live11292?__blob=publicationFile&v=5,
Zugriff: 17.12.2024 um 13:00 Uhr.

[14] Rausch, A., Broy, M., Höhn, R., Schürr, A., *Modellbasierte Entwicklung eingebetteter Systeme*. Deutschland: Springer Verlag, 2010

[15] Stelzer, D., *Software-Entwicklungsmodelle und -methoden*. Deutschland: Springer-Verlag, 2010

[16] TNG - TÜV NORD GROUP , *Funktionale Sicherheit*. Dezember 2023. https://www.tuev-nord.de/de/funktionale-sicherheit/home/,
Zugriff: 08.12.2024 um 09:00 Uhr.

[17] TSI - Technische Spezifikationen für die Interoperabilität, *Bedingungen für VERORDNUNG (EU) Nr. 1302/2014 DER KOMMISSION vom 18. November 2014 über eine technische Spezifikation für die Interoperabilität des Teilsystems „Fahrzeuge — Lokomotiven und Personenwagen“ des Eisenbahnsystems in der Europäischen Union*. November 2014

[18] UIC-Norm 641 2001, *Bedingungen für Sicherheitsfahrschaltungen im internationalen Verkehr*. Februar 2001

[19] Board Uno Rev3 SMD Core ATMega328 https://www.conrad.de/de/p/arduino-a000073-board-uno-rev3-smd-core-atmega328-191789.html?hk=SEM&WT.mc_id=google_pla&hk=SEM&utm_source=google&utm_medium=cpc&utm_campaign=DE+-+PMAX+-+NonBrand+-+HighSeller&utm_id=21937516534&gad_source=1&gbraid=0AAAAAD1-3H6PUgxIgVOXCB9SVK0yfEZLg&gclid=Cj0KCQiA19e8BhCVARIsALpFMgHQ3vmlYANWgKz2qlNmfIxGp5bv1KHODAB6jwZ8QYwcB,
Zugriff: 26.01.2025 um 12:00 Uhr.

[20] Arduino Board Nano Core, Nano ATMega328 https://www.conrad.de/de/p/arduino-a000005-board-nano-core-nano-atmega328-1172623.html?hk=SEM&WT.mc_id=google_pla&utm_source=google&utm_medium=cpc&utm_campaign=DE+-+PMAX+-+Brand+-+All+products&utm_id=21116787988&gad_source=1&gbraid=0AAAAAD1-3H69FV61HNwxBgvwTbEKzT_Df&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGCDxsKW2sg-M4XdpO6CiclFV9X2vCZUjvva_G9ChPYO62bCGbYuPIaAsrOEALw_wcB,
Zugriff: 26.01.2025 um 14:16 Uhr.

[21] Raspberry Pi 4B 2GB 4x1.5 GHz https://www.conrad.de/de/p/raspberry-pi-4-b-2-gb-4-x-1-5-ghz-raspberry-pi-2138863.html?hk=SEM&WT.mc_id=google_pla&hk=SEM&utm_source=google&utm_medium=cpc&utm_campaign=DE+-+PMAX+-+NonBrand+-+HighSeller&utm_id=21937516534&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGsWhW4f4c5Dp-GqPcTQlfoJA9bSz04CEyke8pqH7wcB&refresh=true,
Zugriff: 26.01.2025 um 14:41 Uhr.

[22] Espressif ESP32-DevKitC-VIE https://www.conrad.de/de/p/espressif-esp32-devkitc-vie-entwicklungsboard-esp32-devkitc-vie-24html?hk=SEM&WT.mc_id=google_pla&hk=SEM&utm_source=google&utm_medium=cpc&utm_campaign=DE+-+PMAX+-+NonBrand+-+HighSeller&utm_id=21937516534&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGVbIWyMaKK7-M277BbakEu7-x_

1G5GrJqB9Wf9A0bmo1MdMPhJg_UaAtsbEALw_wcB#productTechData,
Zugriff: 26.01.2025 um 15:02 Uhr.

[23] Arduino UNO R3 https://docs.arduino.cc/resources/datasheets/A000066-datasheet.pdf,
Zugriff: 26.01.2025 um 11:40 Uhr.

[24] Arduino Nano https://docs.arduino.cc/resources/datasheets/A000005-datasheet.pdf,
Zugriff: 26.01.2025 um 13:55 Uhr.

[25] Raspberry Pi 4B https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/,
Zugriff: 26.01.2025 um 14:30 Uhr.

