CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Evaluating Component Reliability in Safety Applications through Failure Analysis

Master's thesis in Embedded Electronic System Design

Kaushik Krishnamurthy
Lakshmi Narasimhan Venkata Ramanan

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2023

Master's thesis 2023

Evaluating Component Reliability in Safety Applications through Failure Analysis

Kaushik Krishnamurthy
Lakshmi Narasimhan Venkata Ramanan

UNIVERSITY OF
GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2023

Evaluating Component Reliability in Safety Applications through Failure Analysis
Kaushik Krishnamurthy
Lakshmi Narasimhan Venkata Ramanan

Supervisor: Lena Peterson, Department of Computer Science and Engineering, Chalmers University of Technology
Company advisor: Marcin Janiszewski, Volvo Cars
Examiner: Per Larsson-Edefors, Department of Computer Science and Engineering, Chalmers University of Technology

Master's Thesis 2023
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Typeset in LaTeX
Gothenburg, Sweden 2023

Evaluating Component Reliability in Safety Applications through Failure Analysis
Kaushik Krishnamurthy
Lakshmi Narasimhan Venkata Ramanan
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

This master's thesis project addresses the critical role of component reliability in safety-critical system design, filling a substantial gap in existing research. It investigates a specific power distribution scenario presented by Volvo Cars, focusing on mitigating reverse current flow between two power supplies. Two design approaches are considered: one featuring an ISO 26262 non-compliant ideal-diode controller (LM74700) and the other incorporating a compliant alternative (STPM801). The study assesses the impact of component reliability through failure-analysis techniques, such as, failure modes, effects, and diagnostic analysis (FMEDA) and fault tree analysis (FTA), which calculates key safety hardware metrics per ISO 26262 — single point fault metric (SPFM), latent fault metric (LFM), and probabilistic metric for random hardware failure (PMHF). Findings indicated that the LM74700 resulted in a less reliable system in context of latent faults when compared with the system that used STPM801.

While the non-compliant indicated to be less reliable due to lack of internal safety mechanisms, the rationale for choosing non-compliant components over compliant ones hinges on the specific application's needs, considering complexity, ISO 26262 compliance, and design flexibility. The insights in this thesis project provide valuable guidance for engineers and stakeholders grappling with the intersection of safety and hardware design. Future research directions encompass comparisons between non-compliant designs with external safety mechanisms and practical verification tests to bridge theoretical and empirical outcomes, facilitating practical applications in safety engineering.

Keywords: ISO 26262, hardware circuit design, functional safety, safety analysis, failure analysis, SPFM, LFM, PMHF, FMEDA, FTA

Acknowledgements

We extend our heartfelt appreciation to the individuals who have played a pivotal role in the completion of this master's thesis. Their support, guidance, and contributions have been instrumental in shaping this research endeavor.
We are very grateful to our thesis supervisor, Prof. Lena Peterson. Her expertise, mentorship, and valuable feedback has greatly enriched the quality of this thesis. Her commitment to academic excellence has been very inspiring. We also wish to express our sincere gratitude to Prof. Per Larsson-Edefors, our thesis examiner from the Department of Embedded Electronic System Design at Chalmers University. His evaluation and insightful suggestions have significantly elevated the thoroughness of this work.
We extend our thanks to Marcin Janiszewski, our master thesis supervisor at Volvo Cars, whose industry insights and guidance have provided a practical dimension to our research. His support has bridged the gap between academia and real-world applications. Furthermore, we would like to acknowledge the constant support of David Martin Gonzalez, from Volvo Cars. His assistance and engagement have been invaluable throughout this journey. We especially would like to thank our manager, Ronny Hallberg, for providing the opportunity to do this thesis project at Volvo Cars.
To all our mentors, colleagues, friends, and families who have stood by us, we express our gratitude for your unwavering encouragement and belief in our capabilities. This collaborative thesis is a reflection of our collective effort, and we sincerely thank these exceptional individuals for their guidance, insights, and encouragement.

Kaushik Krishnamurthy
Lakshmi Narasimhan Venkata Ramanan

Gothenburg, October 2023

List of Abbreviations

AEB - Automotive Emergency Brakes

ASIL - Automotive Safety Integrity Level

BOM - Bill of Materials

CFI - Conditional Failure Intensity

DFA - Dependent Failure Analysis

E/E - Electrical and Electronic

ECU - Electronic Control Unit

EMI - Electromagnetic Interference

FMEA - Failure Mode and Effects Analysis

FIT - Failure-in-Time

FFI - Freedom from Interference

FMEDA - Failure Mode, Effect and Diagnostic Analysis

FSC - Functional safety Concept

FTA - Fault Tree Analysis

HARA - Hazard and Risk Analysis

HSI - Hardware Software Interface

IEC - International Electrotechnical Commission

ISO - International Organisation for Standardisation

LFM - Latent Fault Metric

MCU - Microcontroller Unit

MOSFET - Metal-oxide Field Effect Transistor

MPF - Multiple Point Fault

MTBF - Mean Time Between Failures

OEM - Original Equipment Manufacturers

PFD - Probability of Failure-in-demand

PCB - Printed Circuit Boards

PMHF - Probabilistic Metrics for Random Hardware Failures

QM - Quality Managed

RF - Residual Fault

SEooC - Safety Element out of Context

SIL - Safety Integrity Level

SN - Siemens Norm

SPF - Single Point Fault

SPFM - Single Point Fault Metric

TSA - Technical Safety Architecture

TSR - Technical Safety Requirement

TSC - Technical Safety Concept

TVS - Transient-voltage-suppression

VCC - Volvo Cars Corporation

ZC - Zone Controller

Contents

1

Introduction

The advancements in automotive technologies in the recent past have resulted in vehicles becoming increasingly complex with their interconnected systems and automation [1]. As the dependence on technology grows further, the importance of the safety and reliability of the vehicle is more relevant now than ever before, particularly with the vast amount of electrical and electronic (E/E) systems used to determine the functional behavior of the vehicle. Any issue or failure in these electronic systems can potentially lead to a hazardous situation for the driver and the passengers. To tackle this problem, many safety mechanisms have been put in place from safety belts to airbags, anti-lock braking systems, automatic emergency brakes and so on. Even with these technologies in place, close to 1.3 million casualties occur annually due to automobile accidents [2]. The discussion on improving safety standards for automotive vehicles led to the International Organisation for Standardization (ISO) to officially release the road vehicles functional-safety standard ISO 26262 in 2011 and a second edition followed in the year 2018 [3].

ISO 26262 is an international standard for the functional-safety of E/E systems in road vehicles. The standard defines the safety life-cycle of electronic systems in vehicles, including hazard and risk analysis, safety requirements specification, design and implementation, verification and validation and, production and operation. It also specifies the roles and responsibilities of different stakeholders involved in the development process, including the original equipment manufacturers (OEMs), suppliers, and engineering service providers. It aims to ensure that electronic systems in vehicles are designed and tested to meet specific safety requirements, including the prevention of accidents and minimising the risks of injury or damage in the event of an accident.

ISO 26262 is widely recognised and adopted by the automotive industry, and is becoming increasingly important as vehicles become more autonomous and rely more on electronic systems. Compliance with the standard is often a requirement for suppliers and OEMs working in the automotive industry, and is seen as a way to enhance safety and ensure compliance with legal and regulatory requirements.

1.1 Background

In the field of automotive engineering, functional-safety plays a crucial role in the overall safety of the vehicle. Since the time of its introduction in 2011, ISO 26262 series of standards has striven to provide the best set of guidelines to build a safe

and reliable vehicle. In 2018, a second edition of the ISO 26262 was introduced with added chapters to the different parts of the series of standards. A new chapter in ISO 26262 part 8, clause 13 discusses about reliability of hardware elements in safety applications. As per the standards, to build a safe and reliable system, the components used to build the E/E architecture should also be reliable. One way to achieve this is to develop the component as per the development process detailed in the standards. For the purposes of the thesis project, these components will be called ISO 26262 compliant components or just compliant components. The standards also provide details on ways to use components that have not been developed as per the ISO 26262 in safety applications. For the purposes of this project, these components will be termed ISO 26262 non-compliant components or just non-compliant components. While there have been numerous research papers that have explained different ways to implement safe systems as per the ISO 26262 guidelines, they do not specifically explore the reliability of the components being used in their designs. The related work in the field of this thesis project is elaborated in Section 1.2.

For the purposes of this thesis project, a power-distribution solution is considered as it is an integral part of building a vehicle. Power distribution plays a crucial role in ensuring the safe operation of modern vehicles. It is a safety critical functionality that needs to be developed with high integrity and reliability. For this purpose, Volvo Cars has proposed to analyze a hardware design that provides safe and reliable power source to a zone controller, from a safety perspective. Zone controllers are critical components in the vehicle with wide range of functionalities ranging from power distribution to managing resources between electronic control units (ECUs), sensors and actuators.

1.2 Related Work

This section focuses on the related works that discuss safety-oriented hardware design. The section is mainly divided into two parts. The first part discusses the different works that have been pursued for performing failure analysis. The second part discusses papers that have implemented a power-distribution solution using the safety standards described in ISO 26262.

1.2.1 Related Works on Failure Analysis

The research done on failure analysis mainly addresses the determination of random hardware failures and performing safety analysis through methods such as fault tree analysis (FTA), dependent failure analysis (DFA), failure modes and effect analysis (FMEA) and so on. As per ISO 26262, failures can be classified into systematic failures and random failures. Systematic failure is defined in ISO 26262 as, "failure related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factor". Random hardware failure is defined in ISO 26262 as, "failure that can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution". One main factor that

determines the random hardware failures is the hardware metrics defined in ISO 26262 standards. These hardware metrics include the probabilistic metrics for random hardware failures (PMHF), single point fault metric (SPFM) and latent fault metric (LFM) [4].

In [5], the authors propose an ISO 26262 Automotive Safety Integrity Level (ASIL) oriented hardware design framework using an example of autonomous emergency braking (AEB) system. ASIL is a risk classification scheme used in the automotive industry. A detailed explanation of ASIL is provided in Section 2.2. The authors propose an FTA-based weak point analysis to effectively apply safety mechanisms to the system design that can be used to design a system of any ASIL integrity. The paper focuses on calculating the PMHF, which is a concept used to quantify the likelihood and impact of random hardware failures in a system. It is used to evaluate the reliability of different hardware components, as well as to assess the overall reliability of a system. While the proposed FTA method in the paper is useful to calculate the PMHF values, the authors are yet to improve the method for calculating the other hardware metrics that are stated in ISO 26262. There are other quantitative and qualitative methods that help in evaluating the SPFM and LFM hardware metrics such as failure mode, effect and diagnostic analysis (FMEDA), timing analysis and DFA which are discussed in [6]. This paper presents a comprehensive introduction to the basic concepts of functional-safety analysis and optimization. The authors also present the impact of the different design methodologies on design and verification of safety applications by addressing the various types of failure analysis used to determine the hardware metrics of the system.

The authors of [7] present a novel approach for automotive system safety analysis, focusing on FMEDA. This method employs model-based techniques, such as meta-modeling and code generation, to streamline FMEDA processes. Model-based development (MBD) reduces complexity, promotes standardization, and boosts productivity by leveraging models and model technologies to elevate the level of abstraction in the development of applications. Meta-models serve as an additional layer of abstraction, emphasizing the characteristics of models and defining the connections among their constituent elements. These techniques enhance consistency and save up to 60% of effort compared to manual methods. It includes reusable failure-modes database, interface adapters for component interrelations, and improves data maintainability and correction implementation. Additionally, the approach introduces a verification aspect through simulation-based failure propagation analysis. While it reduces manual tasks, elementary component analysis remains necessary, with plans to integrate fault injection experiments for further automation.

For the purpose of this thesis project, we rely on the quantified FTA and FMEDA methods to address failure analysis. The referenced papers provide a comprehensive and insightful understanding of quantified FTA and FMEDA. However, the traditional approach of these techniques have been considered for this thesis project.

1.2.2 Related Works on Power Distribution in Safe Applications

Power distribution in automotive safety applications is crucial in ensuring the safe operation of modern vehicles. In recent years, researchers and engineers have been working on developing new technologies and techniques to improve the reliability, efficiency, and safety of power-distribution systems. In [8], the authors show the current developments in power supply systems for electronic fuse applications having a 12 V and 48 V power bus. The paper presents the rise of E/E concept in contrast with the traditional hardware oriented design approach. The E/E architecture is a more software-oriented design that uses zone controllers which interacts with the ECUs based on their placement in the vehicle. This architecture was found to have a higher voltage and current rating, higher sensing precision, usage of augmented digital processing and non volatile memory.

While the implementation of E/E systems has been on the rise, integrating hardware-software interface (HSI) with their power input is still dependent on the power supply system that is shared across the vehicle. Any failure in the power distribution can lead to critical situations. In [9], the importance of having requirements on safety-related availability (SaRA) of power-supply systems is explored. The paper evaluates the similarities and differences between these SaRA requirements, fail-passive behavior and fail-active behavior. It proposes that, along with fault tolerance measures, fault prediction and fault avoidance also need to be considered. It provides a comprehensive methodology on dealing with SaRA for power supply from failure analysis, fault detection, to design considerations for safety mechanisms in the context of ISO 26262. The paper aims to standardize functional-safety concepts in the power-supply domain.

The same authors have also worked on another paper, [10], that provides guidelines on developing a safe power-supply system. The main objective of this paper is to provide a standard approach to design and ensure safety in power-supply systems. The authors discuss the trends in electrification and automation in the industry and state that, in order to ensure safety in power supply, three main safety requirements are to be considered for power input: the power sources, the distribution through wiring harness and the freedom from interference (FFI) between safety and non-safety relevant loads. FFI, as defined in ISO 26262, is the 'absence of cascading failures between two or more elements that could lead to the violation of a safety requirement'. Overall, the paper gives a deep insight and gives useful suggestions on developing power-supply systems.

1.2.3 Research Gap

In this thesis project, the main focus is on determining the impact of using ISO 26262 compliant and ISO 26262 non-compliant components in designing the safe power-distribution. ISO 26262 standards provide certain guidelines, design recommendations and the evaluation methods to ensure that non-compliant components can be used to achieve a safety goal. However, in the process of understanding the previous works, we found that there is a lack of research papers that address

reliability of components being used in safety applications. To address this gap in the open literature, this thesis project aims to contribute to understanding the issue better.

1.3 Problem Statement

While performing the literature survey, it was found that there were multiple safe power-distribution solutions proposed, that comply with ISO 26262. However, the research papers fail to address whether the components that are being used have been developed in accordance with the standards. Component selection is an important factor to be considered during hardware design. In the automotive industry, high ASIL ECUs are extremely important and the components selected for designing such ECUs are preferred to have been designed, tested and analysed for potential faults as per ISO 26262 standards.

When a component is not developed as per ISO 26262 standards, there is a chance that the supplier has not performed the failure analysis in depth, which could lead to failures in the system that can potentially violate the safety goals. These components do not have extensive safety documentation done to qualify them for use in safety applications as compared to the components developed as per the standards. However, Part 8 Clause 13 of ISO 26262 specifically discusses the methods to approach using such components in safety applications. The standards do not restrict designers from considering to use non-compliant components for safety applications. Instead, the standards suggest for the components to meet certain requirements and additional testing, to be qualified for use in safety-critical systems. In the automotive industry, this is generally done by the supplier who designs and manufactures the component. This analysis is then provided to the OEMs for their safety analysis of the system.

In this thesis project, the aim is to assess if component reliability is an important factor to consider while designing safe systems. To realize this, Volvo Cars has proposed to analyze a hardware design that provides safe and reliable power source to a zone controller, from a safety perspective. For the purposes of this thesis project, the goal is to provide power to an ASIL D System Basis Chip (SBC) that monitors the microcontroller within the zone controller. The concept of ASIL levels is discussed in section 2.2. To achieve ASIL D in the power-distribution functionality of zone controllers, a comprehensive failure analysis needs to be performed on the requirements and design to understand the possible failures that can occur within the system.