[26] ESP32 https://asset.conrad.com/media10/add/160267/c1/-/gl/002490159DS00/datenblatt-2490159-espressif-esp32-devkitc-vie-er
pdf,
Zugriff: 26.01.2025 um 14:50 Uhr.

[27] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).* 2010

[28] DIN EN 61508, *Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer Systeme.* Februar 2011

[29] Optokoppler. Computer Weekly. https://www.computerweekly.com/de/definition/Optokoppler,
Zugriff: 26.01.2025 um 16:10 Uhr.

[30] Digitale Isolatoren. Texas Instruments. https://www.ti.com/de-de/isolation/digital-isolators/overview.html,
Zugriff: 26.01.2025 um 16:20 Uhr.

[31] Isolierte DC-DC-Wandler. Bicker. https://www.bicker.de/produkte/dcdc-wandler?gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgHVPbQAwMelcu1hLtiidbduM_ScEEEqA5F0Soo-0_uQzsmbxER_Z8waAsdQEALw_wcB&nbnet=0#,
Zugriff: 26.01.2025 um 16:35 Uhr.

[32] Transformator (Übertrager). Bicker. https://www.chemie.de/lexikon/%C3%9Cbertrager.html,
Zugriff: 26.01.2025 um 17:10 Uhr.

[33] Relais https://www.elektronik-kompendium.de/sites/bau/0207211.htm,
Zugriff: 26.01.2025 um 17:40 Uhr.

[34] Optokoppler Reichelt. https://www.reichelt.de/de/de/shop/produkt/1-fach_optokoppler_5kv_35v_50ma_200-400_dip-4-312476?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGaDpVjS2CbHro6eTZG7CXnCfE5md12F1fAx2_CueN2CNao0lHUcy4aAlVwEALw_wcB,
Zugriff: 26.01.2025 um 17:50 Uhr.

[35] Funduino Optokoppler NPN 4-Kanal. https://funduinoshop.com/bauelemente/taster-und-schalter/optokoppler/optokoppler-npn-4-kanal-modul-dst-1r4p-n,
Zugriff: 26.01.2025 um 17:55 Uhr.

[36] Digitaler Isolator, 8-Kanal, DIL-20 Reichelt. https://www.reichelt.de/de/de/shop/produkt/digitaler_isolator_8-kanal_dil-20-19198?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgHJJIwqZy4corFPBidAQChFfIGCMmNQnqXd5mLmB_jv5Oq155_RbMYaAq1VEALw_wcB,
Zugriff: 26.01.2025 um 18:10 Uhr.

[37] DC/DC-Wandler TEA 1, 1 W, 4,5-5,5/5,0 VDC, SIL-4. Reichelt https://www.reichelt.de/de/de/shop/produkt/dc_dc-wandler_tea_1_1_w_4_5-5_5_5_0_vdc_sil-4-288651?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgEZE_0pzFXRb5kvgiaeekyhx9o5Ek0Y9iqg2EKDtWny3GnbUfguUN0aAsiNEALw_wcB,
Zugriff: 26.01.2025 um 18:23 Uhr.

[38] DC/DC Converter https://cdn-reichelt.de/documents/datenblatt/C700/TEA1-0505_DB_EN.pdf,
Zugriff: 26.01.2025 um 17:04 Uhr.

[39] NF-Überträger, 1:6, RM 10 x 12,5 mm Reichelt https://www.reichelt.de/de/de/shop/produkt/nf-_ebertraeger_1_6_rm_10_x_12_5_mm-73040?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgFygeZzeJ8itV12gEQI_JDRfYOJ5A7Nl__k_b9wtI3LfdKOfRxGKUoaAl3_EALw_wcB,
Zugriff: 26.01.2025 um 19:15 Uhr.

[40] Relais Omron Electronics G5V-2-H1-DC6 https://www.mouser.de/ProductDetail/Omron-Electronics/G5V-2-H1-DC6?qs=B3tblJ0Nlt9Fq9cdt%2FZUvQ%3D%3D&mgh=1&vip=1&utm_id=20979042628&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGKd9vg8KutKRn7Lo7lH9SrxKRdfkCHvkHhLRpWFUoZgKzA9hqkaAg75EALw_wcB,
Zugriff: 26.01.2025 um 19:28 Uhr.

[41] Miniatur-Kippschalter, EIN-AUS-EIN, 3 A / 250 V Datenblatt https://cdn-reichelt.de/documents/datenblatt/C200/10022_PRODUKT-DATENBLATTPRODUCTDATASHEET.pdf,
Zugriff: 26.01.2025 um 19:49 Uhr.