The design is implemented to have a redundant power source for power supply to zone controller. To ensure that the redundant power supply implementation does not lead to a current flow between the supplies, reverse current protection is required. In pursuit of this objective, the thesis involves the development of two distinct systems focused on reverse current protection. To achieve this, diodes can be used to block current from flowing in opposite direction. However, diodes have a higher forward voltage drop (typically 0.7 V) compared to the voltage drop in an ideal diode controller. Therefore, an ideal diode controller is used for reverse current

protection.

One design chosen for this project incorporates compliant ideal-diode-controller while the other utilizes non-compliant ideal-diode-controller. The main focus of analysis will be the probabilistic metrics values obtained for random hardware failures to occur in the proposed designs and compare the results. The results are expected to indicate the significance of using compliant and non-compliant components in safety systems.

1.4 Research Questions

Based on the problem statement, the following research questions are answered in this thesis report.

1. Why is evaluating component reliability required while designing safety-critical systems?
2. What methodologies can be employed to conduct failure analysis and subsequently assess the reliability of components in a system?
3. How does the utilization of ISO 26262 compliant and non-compliant components influence the overall reliability of a system in the context of safety-critical applications?
4. What are the practical considerations and methodologies for the integration of non-compliant components in safety-critical systems while maintaining or enhancing overall system safety and reliability?

1.5 Thesis Outline

This section provides insight to the contents of the coming chapters. Chapter 2 provides the theoretical foundations of hardware design for safety-critical applications as per ISO 26262. It also provides an insight to terms and techniques used within the automotive industry for functional-safety. Chapter 3 explains the research approach, tools used in the thesis project, scope limitations and assumptions. Chapter 4 focuses on the design of the circuits using non-compliant component and compliant component for failure analysis, including technical safety concept, components, design considerations and the failure analysis. Chapter 5 presents the results obtained from the analysis of both designs. It also discusses the interpretations and implications of the results obtained. Chapter 6 summarizes the research objectives, methodology, major findings, and contributions. It also discusses limitations, future of scope of the research and final reflections on the thesis project.

2

Theory

In this chapter, the theoretical concepts used in this thesis project are explained. The chapter is mainly focused on the topics that contribute to understanding the different aspects of hardware design. Firstly, ISO 26262 standard and its parts are explained. The concepts of ASIL is then discussed in detail, followed by information on the types of failures, bathtub curve and other failure analysis terminologies. A brief overview of the power-distribution design recommendations by ISO 26262 is then provided. Finally, the differences between ISO 26262 compliant and ISO 26262 non-compliant components and their corresponding failure analysis are discussed.

2.1 Functional Safety and ISO 26262

Functional safety in vehicles refers to the ability of a vehicle's electronic systems to operate safely, reliably, and consistently under all foreseeable conditions. It involves the use of engineering techniques and safety measures to minimize the risk of accidents or injuries resulting from malfunctions or failures in a vehicle's electronic systems. The automotive industry has established several standards for functional safety, including the ISO 26262 standard, which provides a framework for managing the safety of automotive electrical and electronic systems throughout their entire lifecycle, from design and development to operation and maintenance.

The ISO 26262 standard is a risk-based safety standard that is derived from IEC 61508 and applies to E/E systems in production vehicles. It covers all of the functional safety aspects of the entire development process, including requirements specification, design, implementation, and integration. The standard is critical for automotive product development. The OEMs, their suppliers, and developers of automotive components, all need to comply with it while designing and manufacturing a road vehicle. The standard is divided into twelve parts, each covering a different aspect of functional safety in road vehicles. Figure 2.1 shows an overview of the ISO 26262 series of standards. A brief explanation of each part is given below:

1. Vocabulary: This part defines the terms and concepts used throughout the standard.
2. Management of functional safety: This part covers the management processes and requirements for ensuring functional safety throughout the product life cycle.
3. Concept phase: This part covers the development of the concept for the product and its functional safety requirements.

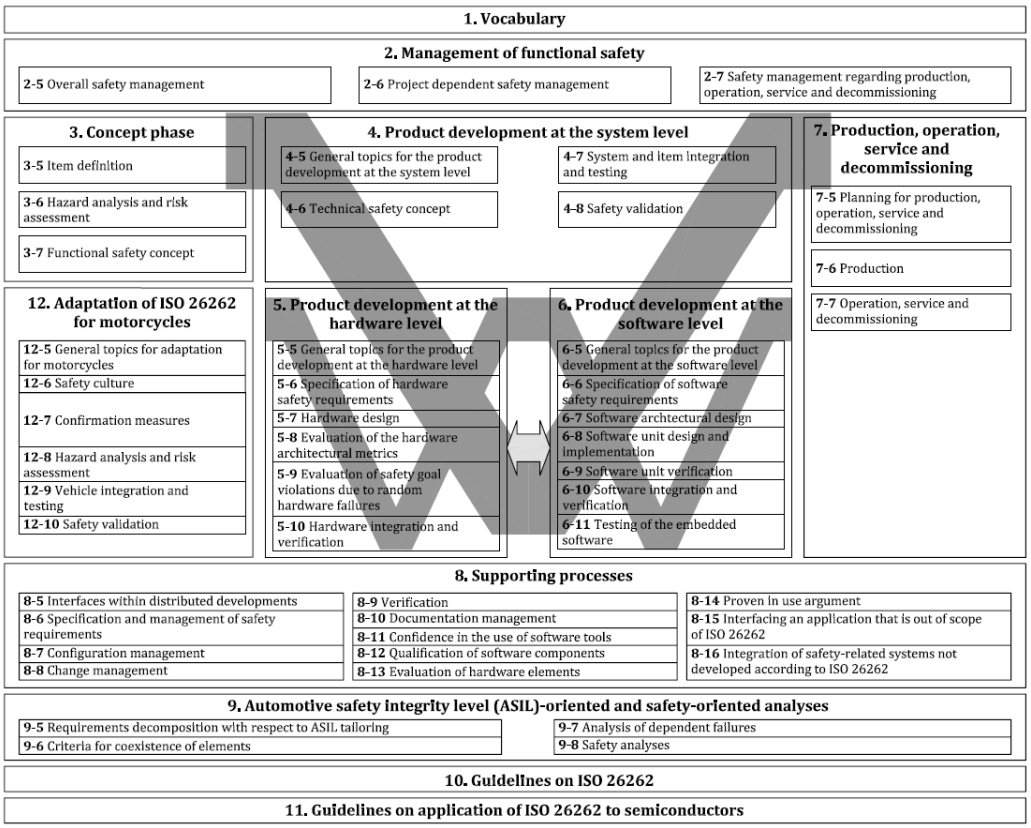


Figure 2.1: Overview of ISO 26262 series of standards [3].

4. Product development at the system level: This part covers the development of the system-level requirements and the overall safety concept.
5. Product development at the hardware level: This part covers the development of the hardware requirements and the safety integrity levels (SILs) for the components.
6. Product development at the software level: This part covers the development of the software requirements and the SILs for the software components.
7. Production, operation, service and decommissioning: This part covers the requirements for ensuring functional safety throughout the entire life cycle of the product, including production, operation, service, and decommissioning.
8. Supporting processes: This part covers the supporting processes that are required to ensure functional safety, such as documentation, change management, and configuration management.
9. Automotive Safety Integrity Levels (ASIL)-oriented and safety-oriented analyses: This part focuses on decomposing the system into elements and assigning ASIL integrity based on their impact on safety. It provides guidelines for assessing hazards, faults, and failure modes to determine the appropriate ASIL level for each element.
10. Guidelines on ISO 26262 - This part provides valuable guidance on how to effectively apply and implement the requirements outlined in the standard,

ensuring the development of safe and reliable automotive systems.

11. Guidelines on Application of ISO 26262 to Semiconductors: This part provides guidance on how to apply the ISO 26262 standard to the development of semiconductors that are used in safety-related automotive systems.
12. Adaptation of ISO 26262 for motorcycles: This part provides guidance on how to apply the ISO 26262 standard to the development of safety-related systems in motorcycles.

For the purposes of this thesis project, we focus mainly on Part 5 [4], Part 8 [11], and Part 9 [12] of the ISO 26262 standard.

2.2 Automotive Safety Integrity Levels (ASIL)

As explained previously in section 1.2.1, ASIL is a risk classification scheme used in the automotive industry to determine the safety requirements for various automotive systems. ASIL is a part of the ISO 26262:3 standard, which is a functional-safety standard that provides guidelines for the development of safety-critical automotive systems. The ASIL rating system is based on the severity and probability of harm that can result from a malfunction or failure of a system. There are four ASIL levels, with ASIL A being the lowest and ASIL D being the highest. ASIL D represents the most stringent safety requirements, and systems with this rating must have the highest levels of safety integrity, for example, airbag system or electronic stability control (ESC). There is another rating known as quality management (QM) which indicates that the hazard is not safety critical in any sense and does not compromise the safety of the driver in case of its occurrence, for example, infotainment systems in vehicles.

To determine the ASIL integrity of a particular system, the potential hazards and probability of occurrence of those hazards are analyzed. As per the ISO 26262 standards, the process of determining the hazards and their impact involves the following steps:

1. Hazard Analysis and Risk Assessment (HARA): The first step in the process is to perform a HARA to identify potential hazards associated with the system. The HARA identifies hazards and assesses their severity, probability of occurrence, and potential impact on the vehicle occupants and other road users.
2. Functional Safety Concept (FSC): The next step is to develop an FSC that describes the functional requirements of the system and how it will mitigate the identified hazards.
3. ASIL Determination: Once the hazards have been identified, and the functional safety concept has been developed, the ASIL can be determined based on the severity and probability of the hazards.
4. ASIL Verification: Once the ASIL has been determined, the system must be designed and verified to meet the safety requirements associated with the ASIL. This includes designing the system to be fault-tolerant, implementing

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

Figure 2.2: ASIL rating determination system

safety mechanisms to detect and mitigate faults, and ensuring that the system meets the required safety standards.

The ASIL determination part of the process involves assigning an ASIL rating to each hazard. This ASIL rating is based on three factors: Severity, Exposure and Controllability.

1. Severity: Severity refers to the potential harm that can be caused by a hazard associated with a system. Hazards can cause harm to people, the environment, or property. Severity is classified into three levels: S1, S2, S3 with S1 being less severe and S3 being critically severe.

2. Exposure: Exposure refers to the frequency or probability of a hazard occurring. Exposure is classified into four levels: E1, E2, E3 and E4 with E1 indicating lower probability and E4 indicating high probability of occurrence.

3. Controllability: Controllability refers to the ability to control or avoid a hazard. It considers the effectiveness of safety mechanisms to detect, control, and mitigate hazards. It is classified into three levels: C1, C2 and C3 with C1 indicating easily controllable and C3 indicating difficult to control.

Overall, the combination of severity, exposure, and controllability determines the ASIL rating of a system. Figure 2.2 indicates the system of rating used to classify the hazards. For example, if a system has a high severity rating, S3, a high probability of occurrence, E4, and low controllability, C3, it will require an ASIL D rating, which represents the most stringent safety requirements. In contrast, if a system has a low severity rating, S2, a low probability of occurrence, E3, and high controllability, C2, it may only require an ASIL A rating.

2.3 Types of failures

ISO 26262 defines different types of failures that can occur in automotive electronic systems. These failures are classified into two categories based on their severity and potential impact on the vehicle and its occupants. These categories are:

1. Systematic failures: These are failures that occur due to a systematic error in the development process, such as a mistake in the requirements or design. Systematic failures can have a significant impact on the safety of the system if not detected and corrected.
2. Random hardware failures: These are failures that occur due to random events or conditions, such as a component failure or a voltage spike. Random hardware failures can have a moderate to severe impact on the safety of the system, depending on the criticality of the affected component.

2.3.1 Systematic failures

When it comes to hardware design of power distribution, the systematic failures and random hardware failures are very important to analyze, particularly in the case of using ISO 26262 non-compliant devices where the probability of these failures is higher as the components are not developed as per the ISO 26262 standards. As per the standards, in clause 4.6 of Part 4 of ISO 26262 titled "Systematic Capability" [13], it emphasizes the need for organizations to establish systematic capability management to address and mitigate systematic failures. It provides guidance on implementing processes, techniques, and measures to ensure that systematic failures are systematically managed throughout the development life-cycle.

System and design FMEA, give a deep insight into the possible failures and their effects on the system. As per ISO 26262, FMEA, DFA and qualitative FTA are recommended failure analysis techniques to identify systematic failures during development of hardware designs for safety applications [4]. Components that are not developed as per the ISO 26262 often do not have these failure analysis performed on their hardware design as required by the standards. However, if the components are to be used for safety application, a comprehensive failure analysis and rigorous testing needs to performed on it in order to identify the potential failures [11].

Part 8 of ISO 26262 provides requirements for hardware elements that are not developed as per the standards but are used for safety applications. It provides methods for evaluating the hardware elements through analysis and testing. The steps involve the following:

1. An evaluation plan needs to be developed that provides a specification of the environment in which the component is planned to be used, along with a strategy outlining the analysis methods and necessary tests.
2. Evaluation of the hardware elements by analysis and testing.
3. Test plan developed with allocated safety requirements, test specification, traceability methods between the tests and safety requirements and test environment description.

4. A comprehensive argument developed based on the analysis, data obtained from operational experience and the test results obtained, to show sufficient evidence for systematic failure avoidance.

While ISO 26262 does not guarantee the complete elimination or reduction of all systematic failures, it provides a comprehensive framework that, when properly implemented, significantly enhances the capability to identify, manage, and mitigate systematic failures. The standard promotes a systematic mindset and sets the foundation for organizations to develop safe and reliable automotive systems. It is important to note that the effectiveness of reducing systematic failures depends on the thoroughness and diligence with which the ISO 26262 processes and guidelines are applied.

2.3.2 Random failures

Random hardware failure, within the context of ISO 26262, refers to unforeseen and unpredictable faults that can occur in electronic or electrical hardware components of automotive systems. These failures are considered random because they can happen at any time without a specific pattern or easily identifiable cause. Random hardware failures can lead to hazardous situations or malfunctions in the vehicle's electrical and electronic systems, posing risks to the driver, passengers, and other road users.

ISO 26262 provides a systematic approach to manage random hardware failures, and it involves the use of various hardware metrics to determine their impact on functional safety. The different metrics used to quantify random hardware failures under ISO 26262 are SPFM, LFM and PMHF. These hardware metrics play a crucial role in the safety analysis of automotive systems under ISO 26262. As per the standard, these metrics are determined by identifying the total failure rate of single point faults (λ_{SPF}), total failure rate of residual faults (λ_{RF}), total failure rate of safety related failures (λ_{SR}) and total failure rate of multiple point faults (λ_{MPF}).

The failure rates of each component in the hardware design are provided by the respective suppliers or they are taken from a failure-rates catalog that provides failure rates for commonly used components. The failure-rates catalogs commonly used for automotive industry are IEC TR 62380 and SN 29500. These catalogs will be discussed in detail in further sections. Along with failure rates, failure modes are also considered. Failure modes are different ways in which a hardware element or an item fails to fulfill its intended functionality. The suppliers of components provide the failure modes and the failure-mode distribution. Failure-mode distribution provides the failure-rate contribution of each failure mode on overall failure rate of the component. For example, a ceramic capacitor has three failure modes as per IEC TR 62380 failure-mode library, which are 'open', 'short' and 'drift'. The failure-mode distribution is 80% probability for capacitor failure to lead to open circuit, 15% for capacitor failure to lead to short circuit and 5% probability of for capacitor to provide output outside the range if expected value. Once the hardware design has been realised, a deep analysis on the role of failure modes of each component is performed to determine the ones that lead to a violation of safety goal. The re-

sulting failure rates associated with the failure mode is then used to calculate the hardware metrics.

2.3.2.1 Single Point Fault Metric

SPFM assesses the probability of a single fault leading to a hazardous event. It measures how likely it is for a single hardware failure to cause a safety-critical malfunction or hazardous situation in the system. The SPFM is calculated using

$$SPFM = 1 - \frac{\Sigma(\lambda_{SPF} + \lambda_{RF})}{\Sigma\lambda_{SR}} \tag{2.1}$$

where $\Sigma(\lambda_{SPF} + \lambda_{RF})$ is sum of all single-point faults and residual faults, and $\Sigma\lambda_{SR}$ is sum of all safety-related faults.

2.3.2.2 Latent Fault Metric

LFM quantifies the potential undetected faults in the system that could lead to hazardous situations. It evaluates the probability of latent faults remaining dormant or undetectable until they are activated by specific conditions or events. The LFM is calculated using

$$LFM = 1 - \frac{\Sigma\lambda_{MPF}}{(\Sigma\lambda_{SR} - \Sigma(\lambda_{SPF} + \lambda_{RF}))} \tag{2.2}$$

where $\Sigma\lambda_{MPF}$ is the sum of all multiple-point failures (MPF), $\Sigma(\lambda_{SPF} + \lambda_{RF})$ is the sum of all single-point faults and residual faults, and $\Sigma\lambda_{SR}$ is the sum of all safety-related faults.

2.3.2.3 Probabilistic Metric for Random Hardware Failures

PMHF is a comprehensive metric that considers both SPFM and MPF to evaluate the overall probability of a hazardous event occurring due to random hardware failures. It provides a more complete picture of the system's safety integrity concerning random hardware failures, considering both detected and undetected faults. The PMHF is calculated using

$$PMHF = \Sigma(\lambda_{SPF} + \lambda_{RF}) + \Sigma\lambda_{MPF} \tag{2.3}$$

where $\Sigma(\lambda_{SPF} + \lambda_{RF})$ is the sum of all single-point faults and residual faults, and $\Sigma\lambda_{MPF}$ is the sum of all multiple-point faults.

These hardware metrics help developers assess the safety of their systems regarding random hardware failures and identify potential weaknesses in safety mechanisms. It also provides an indication to implement additional safety mechanisms, such as redundancy or fault-detection systems, to reduce the risks associated with random hardware failures. By utilizing these metrics, automotive developers can make informed decisions, enhance functional safety, and reduce the likelihood of safety-critical incidents caused by unpredictable hardware faults. This approach is essential to building safe and reliable electronic systems for vehicles in accordance with ISO 26262 standards.

2.4 Failure analysis techniques

Failure analysis is highly relevant in the automotive industry due to the critical nature of safety and reliability in vehicle systems. Automotive systems are complex and consist of numerous interconnected components, subsystems, and software. Any failure in these systems can have severe consequences, including accidents, injuries, or even loss of life.

ISO 26262 proposes different failure analysis techniques to reduce the systematic failures and random hardware failures. As explained in Section 2.3, systematic faults occur due to mistakes in requirements or design of a system while random hardware faults, as the name suggests, occur due to failures in hardware components over time.

2.4.1 Systematic failures analysis

Some techniques which can be used to reduce systematic faults are FMEA, DFA and qualitative FTA.

2.4.1.1 Failure Modes Effect Analysis

FMEA is a detailed component and functional-level-failure analysis which considers the failure modes of different components used and the effects the failure modes have on the functionality of the system. It is a bottom-up approach where the different failure modes for each component are listed. Once the failure modes are linked to the components, the effects of a combination of the failures or the individual component failures are analyzed on a functional level. The result of an FMEA is to suggest safety mechanism to be implemented or suggest a different design approach to implement the functionality. The FMEA also suggests the testing strategy to verify different use cases and the procedure to document them to ensure a safe hardware. A pictorial representation of the FMEA process is shown in Figure 2.3.

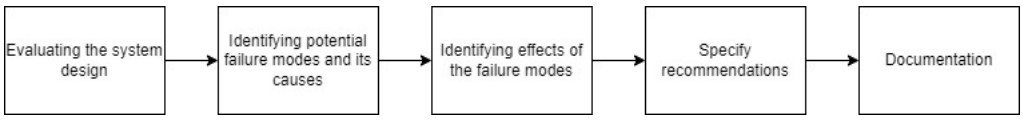


Figure 2.3: A basic FMEA process [14].

2.4.1.2 Dependant Failure Analysis (DFA)

DFA is used to analyze failures in a system when there are shared resources between two sub-systems [6]. The main purpose of performing a DFA is to analyze if there are any common failures affecting different sub-systems. One of the scenarios for which a DFA should be performed is when there are two sub-systems with similar architectural designs since a common failure could affect the performance of both the sub-systems with similar probabilities.

2.4.1.3 Qualitative Fault Tree Analysis (FTA)

FTA is a top-down approach where the top-level safety goal is defined. Once the safety goal is defined, the allocation of safety mechanisms to the specific interfaces is done. For example, under-voltage and over-voltage protection mechanisms can be allocated to a power-management IC (PMIC). Similarly, different safety mechanisms are allocated to different hardware elements. Once that is done, the violation of the safety goal is broken down into the failure modes which could occur in a specific element. 'AND' and 'OR' symbols are used when a combination of failures would lead to the violation of safety goal. The goal of the qualitative FTA is to analyze the cause-effects relationship in a system design and to suggest preventive measures that should be taken to have a desirable ASIL.

2.4.2 Random hardware failures analysis

The commonly used techniques to analyze the random hardware failures are FMEDA and quantitative FTA.

2.4.2.1 Failure Modes, Effects and Diagnostic Analysis

Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is a failure analysis approach to assess the reliability of a system. Every component is analysed to understand the functionality it provides in a system. The effects of each failure-mode in the component on the entire system is evaluated and estimated to either be a SPF or a MPF. The failure in time (FIT) rates and the failure-mode distribution of each component is obtained from a catalog called SN 29500 which is explained Section 2.8.1. After the analysis of each failure mode for all the components in the system, the SPF and the LFM metrics are obtained to check the ASIL rating the system satisfies.

2.4.2.2 Quantitative Fault Tree Analysis

Quantitative FTA is a similar approach to the qualitative FTA but the objective of a quantitative FTA is to obtain the PHMF metric which gives the reliability of the system over its entire lifetime of operation. The metrics are calculated by considering a top-level event and the subsequent failures that violate it. Each failure that violates the top-level event is further analysed and down to the failures of individual components. The failures of individual components are either provided by the supplier of the component or they are based on the SN 29500 catalog and IEC TR 62380 failure-mode library which provides the FIT rates for commonly used components and the failure-mode distribution of the components. While FIT rates are defined as failures occurring per 10^9 hrs, in the automotive field, the PHMF is estimated for 10-15 years of operational life-time. This period is defined based on the concept of bathtub curve described in the next section.

The acceptable ranges of the failures for different ASIL are shown in Table 2.1.

Table 2.1: ASIL Levels and Failure Rates [4]

ASIL Level	SPFM	LFM	PMHF (FIT)
ASIL B	$\geq 90\%$	$\geq 60\%$	≤ 100 FIT
ASIL C	$\geq 97\%$	$\geq 80\%$	≤ 100 FIT
ASIL D	$\geq 99\%$	$\geq 90\%$	≤ 10 FIT

2.5 Bathtub curve

The bathtub curve shown in Figure 2.4 is a graphical representation of the failure rate of a system over time. It is often used in reliability engineering to analyze the reliability of systems, including those in the automotive industry that adhere to the ISO 26262 standard.

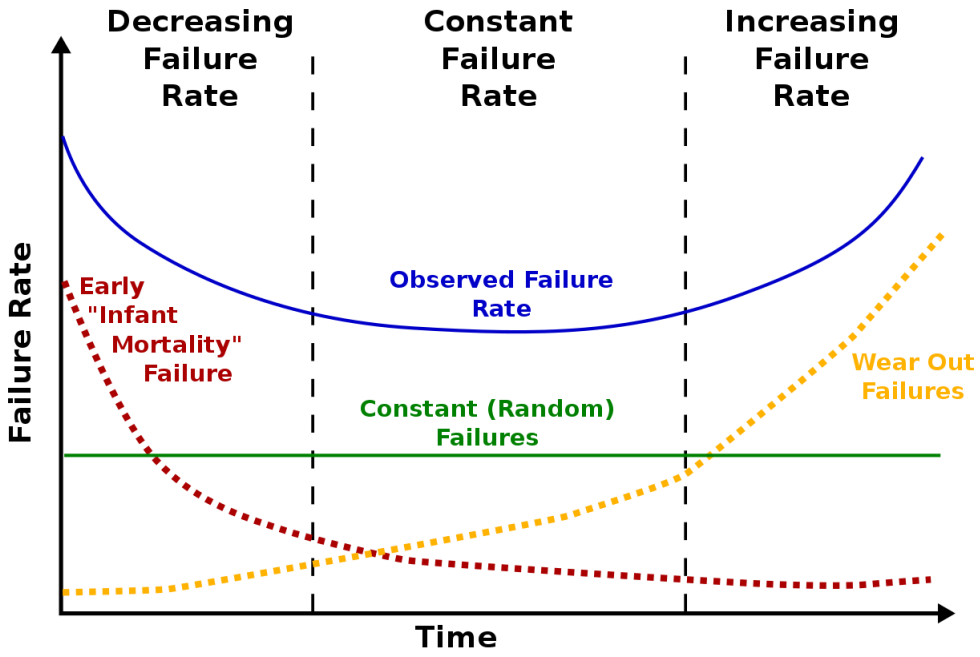


Figure 2.4: The bathtub curve to determine failure rates [15].

In context of ISO 26262, the bathtub curve is used to describe the failure rate of safety-related systems over their lifetime. The curve is divided into three phases:

1. Infant Mortality Phase: This phase represents the initial period after the system is put into service. During this time, failures are more likely to occur due to manufacturing defects, design errors, or installation problems. It is possible to mitigate the early life failures by performing accelerated life tests.
2. Normal Life Phase: This phase represents the period during which the system operates reliably without any major issues. Failures during this period are generally caused by wear and tear, aging, or environmental factors.
3. Wearout Phase: This phase represents the period during which the system's

failure rate starts to increase again exponentially. Failures during this phase are typically caused by the degradation of critical components due to extended use, high stress, or environmental factors. The ISO 26262 standard does not support the estimation of random hardware metrics based on a non constant failure rate. Therefore, an approximation is made on the products lifetime which is used to calculate the PMHF.

ISO 26262 requires safety-related systems to be designed to minimize the risk of failure during all three phases of the bathtub curve. This can be achieved through various measures, including design verification and validation, regular maintenance, and appropriate testing and analysis. The lifetime of the component is also determined using the bathtub curve which is used in calculating the hardware metrics. When performing failure analysis such as quantitative FTAs [16], the system lifetime is a very important factor to consider.

2.6 Hardware design development as per ISO 26262

When developing a hardware design for safety applications, ISO 26262 defines necessary activities and processes for the product development at the hardware level. These include:

1. The hardware implementation of technical safety concept.
2. The analysis of potential hardware faults and their effects.
3. The coordination with software development.

Figure 2.5 illustrates the development process steps in order to comply with ISO 26262 requirements. For the purposes of this thesis project, the highlighted part in the figure is the main focus. Each step in the figure refers to a section in the standard. A brief overview for each section and its relevance to this thesis project can be seen below.

1. 5-7: Hardware design - Provides requirements and design recommendations when developing hardware. This section helps in the development of the two designs explored in this thesis project.
2. 5-8: Evaluation of the hardware architectural metrics - Provides details on types of failures and safety-related failure metrics to be evaluated (Refer section 2.3). This section provides guidelines on performing failure analysis specifically to obtain the SPFM and LFM values.
3. 5-9: Evaluation of safety goal violations due to random hardware failures - Provides guidelines on evaluating PMHF for safety-goal violations.
4. 8-13: Evaluation of hardware elements - Provides insight in differences between compliant and non-compliant components. Additionally, it provides requirements that need to be fulfilled by non-compliant components in order to be used in safety applications.

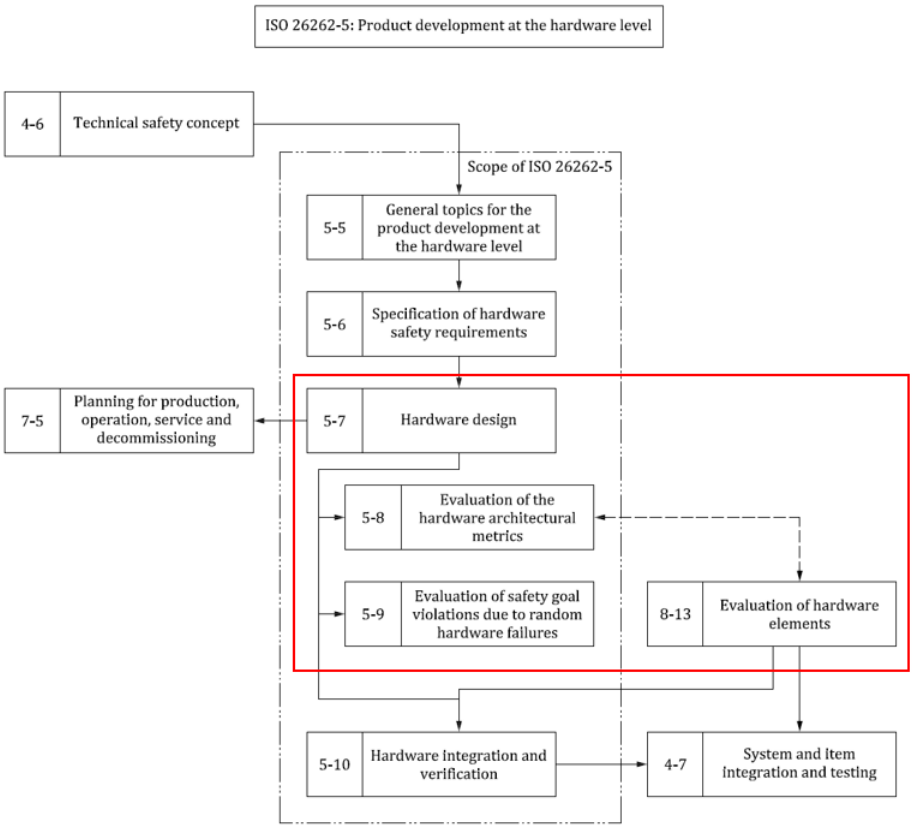


Figure 2.5: Reference phase model for hardware development [4]

2.7 ISO 26262 compliant and non-compliant components

When it comes to safety applications in the automotive industry, there are significant differences between using ISO 26262 compliant components and ISO 26262 non-compliant components:

1. Safety Considerations: Compliant components are specifically designed and developed with safety considerations in mind. They undergo a rigorous development process that includes safety analyses, risk assessments, and systematic safety requirements. Non-compliant components may not have undergone such extensive safety-oriented processes.
2. Documentation and Traceability: Compliant components are accompanied by comprehensive documentation that includes safety plans, safety cases, and other safety-related artifacts. These documents provide evidence of the component's compliance with safety requirements. Non-compliant components may not have the same level of documentation and traceability.
3. Safety Verification and Validation: Compliant components undergo safety verification and validation activities to ensure that they meet the required SIL as per the standard. This involves extensive testing, analysis, and evaluation of the component's behavior under various safety scenarios. Non-compliant

components may not have undergone the same level of safety verification and validation.

4. Functional-Safety Management: Compliant components are developed within a functional-safety-management system, which ensures that safety-related processes are followed throughout the component's development life-cycle. This includes activities such as safety planning, safety-requirements management, and safety assessment. Non-compliant components may lack the same level of formalized functional-safety management.
5. Certification and Compliance: Compliant components can be certified by independent third-party organizations to demonstrate their compliance with the standard. This certification provides confidence in their safety capabilities. Non-compliant components may not have undergone similar certification processes.

Using compliant components in safety applications provides a higher level of confidence in their safety performance, as they are developed with specific safety requirements and undergo extensive safety-oriented processes. Non-compliant components may still be used in certain applications, but additional measures are required to ensure their suitability and to mitigate potential safety risks.

ISO 26262 Part 8 Section 13 introduces the classification of hardware elements into Class I, Class II, and Class III in the context of safety applications. Non-compliant hardware elements are those that do not fully comply with the requirements of ISO 26262. The term "hardware elements" specifically refers to non-compliant components that are being considered for safety applications. The classification of hardware elements is performed to evaluate and determine their safety significance and the safety requirements they must fulfill to be used in safety-critical applications. The section provides evaluation guidelines for assessing the class of a non-compliant hardware element based on its potential impact on functional safety.