[42] Miniatur-Kippschalter, EIN-AUS-EIN, 3 A / 250 V https://www.reichelt.de/de/de/shop/produkt/kippschalter_0_4a-20vac_2x_ein-ein_printanschluss-4401?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgFZivy3Cc1B3uIQyzOf657gsMfdQaFKTBT92487c_SlIwc2lS7Y3rYaAhSkEALw_wcB,
Zugriff: 26.01.2025 um 19:49 Uhr.

[43] Mini Kippschalter https://www.amazon.de/MTS-202-Terminals-Positionen-Kippschalter-wasserdichte/dp/B07JNV6SCJ/ref=asc_df_B07JNV6SCJ?mcid=462cb730becd38e2b91bd258cbe97e8a&th=1&tag=googshopde-21&linkCode=df0&hvadid=696950088603&hvpos=&hvnetw=g&hvrand=14891727617670197152&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9116741&hvtargid=pla-691898179607&gad_source=1,
Zugriff: 26.01.2025 um 20:10 Uhr.

[44] Kippschalter Datenblatt https://www.mouser.de/datasheet/2/140/100DP1T1B1M53QEH-3447408.pdf,
Zugriff: 26.01.2025 um 20:18 Uhr.

[45] Kippschalter https://www.mouser.de/ProductDetail/E-Switch/100DP1T1B1M53QEH?qs=f57gQzlyLiqA8Uf1TAc2Bg%3D%3D&mgh=1&vip=1&utm_id=20979042634&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgHRVDvg0YhPEvKQVGmdDc2Hq-eLBrrDJTeVakV-QCwcB,
Zugriff: 26.01.2025 um 20:20 Uhr.

[46] Drucktaster Richelt 2 Pollig Datenblatt https://cdn-reichelt.de/documents/datenblatt/C200/11-SERIE_8000-D.pdf,
Zugriff: 26.01.2025 um 20:45 Uhr.

[47] Drucktaster Richelt 2 Pollig https://www.reichelt.de/de/de/shop/produkt/drucktaster_3a-250vac_2x_ein_printstifte-105688?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgE_fXAmhieI54KxfemG-med6Gp6EHd6tNdzRfc-lTkaX9X0OT9x8c4aAvWoEALw_wcB,
Zugriff: 26.01.2025 um 20:47 Uhr.

[48] Drucktaster Cliff 2 Pol Datenblatt https://cdn-reichelt.de/documents/datenblatt/C200/CLIFF-FC71XX_DB-EN.pdf,
Zugriff: 26.01.2025 um 20:58 Uhr.

[49] Drucktaster Cliff 2 Pol https://www.reichelt.de/de/de/shop/produkt/druckschalter_2_pol_ein-_aus_250_v_ac_1_a-227750?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgHcau7MIFgGthPYu3ri8m8J2E1Cz3NzxO-td97oYk6yoaAsdEEALw_wcB,
Zugriff: 26.01.2025 um 21:00 Uhr.

[50] Vandalismusgeschützter Drucktaster Datenblatt https://asset.re-in.de/add/160267/c1/-/en/000701943DS00/DA_TRU-Components-701943-LAS2GQF-22-S-P-Vandalismusgeschuetzter-Druck.pdf,
Zugriff: 26.01.2025 um 21:15 Uhr.

[51] Vandalismusgeschützter Drucktaster https://www.voelkner.de/products/73413/TRU-Components-701943-LAS2GQF-22-S-P-Vandalismusges.html?ref=11&offer=625217953959b65ca7793a6ee780dc23&utm_source=billiger&utm_medium=CPC&utm_campaign=D79012&utm_content=intern&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgEKNXupLWoDoZmEkMmWjALQ4_bhSOpAr-_roHO5ud58l-3RZsSuqzoaAlUlEALw_wcB,
Zugriff: 26.01.2025 um 21:19 Uhr.

[52] TÜV SÜD, *ABOUT FUNCTIONAL SAFETY*. o.D. https://www.tuvsud.com/en-us/services/functional-safety/about,
Zugriff: 26.01.2025 um 21:25 Uhr.

[53] Relay KY-019RM Datenblatt https://cdn-reichelt.de/documents/datenblatt/A300/COM-KY019RM_DATASHEET_2024-05-13.pdf,
Zugriff: 26.01.2025 um 21:35 Uhr.