To classify a non-compliant hardware element, various criteria are considered, such as its functional behavior, failure modes, and other relevant characteristics. This evaluation helps determine whether the hardware element belongs to Class I, Class II, or Class III. ISO 26262 Part 8 Section 13 also specifies the supporting documentation necessary for classifying hardware elements into their respective classes. This documentation includes details about the hardware element's functional behavior, failure modes, and other relevant information that aids in assessing its safety significance.

By following these guidelines and providing the required documentation, hardware elements can be appropriately classified and subjected to additional measures to mitigate safety risks in safety-critical applications. Based on this, suppliers for automotive application provide information on whether the components they have produced is compliant or not. For example, Infineon is major supplier for automotive applications. They have safety conformity levels that are assigned to all their semiconductor products used for automotive applications. They classify their products into QM products, PRO-SIL™ products, PRO-SIL™ ISO 26262-ready and PRO-SIL™ ISO 26262-compliant products. Table 2.2 shows the mapping of these products to the respective ISO 26262 hardware element classes.

Table 2.2: Infineon automotive product classification [17]

Product classification	**ISO 26262 Clause 8-13 Class I possible**	**ISO 26262 Clause 8-13 Class II possible**	**Conformity to ISO 26262 Standard**
QM products	Customer specific		
PRO-SIL™ products	X		
PRO-SIL™ ISO 26262-ready		X	
PRO-SIL™ ISO 26262-compliant			X

Another example of suppliers classifying their products is Texas Instruments. However, their method of classification varies from Infineon's. Table 2.3 shows the classification of products based on the different aspects of safety documentation. As can be seen from the table, Texas Instruments functional-safety capable and functional-safety quality-managed are not certified but can be argued to be under Class II hardware elements based on their use case.

As per TÜV SÜD, an organization that specializes in ISO 26262 certification among many other, components developed according to ISO 26262 standards can be more expensive to implement compared to the same components that are not developed according to these standards [19]. This is primarily because the development of components in compliance with ISO 26262 involves rigorous documentation, verification, and validation processes to ensure their safety and reliability in safety-critical applications. These additional processes and requirements along with certification costs, contribute to higher development costs, which in-turn affect the final price of the compliant components. On the other hand, non-compliant components might not undergo the same level of scrutiny and verification, resulting in lower development costs and, consequently, potentially lower prices. Another factor to consider is that implementing ISO 26262 requirements can be time consuming for suppliers and have long lead times for the completion of product. In cases where specific functionality need to be fulfilled by a component, having to comply with the standards may require longer time than using a component that is not developed as per the standards.

		FuSa-Capable	FuSa QM	FuSa-Compliant
Development Process	QM process	X	X	X
	FuSa Process			X
Analysis report	FuSa FIT calculation	X	X	X
	Failure mode distribution	X	included in FMEDA	included in FMEDA
	FMEDA		X	X
	FTA			X
Diagnostics description	FuSa Manual		X	X
Certification	FuSa Certification			X

Table 2.3: TI categories for products in functional safety design [18]

2.8 Failure Modes and Failure-Rate Catalogs

In this section, the failure mode and the failure-rate catalogs used in this thesis project is explained.

2.8.1 Siemens Norm SN 29500

Siemens Norm SN 29500 is a reliability prediction standard that provides up-to-date failure-rate data at reference conditions and stress models for electronic components used in harsh environments. The standard is an essential resource for reliability calculations of electronic components used in harsh environments. The SN 29500 standard consists of several separate documents, including expected values for integrated circuits, discrete semiconductors, passive components, electrical connections, connectors and sockets, relays, switches and buttons, signal and pilot lamps, contactors, optical components, and electro-mechanical protection devices in low-voltage networks.

The failure rate, which is the most commonly used characteristic in determining reliability, is specified in the individual parts of the SN 29500 standard and is used by Siemens AG and Siemens companies as a uniform basis for reliability calculations. The standard serves as a basis for converting the failure-rate data at reference conditions to the actual operating conditions in cases where the operating conditions differ significantly from reference conditions

2.8.2 IEC TR 62380

IEC TR 62380 is a technical report published by the International Electrotechnical Commission (IEC). The title of the report is "Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs, and equipment." It was first published in 2004 and provides guidelines and methodologies for pre-

dicting the reliability of electronic components, printed circuit boards (PCBs), and electronic equipment [20]. Although this standard is now obsolete, the ISO 26262 standard has incorporated the IEC 62380 standard as part of its newly published standards in ISO 26262:11 [21].

The report presents a universal model for reliability prediction that can be applied to a wide range of electronic devices and systems. It establishes a standardized approach to assess the reliability of electronics by considering various failure mechanisms, stress factors, and operating conditions.

The key aspects covered in IEC TR 62380 are:

1. Failure Rate Prediction: The report defines methods for predicting failure rates of electronic components, PCBs, and equipment based on stress factors, environmental conditions, and the type of component or system under consideration.
2. Stress Factors: IEC TR 62380 provides a comprehensive list of stress factors that influence the reliability of electronic components and systems. These stress factors include temperature, humidity, mechanical stresses, electrical stresses, and others.
3. Failure Mechanisms: Different failure mechanisms in electronic components are considered, such as wear-out, random failures, and infant mortality failures. The report outlines how to model these failure mechanisms and incorporate them into the reliability predictions.
4. Environment Classes: IEC TR 62380 defines various environment classes that help categorize the conditions under which electronic components and systems are expected to operate. These classes are essential for determining the appropriate stress factors to use in reliability predictions.
5. Component and System Models: The report presents mathematical models and equations for estimating the reliability of various electronic components and systems. These models can be used to calculate the failure rate and mean time between failures (MTBF) for different applications.

IEC TR 62380 aims to promote standardized approaches to reliability prediction in the electronics industry. By utilizing the guidelines and methodologies presented in the report, manufacturers and engineers can better assess the reliability of their electronic designs, plan maintenance schedules, and improve the overall performance and longevity of electronic devices and systems.

3

System Description

As explained in the problem statement, the hardware design used for performing the failure analysis is on a circuit that provides safe and reliable power to a zone controller. One of the main function of the zone controllers is to provide power to different 12 V components within the car. The block diagram shown in Figure 3.1 is the design of a power supply from the high-voltage battery to the zone controller. The voltage from the high-voltage battery is stepped down using a DC-DC converter from 400 V to 12 V, which powers the zone controllers (ZC1 and ZC2).

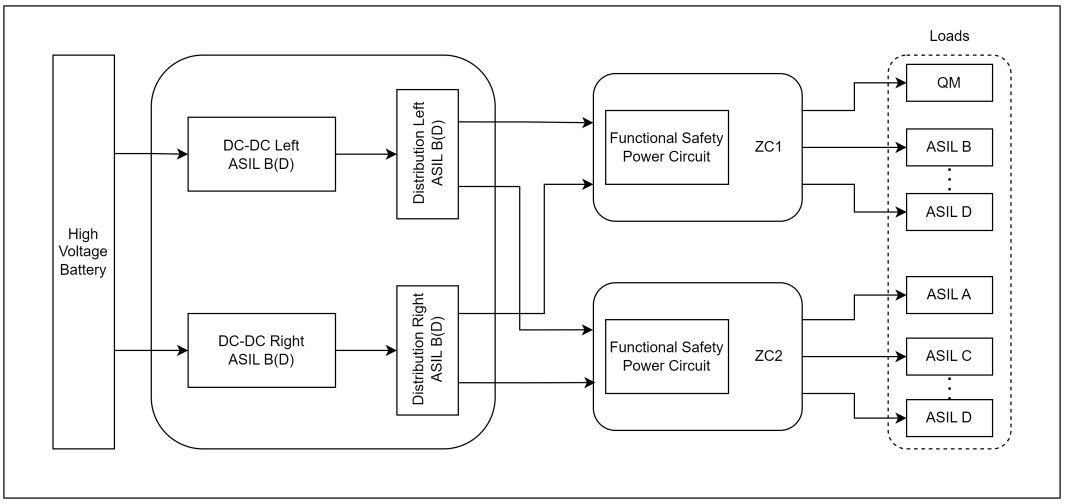


Figure 3.1: Block diagram from the step-down to the zone controllers.

The hardware metrics need to fulfill the target metrics for an ASIL D hardware device as per the standards [12], which is 10 failures per billion hours of operation as detailed in Table 2.1.

This power supplied by the DC-DC converter is distributed to multiple loads in the vehicle. A load can be defined as any sensor, actuator or other ECUs that are connected to the vehicle. Each of the loads have their own safety standards and are classified to different ASIL levels based on the application and requirements they fulfill. In order to fulfill its safety requirements, the safety integrity of the load should be maintained throughout the operation of the load. This means that the power supply to the load should also match the ASIL level that they have been classified to.

3.1 Component selection

To understand the effect of a component on the overall reliability of the power-distribution system, a design using non-compliant component and a design using compliant component are analysed in fulfilling the reverse-current protection requirement.

The non-compliant component chosen for the design is LM74700 developed by Texas Instruments [22]. This component is selected because it is widely available and commonly used in the automotive industry for power-distribution applications. This component is not developed as per the ISO standards, however, TI has provided sufficient documentation for its use in safety applications and has classified it as functional-safety capable which is equivalent to Class II hardware element (See Table 2.3).

The compliant component chosen for the design is STPM801 manufactured by STMicroelectronics [23]. This component is chosen since it is the only ideal-diode controller developed as per ISO 26262 standards [24].

3.1.1 LM74700-Q1 Low I_Q Reverse Battery Protection Ideal Diode Controller

LM74700 ideal-diode controller has its applications in many automotive fields such as in autonomous drive assistance systems (ADAS), automotive infotainment systems, industrial automation solutions and much more. The main application of the LM74700 which is used in this project is the active OR-ing of the redundant power. The LM74700 controller is operated with an external N-channel MOSFET.

The pin diagram of the LM74700 ideal-diode controller is shown in Figure 3.2 and the pin description provided by Texas Instruments is shown in Table 3.1.

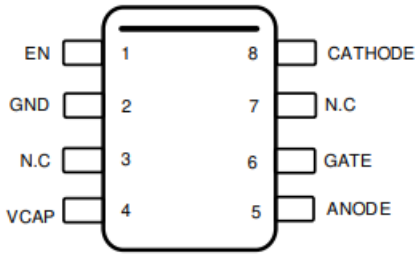


Figure 3.2: Pin layout of the LM74700 ideal diode controller [25]

The functional block diagram of the LM74700 is shown in Figure 3.3.

3.1.1.1 Key features

The key features of LM74700 ideal-diode controller are:

1. Input voltage range of 3.2 V to 65 V
2. 20 mV forward voltage drop from anode to cathode

Table 3.1: Pin description of LM74700

Pin name	I/O/G	Description
EN	I	Enable pin to switch LM74700 ON/OFF
GND	G	Ground pin
N.C	-	Not connected
VCAP	O	Output pin connected to the charge pump capacitor
ANODE	I	Anode pin connected to the anode of the external MOSFET
GATE	O	Output pin connected to the gate of the external MOSFET
N.C	-	Not connected
CATHODE	I	Cathode pin connected to the cathode of the external MOSFET

*I=Input, O=Output, G=Ground

3. Has a shutdown current of 1 µA when EN pin is low
4. Has a 80 µA quiescent current when EN pin is high
5. Fast response to reverse-current blocking, typically less than 0.75 µs

Texas Instruments says that it is only 'functional-safety capable' which means that it can be used in safety applications but extra verification should be performed by the OEM to ensure that the usage of this component satisfies the safety goal of the solution.

3.1.1.2 Safety Related Information

The FIT rate with the SN 29500 catalog for LM74700 is 20 FIT and the failure modes along with the failure-mode distribution is provided by Texas Instruments as shown in Table 3.2.

Table 3.2: Failure modes and the distribution for LM74700

Failure modes	Failure mode distribution (%)
GATE output stuck Low or HIZ	50%
GATE output not in specification - voltage or timing	40%
GATE output stuck on Hi	5%
Short circuit any two pins	5%

3.1.2 STPM801 - Hot Swap and Ideal Diode Controller for high redundancy power architectures

The STPM801 (Figure 3.4) is an integrated circuit developed by ST Microelectronics that offers various protections and functionalities to enhance the safety and

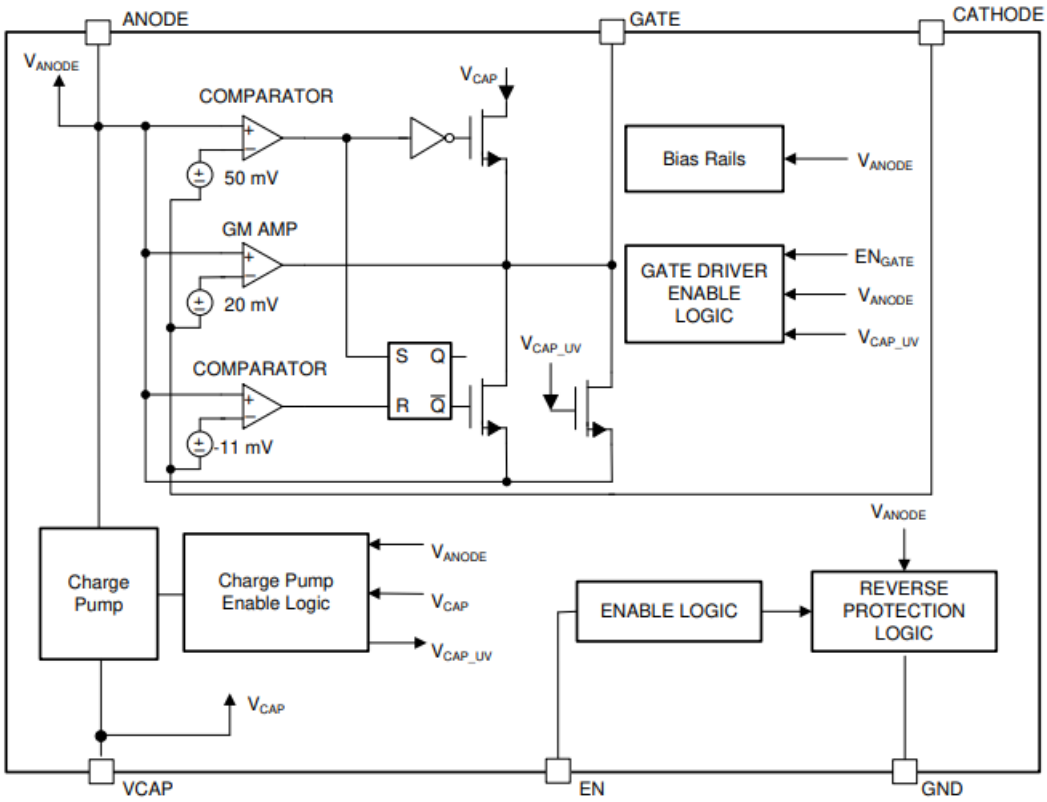


Figure 3.3: Block diagram of LM74700 [25]

reliability of automotive systems. It incorporates hot swap, soft start, and OR-ing protections to safeguard loads from high voltage transients and regulate the output during over-voltage events, such as load dump. The device monitors the input supply to protect against over-voltage and under-voltage conditions. It utilizes an integrated ideal diode controller to drive a second MOSFET (the OR-ing) for reverse-current protection and output voltage holdup, minimizing reverse-current transients in case of power-source failure or input short. The STPM801 is equipped to meet functional-safety requirements as defined by ASIL standards, making it suitable for safety applications.

The block diagram of the STPM801 can be seen in Figure 3.5. STPM801 provides additional diagnostics, monitoring and safety mechanisms, and a fault pin that indicates if an internal failure has occurred.

3.1.2.1 Key features

The key features of STPM801 are:

1. It has a wide input voltage range: 4 V to 65 V.
2. Provides reverse input protection up to −65 V.
3. Drives 2 external N-channel MOSFET.
    (a) One for Hot-swap feature (Note: Hot swapping is a technique used to

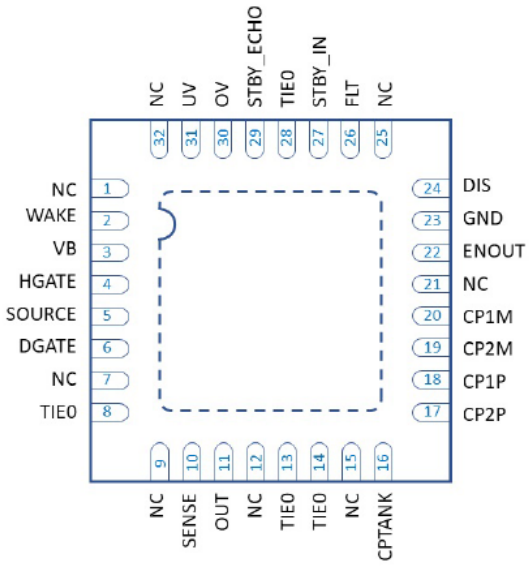


Figure 3.4: STPM801 pin out diagram [23]

add/remove/replace a component from a system while the system is still powered on. It also helps with a soft start of the MOSFET).

(b) One for OR-ing feature (Note: OR-ing feature is used for the reverse-current protection functionality).

4. Has an integrated charge pump with charge pump monitoring.
5. Has input over-voltage and under-voltage protection.
6. Output over-current protection.
7. AEC-Q100 qualified and developed according to ISO 26262 to support ASIL D application.

3.1.2.2 Safety Related Information

ST Microelectronics provides a safety manual that describes the details of each feature and the safety mechanisms. The safety manual also consists of their safety goal and safety requirements, which are defined considering the the STPM801 as a safety element out of context (SEooC). The failure modes for the STPM801 are considered as the violation of their defined safety requirements. The safety manual provides the SPFM, LFM and PMHF values for the failures of each of the safety requirement. The information on the hardware metrics is however confidential and cannot be shared publicly.

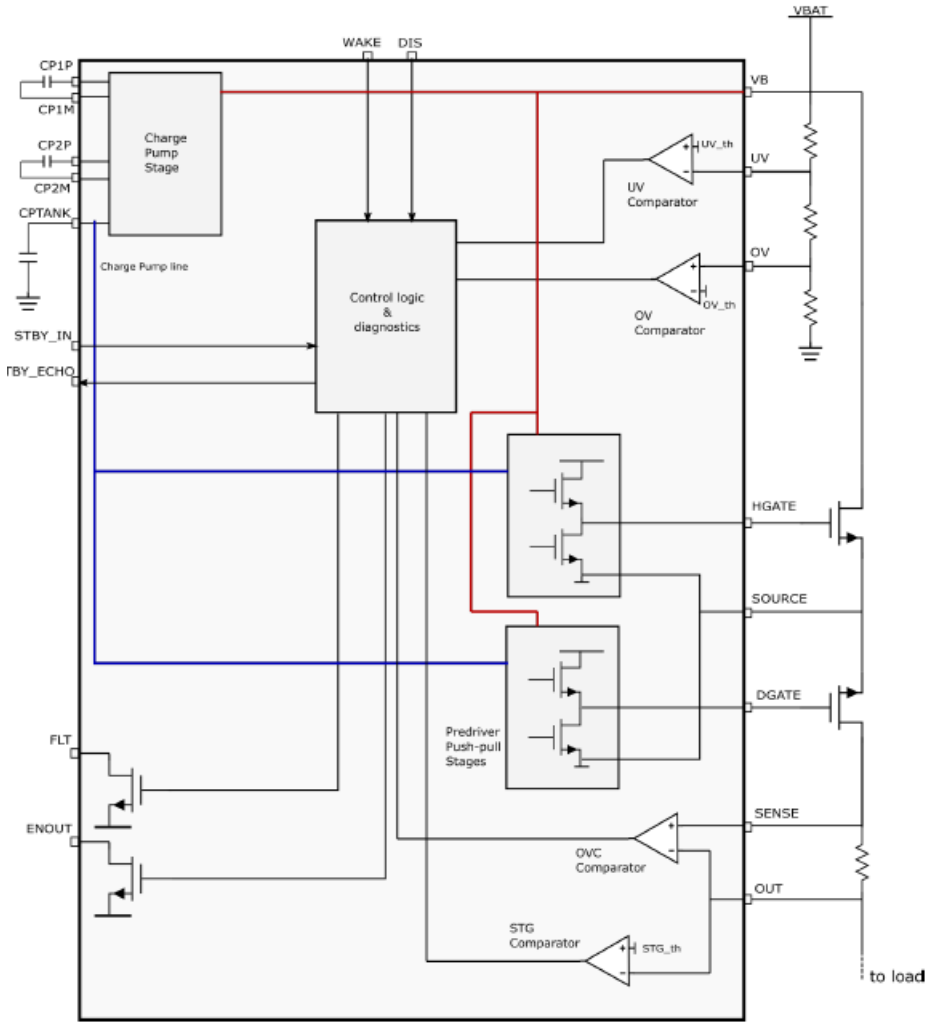


Figure 3.5: STPM801 block diagram [23]

4

Methods

To address the problem statement in Section 1.3 a functional-safety circuit is introduced between the power-supply from the DC-DC converter to the zone controller. The methodology used to achieve this design is derived from the guidelines stated by Volvo Cars Corporation (VCC) and ISO 26262:5 [4] as discussed in Section 2.6. The methodology used for this thesis project is divided into three phases as shown in Figure 4.1. The first phase is 'Analysis Phase', followed by 'Design Phase' and finally 'Result Phase'. These phases are explained in the following sections.

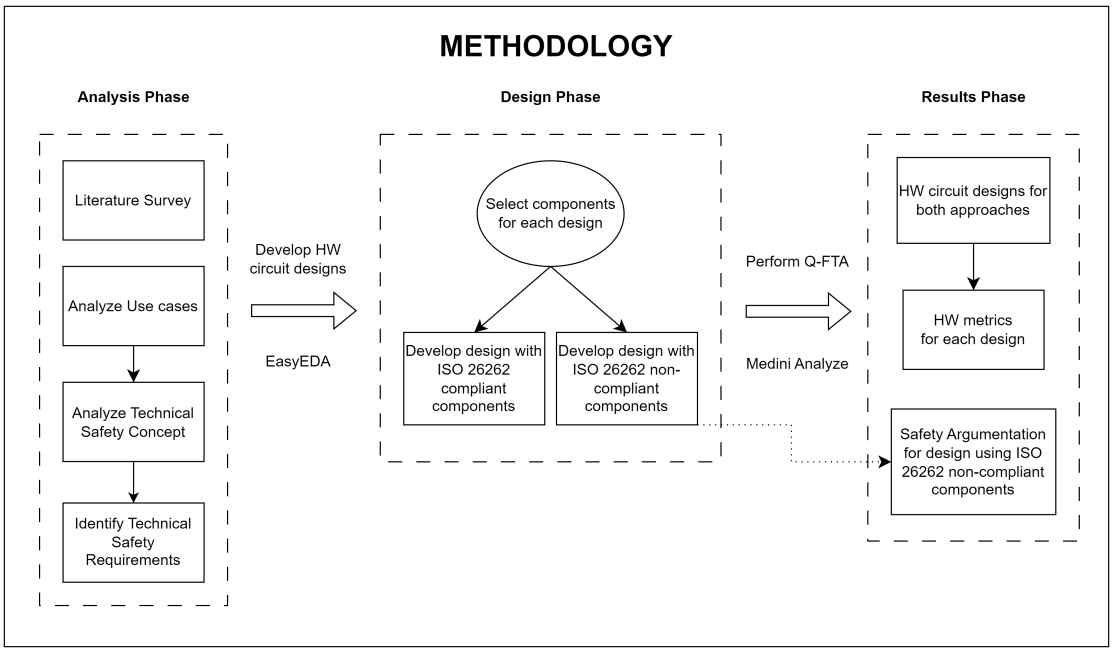


Figure 4.1: Methodology used for the thesis project.

The tools used in this thesis project are:

1. EasyEDA - Used to create the circuit schematics and generate bill of materials
2. Medini Analyze - Used for maintaining safety goal, requirements, performing FMEDA and FTA to calculate the hardware metrics (SPFM, LFM and PMHF)
3. draw.io - Used for creating block diagrams and other figures

4.1 Analysis Phase

To perform the failure analysis, the tool being used is Medini Analyze by Ansys. Medini Analyze provides a platform that allows the user to implement the entire safety process in accordance with the ISO 26262 series of standards. It can be used for requirements management at a system level, performing the hazard and risk assessment, designing system architecture, technical safety concept and performing qualitative and quantitative failure analysis. For the purpose of the project, the failure analysis and developing technical safety concept aspects of the tool are being used.

4.1.1 Safety Goal

The first step of the safety analysis is done by setting the safety goal that is to be achieved by the system. Figure 4.1 shows the safety goal of the system in Medini Analyze.

Table 4.1: Safety Goal provided by VCC

ID	Name	Description	Safe State
G001	SG001	Provide power supply to SBC from two independent power supplies	Inform application when loss of supply to allow degradation

4.1.2 Derived technical safety requirements

The technical safety requirements (TSRs) are derived from the safety goal by VCC and those are outlined in Medini Analyze as shown in Figure 4.2.

4.1.3 Assumptions

1. The power supply to the circuit being designed fulfills the ASIL D requirements.
2. The TSRs are the outcome of qualitative failure analysis performed by VCC.

List of Safety Requirements

N°	ID	Name	Description	Kind	ASIL	Traced FTA Events	Status
1	SR001	TSR 1 - Supply voltage and grounding	The element shall be connected to two independent power supplies (L and R) and maintain operation, where a single fault is not allowed to affect both power supplies simultaneously or propagate from one to the other.	TECHNICAL	D	[E57] [G001] is violated	PROPOSED
1.1	SR004	Supply voltage redundancy	There shall be two redundant voltage supplies (typically called L and R) to the element. Each redundant power supply (L and R) shall be measured separately and provided to applications. It shall be possible to maintain operation with only one of the two voltage supplies active, except for providing power to loads connected to the element where the power is exclusively supplied from the lost input.	HARDWARE	D	[E57] [G001] is violated	PROPOSED
1.2	SR005	Grounding redundancy	There shall be two redundant grounds (typically called L and R) to the element, and it shall be possible to maintain operation with only one of the two grounds.	HARDWARE	D	[E57] [G001] is violated	PROPOSED
1.3	SR006	Reverse current protection on supply lines	Any part that can consume power from both supplies (Load supplied by L+R) shall have protection against reverse current floating from one supply pin to another.	HARDWARE	D	[E57] [G001] is violated	PROPOSED

Figure 4.2: Technical Safety Requirements

4.2 Design Phase

The design phase includes mainly the following:

1. Understanding the technical safety concept (TSC).
2. Designing the hardware based on the concept.
3. Performing the FMEDA on the design by determining the failure modes of components that violate the safety goal. This is required to determine the SPFM and LFM of the design.
4. Performing quantitative FTA on the design to determine the PMHF of the design.

The first step in the design phase is to conceptualize the solution from a safety perspective. This solution is the TSC. This concept is derived from the TSRs from the analysis phase. The hardware circuit design is then realised in EasyEDA tool for designs using ISO 26262 compliant and non-compliant components. The FMEDA and FTA designs are realised in Medini Analyse tool using the bill of materials (BOM) generated by EasyEDA tool.

4.2.1 Ideal-diode controller

The component of interest in this project is the ideal-diode controller. The main purpose of the ideal-diode controller is to prevent reverse current from occurring between the two power supplies. The reason to use this component as basis of

analysis for the thesis project is due to the different operating modes and parameters it has that enables it to fulfill its functionality. The controller can either be developed as per ISO 26262:5 or be classified as a Class II hardware element, which can give an insight to understanding the differences between using compliant component and using non-compliant component for a safety application.

Other components being used in the hardware design are passive components that qualify as Class I hardware elements and therefore, are not of interest while performing the comparison.

4.2.2 Assumptions

1. The system level TSC outside the scope of the design in this project has been developed as per ISO 26262 guidelines.
2. The effect of different physical parameters influencing the failure rates are not analyzed, instead the default recommendations from the failure rate catalog have been considered.
3. ISO 26262:11 provides failure-mode libraries for a combination of components fulfilling a specific functionality (for example: passive networks, MCU with an intended functionality, etc.). However, as the failure analysis of the design in this project is done on an individual component level, IEC TR 62380 failure-mode library has been used instead.
4. For the non-compliant component used in the design, it is assumed that the supplier has done enough tests, as per ISO 26262:8-13, to ensure that the effects of any systematic failure that can occur is not critical.

4.3 Results Phase

The results phase includes analyzing the obtained results from the Medini tool and developing a proposal to improve failure metrics for both designs. The point of reference used to determine the target metrics are defined by the ASIL classification of the requirement. In this thesis project, the aim is to fulfill the target metrics of ASIL D. The result phase deals with the interpretation of the results obtained from each design, the design constraints of the components used, identify key differences between the features of the components.

4.3.1 Scope limitation

The limitations of the scope of the thesis project is listed below.

1. The hardware realization of the designs falls outside the scope of this project.
2. The verification and validation of the designs are out of scope for this project.
3. The scope is limited to the results obtained from the quantitative failure analysis.

5

Design

This chapter discusses the TSC, the circuit designs using the non-compliant component and the compliant component along with the failure analysis done on both the circuits using the Medini Analyze tool.

5.1 Technical Safety Concept

The TSC consists of the technical safety architecture (TSA) and the technical safety requirements (TSRs). To fulfill the safety-goal and the TSRs defined in Section 4.1, a functional-safety circuit using the non-compliant component has been provided. The TSA shown in Figure 5.1 gives the overview of the circuit and the control unit in the zone controller.

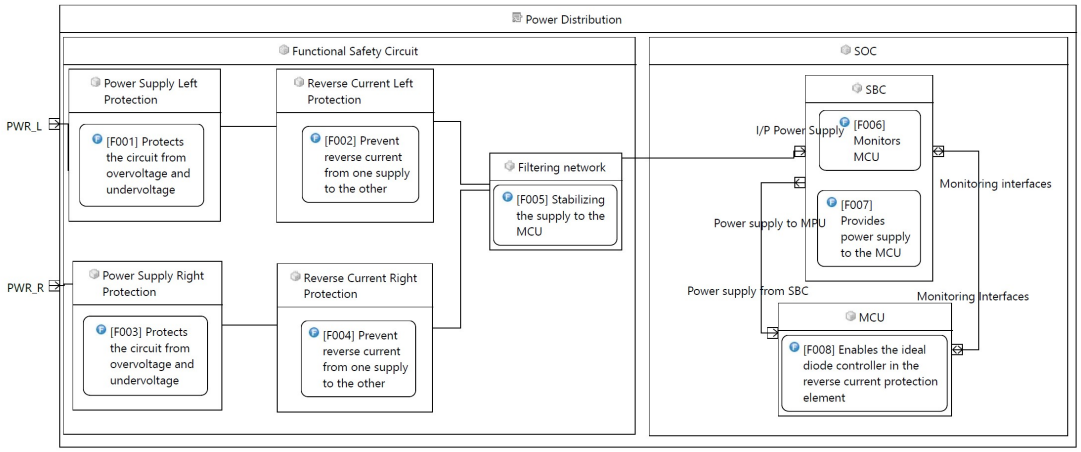


Figure 5.1: Technical Safety Architecture

The functional-safety circuit takes inputs from the left and right DC-DC converters (PWR_L and PWR_R). To fulfill TSR 1.1 and TSR 1.2, one of the inputs is used as a redundant power supply which is used only if the other input fails. The functional-safety circuit is divided into circuit blocks as shown in Figure 5.1. To satisfy TSR 1.3, each supply has an overshoot protection and a reverse-current protection to prevent current flowing from one supply to the other in case of voltage imbalances in the inputs. The blocks associated with PWR_R are denoted as "right" blocks, while those associated with PWR_L are denoted as "left" blocks. The output of the

reverse-current-protection blocks are filtered and rectified before supplying to the control unit.

This TSC is applicable to the design that uses a compliant component and also the design that uses a non-compliant component.

5.2 Design using ISO 26262 non-compliant component

In this section, the hardware design of the circuit with the non-compliant component is shown. The FMEDA analysis and the FTAs for each circuit block linking to the safety goal is also shown.

5.2.1 Hardware design and failure rate allocation

The circuit design with the non-compliant component (LM74700) is shown in Figure 5.2.