[54] Relay KY-019RM https://www.reichelt.de/de/de/shop/produkt/entwicklerboards_-_relais-modul_5_v_srd-05vdc-sl-c-239148?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGMHAh2N6_bVGLoIVJKiFkAb-JqCY1XZhUfuqoqOYDRiof3ZAgEjXMaAqG3EALw_wcB,
Zugriff: 26.01.2025 um 21:38 Uhr.

[55] KF-301 1-Relais 5V Modul Datenblatt https://cdn.shopify.com/s/files/1/1509/1638/files/KF-301_1-Relais_Modul_Datenblatt_AZ-Delivery_Vertriebs_GmbH_2fbfb0f0-d405-4fd8-b04e-1c3ae81a242f.pdf?v=1646995909,
Zugriff: 26.01.2025 um 21:55 Uhr.

[56] KF-301 1-Relais 5V Modul https://www.az-delivery.de/products/kf-301-relais-modul-mit-low-level-trigger?variant=19481728581728&utm_source=google&utm_medium=cpc&utm_campaign=16964979024&utm_content=166733588295&utm_term=&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgEzmntvEMVp36bEqGECW2FdHoSwQpbO2Zcv1qTjzA

wcB,
Zugriff: 26.01.2025 um 21:58 Uhr.

[57] Two-pole Relays Datenblatt https://www.mouser.de/datasheet/2/307/en_g5v_2-3476498.pdf,
Zugriff: 26.01.2025 um 22:10 Uhr.

[58] KF-301 1-Relais 5V Modul https://www.az-delivery.de/products/kf-301-relais-modul-mit-low-level-trigger?variant=19481728581728&utm_source=google&utm_medium=cpc&utm_campaign=16964979024&utm_content=166733588295&utm_term=&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgEzmntvEMVp36bEqGECW2FdHoSwQpbO2Zcv1qTjzA
wcB,
Zugriff: 26.01.2025 um 22:13 Uhr.

[59] LED bedrahtet Datenblatt https://cdn-reichelt.de/documents/datenblatt/A500/383-2SDRD-S530-A3_ENG_TDS.pdf,
Zugriff: 26.01.2025 um 22:25 Uhr.

[60] LED bedrahtet https://www.reichelt.de/de/de/shop/produkt/led_5_mm_bedrahtet_gelb_3_2_mcd_60_-21629?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgFrwJ3Q-X5tBI30iAuq8JN7Jw-CW8Goy3BGtm3Vpl
wcB,
Zugriff: 26.01.2025 um 22:27 Uhr.

[61] LED bedrahtet Datenblatt https://www.mouser.de/datasheet/2/723/HB_C5SMF_RJF_RJE_GJF_GJE_BJF_BJE-3402153.pdf,
Zugriff: 26.01.2025 um 22:25 Uhr.

[62] LED bedrahtet https://www.mouser.de/ProductDetail/Cree-LED/C5SMF-RJE-CT0W0BB2?qs=1sbE9T7hb3bz%2FXMFB8lsHw%3D%3D&mgh=1&vip=1&utm_id=20979042628&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgGRfmw_U1vEeJQYq9xie5hWdX4s9SRc3FUL1du8U1QrDwhHu8VtCm8aAiuJEALw_
wcB,
Zugriff: 26.01.2025 um 22:27 Uhr.

[63] Buzzer CUI Devices Datenblatt https://cdn-reichelt.de/documents/datenblatt/A900/CMI-1295-0585T.pdf,
Zugriff: 26.01.2025 um 22:35 Uhr.

[64] Buzzer CUI Devices https://www.reichelt.de/de/de/shop/produkt/buzzer_85db_2300_hz_5_v-360835?PROVID=2788&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgFPcKWWyKRKXtDJj3y9YwNNjcYgj_RxUeqO0kCJaAmFji7dZUTu8r4aAhsLEALw_wcB,
Zugriff: 26.01.2025 um 22:38 Uhr.

[65] Miniatur Summer Geräusch-Entwicklung Datenblatt https://asset.re-in.de/add/160267/c1/-/en/001511468DS01/DA_93038c213a-Miniatur-Summer-Geraeusch-Entwicklung-85-dB-Spannung-5-pdf,
Zugriff: 26.01.2025 um 22:50 Uhr.

[66] Miniatur Summer Geräusch-Entwicklung https://www.voelkner.de/products/985784/93038c213a-Miniatur-Summer-Geraeusch-Entwicklung-8html?ref=11&offer=e22b15b3c48280411434e2b2669c2d79&utm_source=billiger&utm_medium=CPC&utm_campaign=S991861&utm_content=intern&gad_source=1&gclid=Cj0KCQiA19e8BhCVARIsALpFMgF-CHDOGN_6NAIukx8vuibDDWJDZp5hU_UyZL3BVFp81vjNpBpDP9UaAiBXEALw_wcB,
Zugriff: 26.01.2025 um 22:55 Uhr.