There are 16 capacitors used with different capacitance values, four resistors of 1 kΩ, two TPSMA18AHE3_B/I universal diodes, two KDZVTFTR36B low-power Zener diodes, one VSSAF5M10HM3/H Schottky diode, four SQJ140EP-T1_GE3 MOSFETs, one 100 µH/35 V choke coil and two LM74700-QDDFRQ1 ideal-diode controllers. The entire BOM used for the design is shown in Figure 5.3.

The list of failure modes already available in Medini Analyze is shown in Figure 5.4.

The failure-mode library used for the failure analysis is IEC 62380 failure modes. The reason to use this failure-mode library is already explained is Section 4.2.2.

5.2.1.1 Transient-Voltage Suppression (TVS) block

The TVS blocks are the first block after both DC-DC converters. The TVS circuit block consists of two capacitors in series which is in parallel to a branch of TPSMA18AHE3_B/I and KDZVTFTR36B diodes in series. This circuit block suppresses any transient-voltage spikes from the DC-DC converter to protect the circuitry ahead of the TVS circuit block.

5.2.1.2 Reverse-current-protection block

There are two reverse-current-protection circuit blocks, one after each TVS circuit block from the DC-DC converters. Each reverse-current-protection block has three capacitors of 0.1 µF, two resistors of 1 kΩ, two MOSFETs and one LM74700 ideal-diode controller. One of the capacitors is used to connect the 'VCAP' pin of LM74700 to the 'VCC' and the other two capacitors are connected in series between the 'ANODE' pin to the 'GND'. The MOSFETs are connected in series between the 'ANODE' and the 'CATHODE' pins of LM74700 and the resistors are connected between the gate of the MOSFETs and the 'GATE' pin of LM74700. The outputs from both the reverse-current circuit blocks are combined and current flows to the Pi-filter block explained in Section 5.2.1.3.

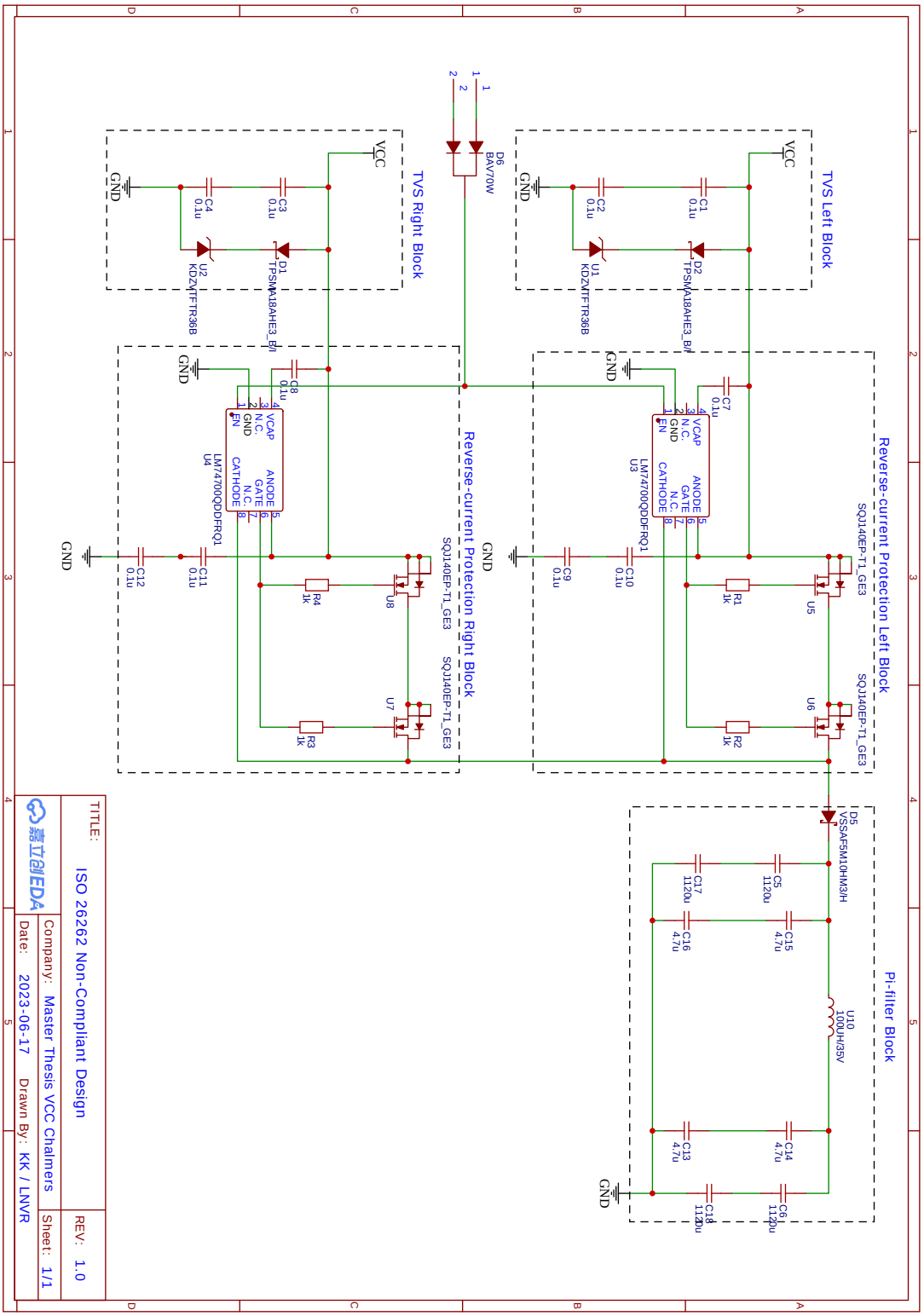
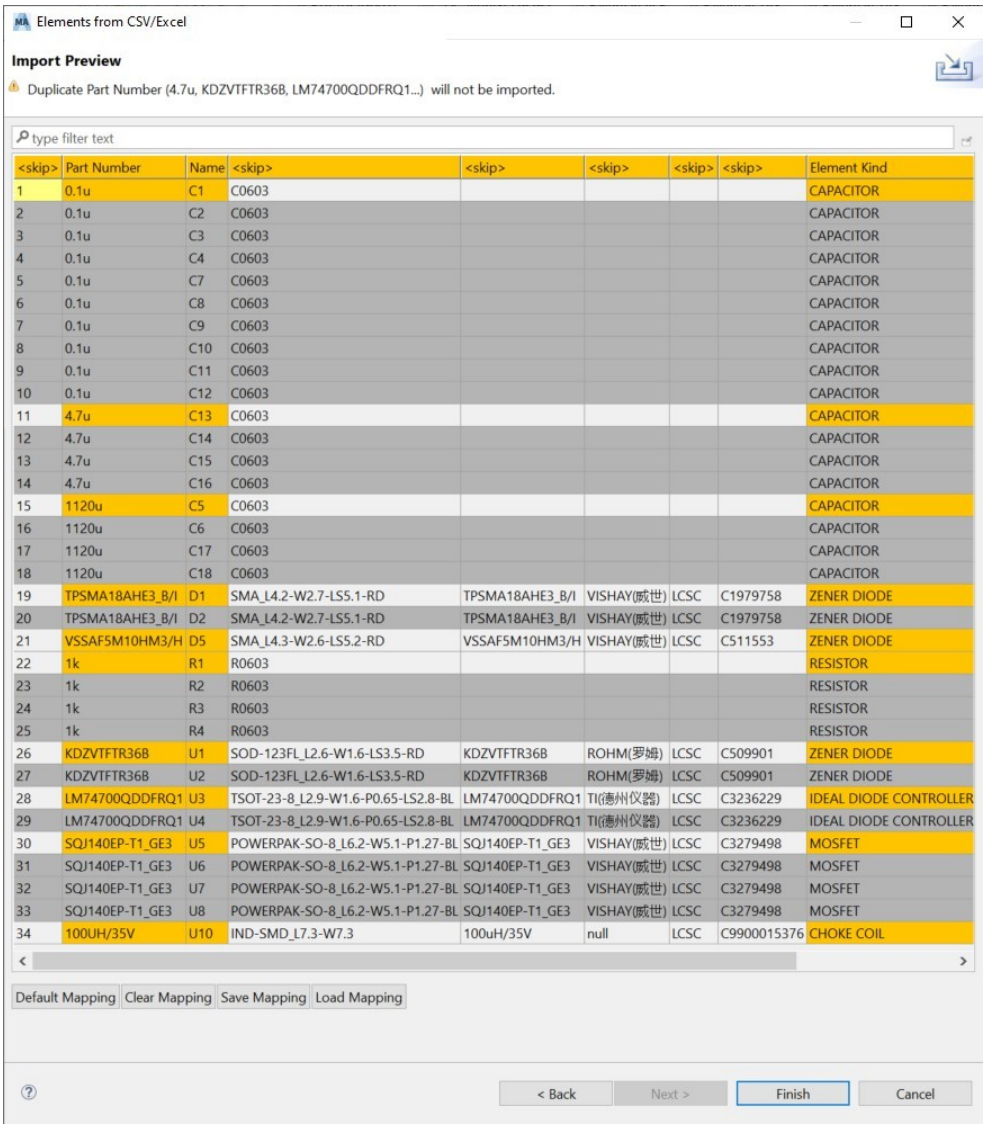


Figure 5.2: HW Schematic of Functional Safety Circuit using ISO26262 non-compliant Ideal Diode Controller (LM74700)

The reverse-current-protection blocks purpose is to prevent reverse-current flowing from the junction point. The MOSFETs are controlled by the ideal-diode controller



<skip>	Part Number	Name	<skip>	<skip>	<skip>	<skip>	<skip>	Element Kind
1	0.1u	C1	C0603					CAPACITOR
2	0.1u	C2	C0603					CAPACITOR
3	0.1u	C3	C0603					CAPACITOR
4	0.1u	C4	C0603					CAPACITOR
5	0.1u	C7	C0603					CAPACITOR
6	0.1u	C8	C0603					CAPACITOR
7	0.1u	C9	C0603					CAPACITOR
8	0.1u	C10	C0603					CAPACITOR
9	0.1u	C11	C0603					CAPACITOR
10	0.1u	C12	C0603					CAPACITOR
11	4.7u	C13	C0603					CAPACITOR
12	4.7u	C14	C0603					CAPACITOR
13	4.7u	C15	C0603					CAPACITOR
14	4.7u	C16	C0603					CAPACITOR
15	1120u	C5	C0603					CAPACITOR
16	1120u	C6	C0603					CAPACITOR
17	1120u	C17	C0603					CAPACITOR
18	1120u	C18	C0603					CAPACITOR
19	TPSMA18AHE3_B/I	D1	SMA_L4.2-W2.7-LS5.1-RD	TPSMA18AHE3_B/I	VISHAY(威世)	LCSC	C1979758	ZENER DIODE
20	TPSMA18AHE3_B/I	D2	SMA_L4.2-W2.7-LS5.1-RD	TPSMA18AHE3_B/I	VISHAY(威世)	LCSC	C1979758	ZENER DIODE
21	VSSAF5M10HM3/H	D5	SMA_L4.3-W2.6-LS5.2-RD	VSSAF5M10HM3/H	VISHAY(威世)	LCSC	C511553	ZENER DIODE
22	1k	R1	R0603					RESISTOR
23	1k	R2	R0603					RESISTOR
24	1k	R3	R0603					RESISTOR
25	1k	R4	R0603					RESISTOR
26	KDZVTFTR36B	U1	SOD-123FL_L2.6-W1.6-LS3.5-RD	KDZVTFTR36B	ROHM(罗姆)	LCSC	C509901	ZENER DIODE
27	KDZVTFTR36B	U2	SOD-123FL_L2.6-W1.6-LS3.5-RD	KDZVTFTR36B	ROHM(罗姆)	LCSC	C509901	ZENER DIODE
28	LM74700QDDFRQ1	U3	TSOT-23-8_L2.9-W1.6-P0.65-LS2.8-BL	LM74700QDDFRQ1	TI(德州仪器)	LCSC	C3236229	IDEAL DIODE CONTROLLER
29	LM74700QDDFRQ1	U4	TSOT-23-8_L2.9-W1.6-P0.65-LS2.8-BL	LM74700QDDFRQ1	TI(德州仪器)	LCSC	C3236229	IDEAL DIODE CONTROLLER
30	SQJ140EP-T1_GE3	U5	POWERPAK-SO-8_L6.2-W5.1-P1.27-BL	SQJ140EP-T1_GE3	VISHAY(威世)	LCSC	C3279498	MOSFET
31	SQJ140EP-T1_GE3	U6	POWERPAK-SO-8_L6.2-W5.1-P1.27-BL	SQJ140EP-T1_GE3	VISHAY(威世)	LCSC	C3279498	MOSFET
32	SQJ140EP-T1_GE3	U7	POWERPAK-SO-8_L6.2-W5.1-P1.27-BL	SQJ140EP-T1_GE3	VISHAY(威世)	LCSC	C3279498	MOSFET
33	SQJ140EP-T1_GE3	U8	POWERPAK-SO-8_L6.2-W5.1-P1.27-BL	SQJ140EP-T1_GE3	VISHAY(威世)	LCSC	C3279498	MOSFET
34	100UH/35V	U10	IND-SMD_L7.3-W7.3	100uH/35V	null	LCSC	C9900015376	CHOKE COIL

Figure 5.3: HW part Library created from Bill of Materials

to block any reverse current. The LM74700 controls the MOSFETs by keeping them closed to allow forward current and turns the MOSFETs OFF during any reverse-current event.

5.2.1.3 Pi-filter block

The Pi-filter block has a set of capacitors in parallel, one VSSAF5M10HM3/H Schottky diode and a 100 µH/35 V choke-coil inductor. This set of components is used to protect the circuitry from any external electromagnetic interference (EMI) and rectification of the supply from the DC-DC converters. The intention is to finally have a stable DC voltage to the control unit from the Pi-filter block.

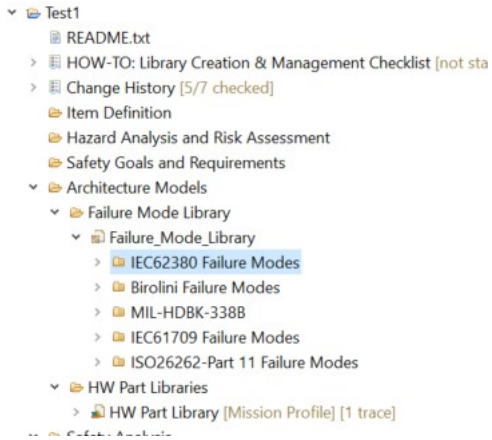


Figure 5.4: Failure Mode Library available in Medini Analyze

5.2.1.4 Failure-mode allocation

The allocation of the failure modes to the components is shown in Figure 5.5.

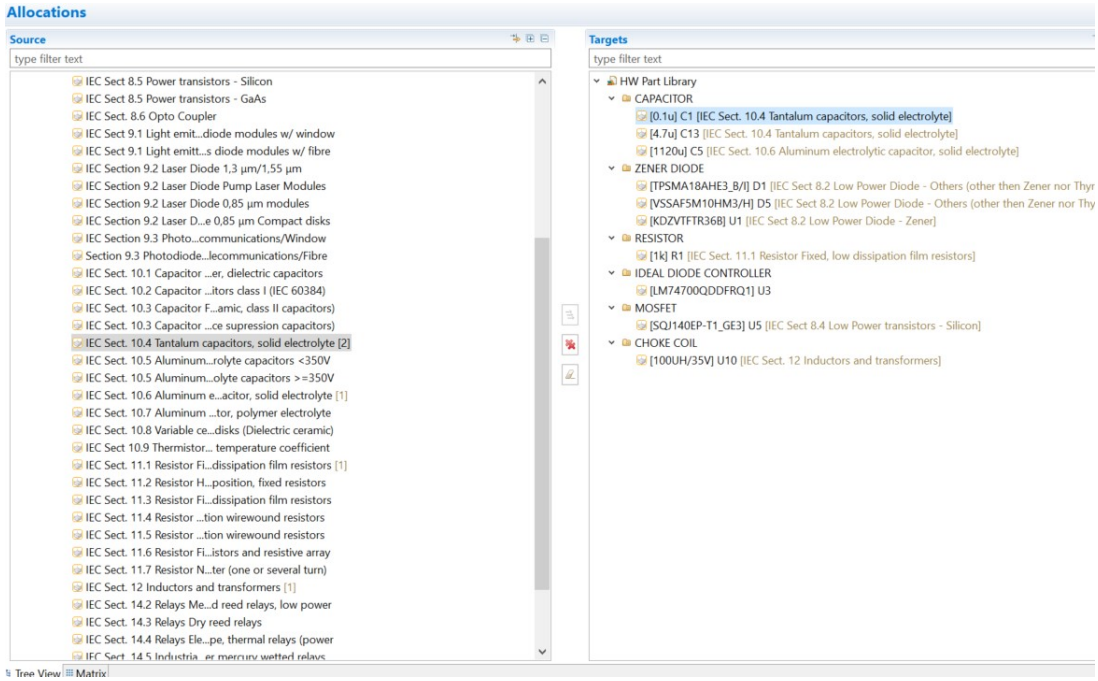


Figure 5.5: Allocating failure modes to component part numbers

The SN 29500 failure-rate catalog is used to assign the FIT rates for the components used in the design. The set of components available in SN 29500 catalog for failure rates is shown in Figure 5.6. The failure rates for the passive components are imported using the SN 29500 catalog but for the LM74700 ideal-diode controller, the failure modes and failure rates are defined manually as provided by Texas Instruments.

The hardware parts with the individual failure rates and failure modes are shown in Figure 5.7.

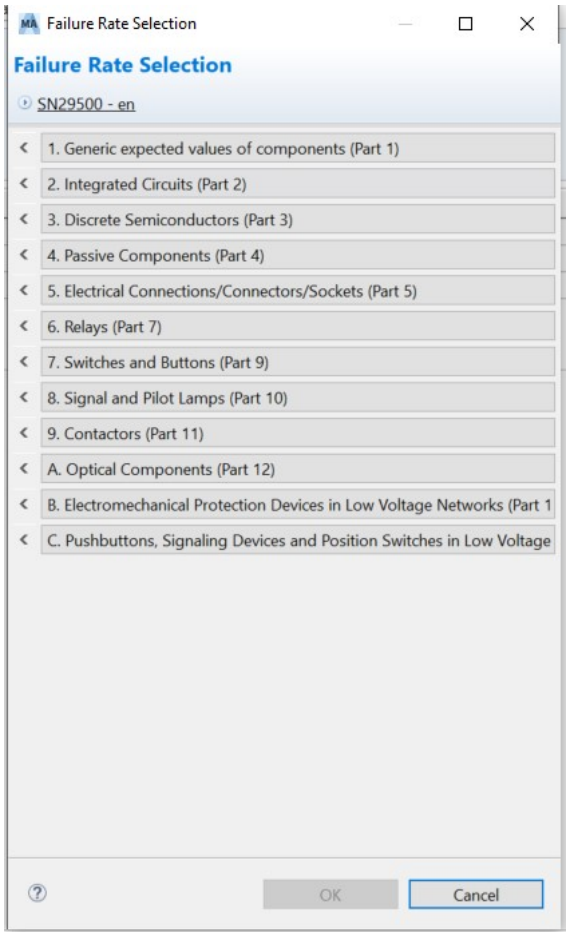


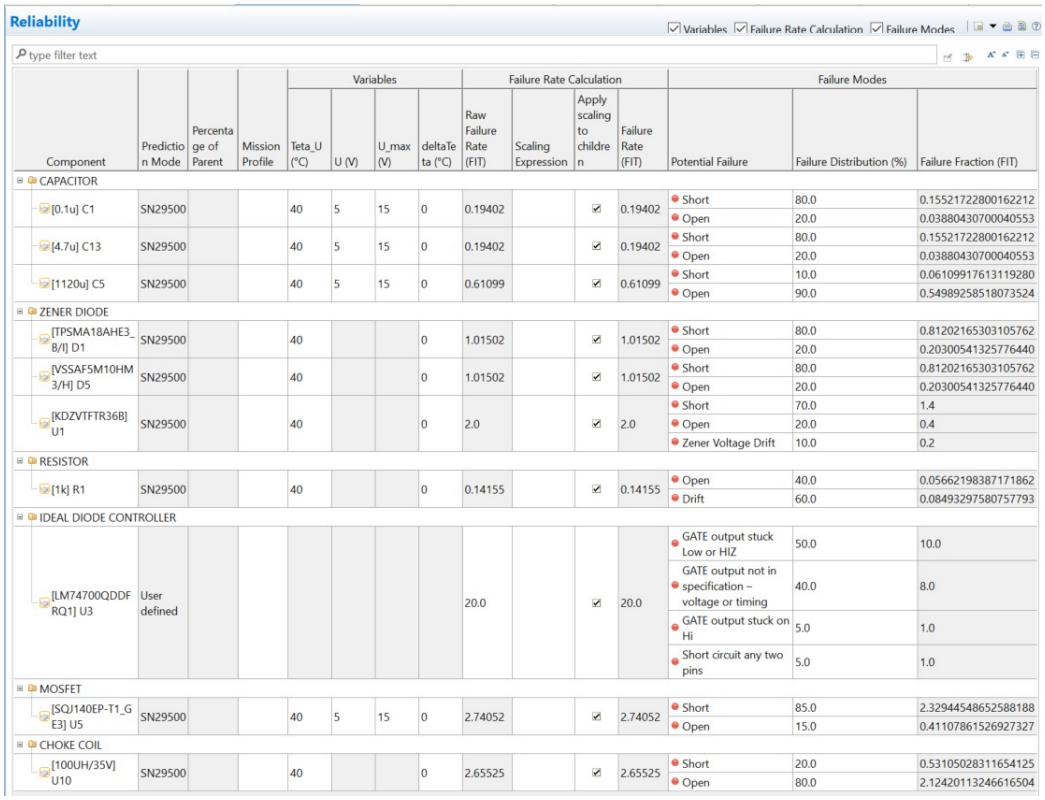
Figure 5.6: SN29500 Failure rate catalog

5.2.2 FMEDA

The FMEDA is done for the circuit in Figure 5.2 by analyzing the failure modes for different components which could potentially violate the top-level safety goal. The safe-fault distribution for failure modes of different components is estimated by analyzing the percentage of failures which could lead to not providing power to the control unit.

5.2.2.1 TVS blocks

There are two TVS blocks of circuits used as shown in Figure 5.2, one for each output from the DC-DC converters. There are two capacitors, one TPSMA18AHE3_B/I diode and one KDZVTFTR36B Zener diode used in a TVS circuit block. Based on the circuit design in Figure 5.2, a 'Short' in all the four capacitors leads to a failure in the power supply circuit since it leads to a short between 'VCC' and 'GND'. This is the reason a 75% safe fault distribution is allotted for all the four capacitors with a 'Short' failure mode. An 'Open' failure in any of the capacitors would not affect the functionality of the circuit hence they are not selected to be violating the safety goal. Similarly, the TVS diodes, 'U1', 'U2', 'D1' and 'D2' are used as shown in Figure 5.2. Similar to the capacitors, only a 'Short' failure mode in all the four diodes leads to



Reliability

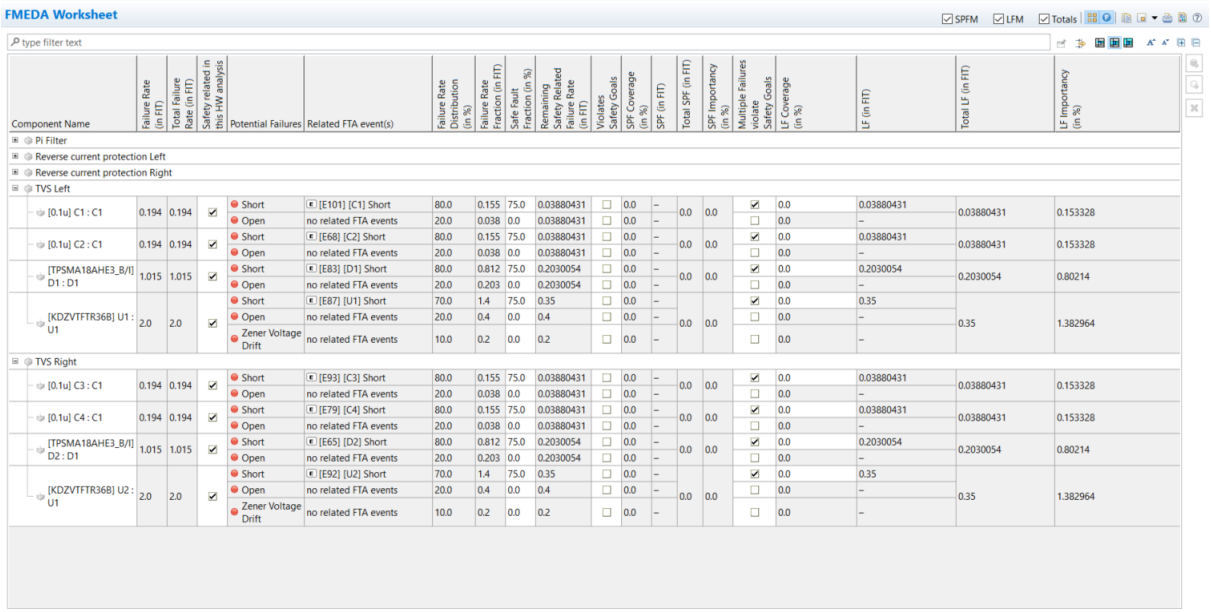
Variables | Failure Rate Calculation | Failure Modes

type filter text

Component	Prediction Mode	Percentage of Parent	Mission Profile	Variables: Teta_U (°C)	Variables: U (V)	Variables: U_max (V)	Variables: deltaTeta (°C)	Failure Rate Calculation: Raw Failure Rate (FIT)	Failure Rate Calculation: Scaling Expression	Failure Rate Calculation: Apply scaling to children	Failure Rate Calculation: Failure Rate (FIT)	Failure Modes: Potential Failure	Failure Modes: Failure Distribution (%)	Failure Modes: Failure Fraction (FIT)
CAPACITOR														
[0.1u] C1	SN29500			40	5	15	0	0.19402		☑	0.19402	Short	80.0	0.15521722800162212
												Open	20.0	0.03880430700040553
[4.7u] C13	SN29500			40	5	15	0	0.19402		☑	0.19402	Short	80.0	0.15521722800162212
												Open	20.0	0.03880430700040553
[1120u] C5	SN29500			40	5	15	0	0.61099		☑	0.61099	Short	10.0	0.06109917613119280
												Open	90.0	0.54989258518073524
ZENER DIODE														
[TPSMA18AHE3_B/I] D1	SN29500			40			0	1.01502		☑	1.01502	Short	80.0	0.81202165303105762
												Open	20.0	0.20300541325776440
[VSSAF5M10HM3/H] D5	SN29500			40			0	1.01502		☑	1.01502	Short	80.0	0.81202165303105762
												Open	20.0	0.20300541325776440
[KDZVTFTR36B] U1	SN29500			40			0	2.0		☑	2.0	Short	70.0	1.4
												Open	20.0	0.4
												Zener Voltage Drift	10.0	0.2
RESISTOR														
[1k] R1	SN29500			40			0	0.14155		☑	0.14155	Open	40.0	0.05662198387171862
												Drift	60.0	0.08493297580757793
IDEAL DIODE CONTROLLER														
[LM74700QDDFRQ1] U3	User defined							20.0		☑	20.0	GATE output stuck Low or HIZ	50.0	10.0
												GATE output not in specification – voltage or timing	40.0	8.0
												GATE output stuck on Hi	5.0	1.0
												Short circuit any two pins	5.0	1.0
MOSFET														
[SQJ140EP-T1_GE3] U5	SN29500			40	5	15	0	2.74052		☑	2.74052	Short	85.0	2.32944548652588188
												Open	15.0	0.41107861526927327
CHOKE COIL														
[100UH/35V] U10	SN29500			40			0	2.65525		☑	2.65525	Short	20.0	0.53105028311654125
												Open	80.0	2.12420113246616504

Figure 5.7: HW parts with their failure rates and respective failure modes

a complete failure in the power supply. Since the diodes are different, a 50% safe fault distribution for all the four diodes are allotted. The FMEDA analysis for the TVS circuit blocks is shown in Figure 5.8.



FMEDA Worksheet

SPFM | LFM | Totals

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Related FTA event(s)	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Total SPF (in FIT)	SPF Importancy (in %)	Multiple Failures violate Safety Goals	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
Pi Filter																			
Reverse current protection Left																			
Reverse current protection Right																			
TVS Left																			
[0.1u] C1 : C1	0.194	0.194	☑	Short	[E101] [C1] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[0.1u] C2 : C1	0.194	0.194	☑	Short	[E68] [C2] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[TPSMA18AHE3_B/I] D1 : D1	1.015	1.015	☑	Short	[E83] [D1] Short	80.0	0.812	75.0	0.2030054	☐	0.0	–	0.0	0.0	☑	0.0	0.2030054	0.2030054	0.80214
				Open	no related FTA events	20.0	0.203	0.0	0.2030054	☐	0.0	–			☐	0.0	–		
[KDZVTFTR36B] U1 : U1	2.0	2.0	☑	Short	[E87] [U1] Short	70.0	1.4	75.0	0.35	☐	0.0	–	0.0	0.0	☑	0.0	0.35	0.35	1.382964
				Open	no related FTA events	20.0	0.4	0.0	0.4	☐	0.0	–			☐	0.0	–		
				Zener Voltage Drift	no related FTA events	10.0	0.2	0.0	0.2	☐	0.0	–			☐	0.0	–		
TVS Right																			
[0.1u] C3 : C1	0.194	0.194	☑	Short	[E93] [C3] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[0.1u] C4 : C1	0.194	0.194	☑	Short	[E79] [C4] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[TPSMA18AHE3_B/I] D2 : D1	1.015	1.015	☑	Short	[E65] [D2] Short	80.0	0.812	75.0	0.2030054	☐	0.0	–	0.0	0.0	☑	0.0	0.2030054	0.2030054	0.80214
				Open	no related FTA events	20.0	0.203	0.0	0.2030054	☐	0.0	–			☐	0.0	–		
[KDZVTFTR36B] U2 : U1	2.0	2.0	☑	Short	[E92] [U2] Short	70.0	1.4	75.0	0.35	☐	0.0	–	0.0	0.0	☑	0.0	0.35	0.35	1.382964
				Open	no related FTA events	20.0	0.4	0.0	0.4	☐	0.0	–			☐	0.0	–		
				Zener Voltage Drift	no related FTA events	10.0	0.2	0.0	0.2	☐	0.0	–			☐	0.0	–		

Figure 5.8: FMEDA for the left and right TVS blocks

5.2.2.2 Reverse-current-protection blocks

The FMEDA analysis for the reverse-current-protection circuits on both supplies is same since the type of components used in both the blocks are the same. The capacitors 'C9', 'C10', 'C11' and 'C12' used are connected to ground and connected to the 'ANODE' pins of the LM74700. The capacitors, when shorted, lead to a direct short between the 'VCC' and the 'GND'. This leads to a failure in controlling the MOSFETs as intended. The safe-fault distribution for each capacitor is 75% since only if three of the four capacitors are shorted, the power supply fails.

The resistors 'R1', 'R2', 'R3' and 'R4' are connected between the 'GATE' of the MOSFETs and the 'GATE' pins of LM74700. There is no issue with the functionality when the resistors are shorted as the MOSFETs can still be controlled as intended but an 'Open' failure in the resistors makes the connection between the 'GATE' of the MOSFETs and the 'GATE' pin of the LM74700 not connected. This leads to the MOSFETs being uncontrollable by LM74700. A 50% safe-fault distribution is allotted as a failure in 'R1' or 'R2' will lead to a failure in the 'reverse current protection left' failure but a functioning 'reverse current protection right' block. Similar failures occur when either 'R3' or 'R4' resistors fail but the power supply still manages to function with the 'reverse current protection left' circuit block.

The capacitors 'C7' and 'C8' are connected between the 'VCC' and the 'VCAP' pins of the LM74700. A short in the capacitors would not lead to any failures in the power supply but if the capacitors are open, there would be no supply to the LM74700 controller which leads to a failure in the reverse-current protection. The power-supply would still be intact if any one of the capacitors fail which is the reason to allocate 50% as a safe-fault distribution.