[67] Kumar, S., *Common cause failures and dependency modeling in single and multiunit NPP sites*. ScienceDirect. 2023. https://www.sciencedirect.com/topics/engineering/common-cause-failure,
Zugriff: 29.01.2025 um 14:00 Uhr.

[68] Joy-it com-lcd 16x2 Display https://www.conrad.de/de/p/joy-it-com-lcd-16x2-display-modul-6-6-cm-2-6-zoll-16-x-4-pixel-pahtml?refresh=true,
Zugriff: 30.01.2025 um 19:21 Uhr.

[69] Datenblatt Potentiometer https://www.conrad.de/de/p/alpha-rv16af-20-15k-b50k-rv16af20kb50km-dreh-potentiometer-mono-20

html?hk=SEM&WT.mc_id=google_pla&utm_source=
google&utm_medium=cpc&utm_campaign=DE+-+PMAX+
-+Nonbrand+-+Active+&+Passive+Components=
&utm_id=17939114814&gad_source=1&gclid=
Cj0KCQiA4-y8BhC3ARIsAHmjC_FsvySj1u94THCBZaie48BRNst_
J5ngsm3dS89LySu1fdu48N6s2-kaAoQ_EALw_wcB,
Zugriff: 30.01.2025 um 19:21 Uhr.

[70] DIN EN 50125 2014, *Bahnanwendungen – Umweltbedingungen für Betriebsmittel - Teil 1: Betriebsmittel auf Bahnfahrzeugen* November 2014

[71] KVP Institut GmbH, *FMEA – Fehlermöglichkeits- und -Einflussanalyse.* https://www.kvp.de/lexikon/fmea/, Januar 2013.
Zugriff: 31.01.2025 um 10:53 Uhr.

[72] Werdich, M., *FMEA - Einführung und Moderation.* https://www.google.de/books/edition/FMEA_Einf%C3%BChrung_und_Moderation/ar7EqdRRP44C?hl=de&gbpv=1&printsec=frontcover, Januar 2025.
Zugriff: 31.01.2025 um 12:00 Uhr.

[73] Safety Culture, *Fehlerbaumanalyse (FTA): Definition, Erklärung und Vorgehen.* https://safetyculture.com/de/themen/fehlerbaumanalyse/, Januar 2025.
Zugriff: 31.01.2025 um 12:30 Uhr.

[74] Proto-Electronics, *Top 10 der besten Software für die Entwicklung von Leiterplatten.* https://www.proto-electronics.com/de/blog/top-10-der-besten-softwareprogramme-entwicklung-von-leiterplatten, Januar 2025.
Zugriff: 01.02.2025 um 13:12 Uhr.

[75] , Günther, Jena *Tastenentprellung.* https://www.semiversus.com/dic/hardwarenahe_programmierung/tastenentprellung.html, Dezember 2024.
Zugriff: 02.02.2025 um 11:31 Uhr.

[76] TÜV-SÜD, *WHAT IS A RAILWAY INDEPENDENT SAFETY ASSESSMENT (ISA)?.* https://www.tuvsud.com/en/industries/infrastructure-and-rail/

rail/independent-safety-assessment.
Zugriff: 04.02.2025 um 21:12 Uhr.

[77] DIN EN ISO 9001,*Qualitätsmanagementsysteme - Anforderungen.* November 2015

[78] ATmega328 8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf,
Zugriff: 26.01.2025 um 13:58 Uhr.

[79] Datenblatt Relais Siemens 3sk1111-1AB30 https://docs.rs-online.com/a837/0900766b817035a4.pdf,
Zugriff: 29.01.2025 um 08:58 Uhr.

[80] Dattenblatt Optokoppler Reichelt. https://cdn-reichelt.de/documents/datenblatt/A500/EL817-EVL.pdf,
Zugriff: 26.01.2025 um 17:55 Uhr.

[81] IEC 61511, *Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie.* Februar 2019

Hiermit versichere ich, dass ich die vorliegende Arbeit im Sinne der Prüfungsordnung nach §16(5) APSO-TI-BM/APSO-INGI ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen habe ich unter Angabe der Quellen kenntlich gemacht.

Hamburg, 14. Februar 2025 Michael Gustav Jordan Gandolfo