There are four OR-ing MOSFETs used, 'U5', 'U6', 'U7' and 'U8' to control current only through one direction and protect the current in the reverse direction. By analyzing the circuit, both the failure modes, 'Short' and 'Open' leads to issues in the power supply. Only if both the MOSFETs in the same circuit block are shorted, the reverse-current-protection fails. Hence, a 75% safe-fault distribution is allotted to the 'Short' failure mode for all the four MOSFETs. If any of the two MOSFETs on each protection circuit block is 'Open', the power supply fails to supply power to the loads. Hence, a safe-fault distribution of 50% is set to the 'Open' failure modes for each MOSFET.

Two ideal-diode controllers, LM74700, are used to control the MOSFETs which enables reverse-current protection between the two DC-DC converters. The failure modes and the failure-mode distribution for LM74700 provided by Texas Instruments are used for the analysis. The failure mode 'Gate output stuck on Hi' does not lead to a failure in the power supply as the MOSFETs are still active to protect the reverse-current based on the signals received by 'ANODE' and 'CATHODE' pins. The other three failures 'Gate output stuck Low or HIZ', 'Gate output not in specification - voltage or timing' and 'Short circuit any two pins' lead to a failure in protecting reverse current. Since there are two different power supplies, a failure in one LM74700 does not make the circuit non-functional. Hence, a 50% safe-fault distribution is allotted.

FMEDA Worksheet — SPFM LFM Totals

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Related FTA event(s)	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Total SPF (in FIT)	SPF Importancy (in %)	Multiple Failures violate Safety Goals	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
Pi Filter																			
Reverse current protection Left																			
[0.1u] C7 : C1	0.194	0.194	☑	Short	[E86] [C7] Short	80.0	0.155	50.0	0.07760861	☐	0.0	–	0.0	0.0	☑	0.0	0.07760861	0.09701077	0.383321
				Open	[E72] [C7] Open	20.0	0.038	50.0	0.01940215	☐	0.0	–			☑	0.0	0.01940215		
[0.1u] C9 : C1	0.194	0.194	☑	Short	[E107] [C9] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[0.1u] C10 : C1	0.194	0.194	☑	Short	[E108] [C10] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[1k] R1 : R1	0.141	0.141	☑	Open	[E100] [R1] Open	40.0	0.056	50.0	0.02831099	☐	0.0	–	0.0	0.0	☑	0.0	0.02831099	0.02831099	0.111866
				Drift	no related FTA events	60.0	0.084	0.0	0.08493298	☐	0.0	–			☐	0.0	–		
[1k] R2 : R1	0.141	0.141	☑	Open	[E90] [R2] Open	40.0	0.056	50.0	0.02831099	☐	0.0	–	0.0	0.0	☑	0.0	0.02831099	0.02831099	0.111866
				Drift	no related FTA events	60.0	0.084	0.0	0.08493298	☐	0.0	–			☐	0.0	–		
[LM74700QDDFRQ1] U3 : U3	20.0	20.0	☑	GATE output stuck Low or HIZ	[E77] [U3] GATE output stuck Low or HIZ	50.0	10.0	50.0	5.0	☐	0.0	–	0.0	0.0	☑	0.0	5.0	10.0	39.51328
				GATE output not in specification – voltage or timing	[E59] [U3] GATE output not in specification – voltage or timing	40.0	8.0	50.0	4.0	☐	0.0	–			☑	0.0	4.0		
				GATE output stuck on Hi	no related FTA events	5.0	1.0	50.0	0.5	☐	0.0	–			☑	0.0	0.5		
				Short circuit any two pins	[E70] [U3] Short circuit any two pins	5.0	1.0	50.0	0.5	☐	0.0	–			☑	0.0	0.5		
[SQJ140EP-T1_GE3] U5 : U5	2.740	2.740	☑	Short	[E103] [U5] Short	85.0	2.329	75.0	0.5823614	☐	0.0	–	0.0	0.0	☑	0.0	0.5823614	0.7879007	3.113254
				Open	[E99] [U5] Open	15.0	0.411	50.0	0.2055393	☐	0.0	–			☑	0.0	0.2055393		
[SQJ140EP-T1_GE3] U6 : U5	2.740	2.740	☑	Short	[E104] [U6] Short	85.0	2.329	75.0	0.5823614	☐	0.0	–	0.0	0.0	☑	0.0	0.5823614	0.7879007	3.113254
				Open	[E91] [U6] Open	15.0	0.411	50.0	0.2055393	☐	0.0	–			☑	0.0	0.2055393		
Reverse current protection Right																			
TVS Left																			
TVS Right																			

Figure 5.9: FMEDA for the left reverse current protection block

FMEDA Worksheet — SPFM LFM Totals

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Related FTA event(s)	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Total SPF (in FIT)	SPF Importancy (in %)	Multiple Failures violate Safety Goals	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
Pi Filter																			
Reverse current protection Left																			
Reverse current protection Right																			
[0.1u] C8 : C1	0.194	0.194	☑	Short	[E96] [C8] Short	80.0	0.155	50.0	0.07760861	☐	0.0	–	0.0	0.0	☑	0.0	0.07760861	0.09701077	0.383321
				Open	[E85] [C8] Open	20.0	0.038	50.0	0.01940215	☐	0.0	–			☑	0.0	0.01940215		
[0.1u] C11 : C1	0.194	0.194	☑	Short	[E105] [C11] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[0.1u] C12 : C1	0.194	0.194	☑	Short	[E106] [C12] Short	80.0	0.155	75.0	0.03880431	☐	0.0	–	0.0	0.0	☑	0.0	0.03880431	0.03880431	0.153328
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[1k] R3 : R1	0.141	0.141	☑	Open	[E81] [R3] Open	40.0	0.056	50.0	0.02831099	☐	0.0	–	0.0	0.0	☑	0.0	0.02831099	0.02831099	0.111866
				Drift	no related FTA events	60.0	0.084	0.0	0.08493298	☐	0.0	–			☐	0.0	–		
[1k] R4 : R1	0.141	0.141	☑	Open	[E62] [R4] Open	40.0	0.056	50.0	0.02831099	☐	0.0	–	0.0	0.0	☑	0.0	0.02831099	0.02831099	0.111866
				Drift	no related FTA events	60.0	0.084	0.0	0.08493298	☐	0.0	–			☐	0.0	–		
[LM74700QDDFRQ1] U4 : U3	20.0	20.0	☑	GATE output stuck Low or HIZ	[E69] [U4] GATE output stuck Low or HIZ	50.0	10.0	50.0	5.0	☐	0.0	–	0.0	0.0	☑	0.0	5.0	10.0	39.51328
				GATE output not in specification – voltage or timing	[E75] [U4] GATE output not in specification – voltage or timing	40.0	8.0	50.0	4.0	☐	0.0	–			☑	0.0	4.0		
				GATE output stuck on Hi	no related FTA events	5.0	1.0	50.0	0.5	☐	0.0	–			☑	0.0	0.5		
				Short circuit any two pins	[E89] [U4] Short circuit any two pins	5.0	1.0	50.0	0.5	☐	0.0	–			☑	0.0	0.5		
[SQJ140EP-T1_GE3] U7 : U5	2.740	2.740	☑	Short	[E102] [U7] Short	85.0	2.329	75.0	0.5823614	☐	0.0	–	0.0	0.0	☑	0.0	0.5823614	0.7879007	3.113254
				Open	[E109] [U7] Open	15.0	0.411	50.0	0.2055393	☐	0.0	–			☑	0.0	0.2055393		
[SQJ140EP-T1_GE3] U8 : U5	2.740	2.740	☑	Short	[E80] [U8] Short	85.0	2.329	75.0	0.5823614	☐	0.0	–	0.0	0.0	☑	0.0	0.5823614	0.7879007	3.113254
				Open	[E110] [U8] Open	15.0	0.411	50.0	0.2055393	☐	0.0	–			☑	0.0	0.2055393		
TVS Left																			
TVS Right																			

Figure 5.10: FMEDA for the right reverse current protection block

The entire FMEDA analysis from both the reverse-current-protection blocks in shown in Figure 5.9 and Figure 5.10.

5.2.2.3 Pi-filter block

For the Pi-filter in the circuit, the power distribution fails if both the capacitors on each branch are shorted. Hence, the 'Short' failure mode for the capacitors is a possibility which could violate the safety goal. These failures are multiple faults as only if both the capacitors on the branch fails, it leads to loss of power. The safe-

FMEDA Worksheet

SPFM LFM Totals

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Related FTA event(s)	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Total SPF (in FIT)	SPF Importancy (in %)	Multiple Failures Violate Safety Goals	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
Pi Filter																			
[4.7u] C13 : C13	0.194	0.194	☑	Short	[E67] [C13] Short	80.0	0.155	50.0	0.07760861	☐	0.0	–	0.0	0.0	☑	0.0	0.07760861	0.07760861	0.306657
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[4.7u] C14 : C13	0.194	0.194	☑	Short	[E82] [C14] Short	80.0	0.155	50.0	0.07760861	☐	0.0	–	0.0	0.0	☑	0.0	0.07760861	0.07760861	0.306657
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[4.7u] C15 : C13	0.194	0.194	☑	Short	[E58] [C15] Short	80.0	0.155	50.0	0.07760861	☐	0.0	–	0.0	0.0	☑	0.0	0.07760861	0.07760861	0.306657
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[4.7u] C16 : C13	0.194	0.194	☑	Short	[E76] [C16] Short	80.0	0.155	50.0	0.07760861	☐	0.0	–	0.0	0.0	☑	0.0	0.07760861	0.07760861	0.306657
				Open	no related FTA events	20.0	0.038	0.0	0.03880431	☐	0.0	–			☐	0.0	–		
[1120u] C5 : C5	0.610	0.610	☑	Short	[E84] [C5] Short	10.0	0.061	50.0	0.03054959	☐	0.0	–	0.0	0.0	☑	0.0	0.03054959	0.03054959	0.120711
				Open	no related FTA events	90.0	0.549	0.0	0.5498926	☐	0.0	–			☐	0.0	–		
[1120u] C6 : C5	0.610	0.610	☑	Short	[E71] [C6] Short	10.0	0.061	50.0	0.03054959	☐	0.0	–	0.0	0.0	☑	0.0	0.03054959	0.03054959	0.120711
				Open	no related FTA events	90.0	0.549	0.0	0.5498926	☐	0.0	–			☐	0.0	–		
[1120u] C17 : C5	0.610	0.610	☑	Short	[E74] [C17] Short	10.0	0.061	50.0	0.03054959	☐	0.0	–	0.0	0.0	☑	0.0	0.03054959	0.03054959	0.120711
				Open	no related FTA events	90.0	0.549	0.0	0.5498926	☐	0.0	–			☐	0.0	–		
[1120u] C18 : C5	0.610	0.610	☑	Short	[E98] [C18] Short	10.0	0.061	50.0	0.03054959	☐	0.0	–	0.0	0.0	☑	0.0	0.03054959	0.03054959	0.120711
				Open	no related FTA events	90.0	0.549	0.0	0.5498926	☐	0.0	–			☐	0.0	–		
[VSSAF5M10HM3/H] D5 : D5	1.015	1.015	☑	Short	no related FTA events	80.0	0.812	0.0	0.8120217	☐	0.0	–	0.20	8.723	☐	0.0	–	0.0	0.0
				Open	[E64] [D5] Open	20.0	0.203	0.0	0.2030054	☑	0.0	0.20			☐	0.0	–		
[100UH/35V] U10 : U10	2.655	2.655	☑	Short	no related FTA events	20.0	0.531	0.0	0.5310503	☐	0.0	–	2.12	91.27	☐	0.0	–	0.0	0.0
				Open	[E78] [U10] Open	80.0	2.124	0.0	2.124201	☑	0.0	2.12			☐	0.0	–		
Reverse current protection Left																			
Reverse current protection Right																			
TVS Left																			
TVS Right																			

Figure 5.11: FMEDA for the Pi-filter block

fault distribution for the capacitors is 50% since there is always another capacitor on the same branch which could mitigate the effect of a failure in one capacitor. The power-supply fails if the choke coil is open but has no effects in providing power if it is closed. Similarly, the power-supply fails if the diode VSSAF5M10HM3/H is open. These are single-point faults as it is not dependent on any failure in other components. The consolidated FMEDA for the Pi-filter is shown in Figure 5.11.

5.2.3 Quantified fault tree analysis

The quantified FTA is derived from the FMEDA analysis. The failure-mode analysis done in FMEDA are used in the FTAs. The FTA can be considered as a visualisation of the analysis done in FMEDA. The PMHF metric is calculated by connecting different failure modes of different components with either 'AND' or 'OR' gates to imply that a combination of different failure modes occurring together violates the safety-goal. A failure in the safety-goal occurs only if there is a failure in the Pi-filter or a combination of failures in the reverse-current circuit blocks and the a combination of failures in the TVS circuit blocks. This combination of failures which violates the safety-goal is analyzed by performing a truth table analysis as shown in Figure 5.12. The resulting FTA for the violation of the safety-goal is shown in Figure 5.13.

The FTAs for the TVS blocks is represented based on the FMEDA analysis as shown in Figure 5.14 and Figure 5.15.

Similarly, the FTAs for the reverse-current-protection blocks is shown in Figure 5.16 and Figure 5.17.

Finally, the FTA for the Pi-filter circuit block is as shown in Figure 5.18.

TVS Left	TVS Right	RC Left	RC Right	Failure of top level event
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	0
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1
				0 - No failure
				1 - Failure

Figure 5.12: Truth table for analyzing the TVS and the reverse current blocks

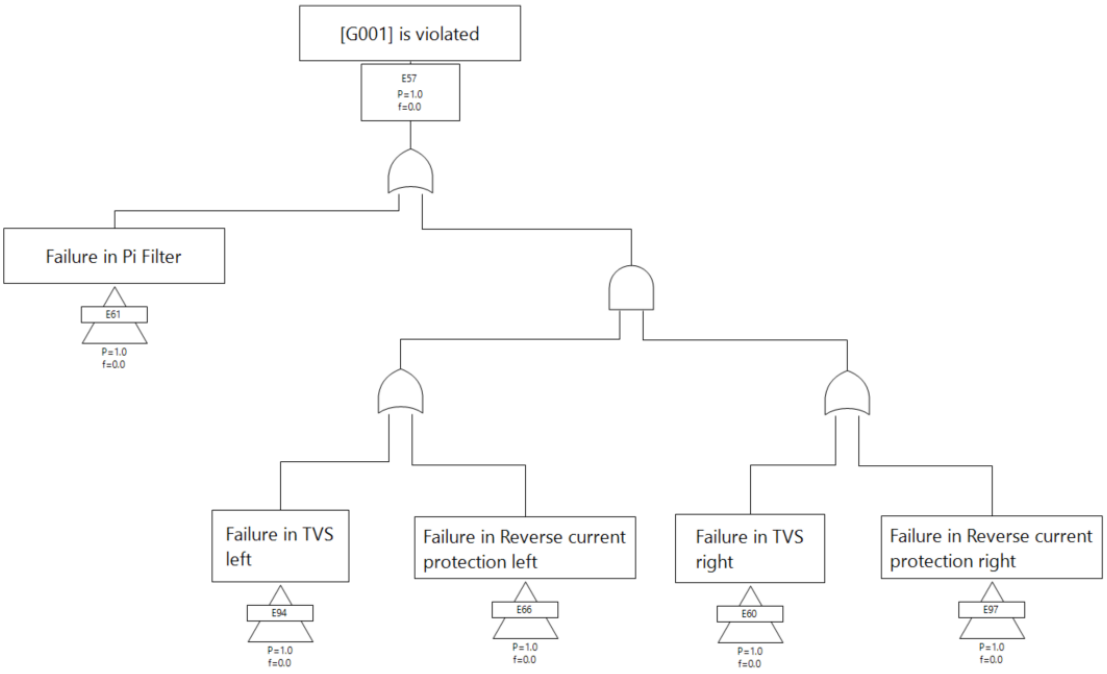


Figure 5.13: FTA of Safety Goal violation

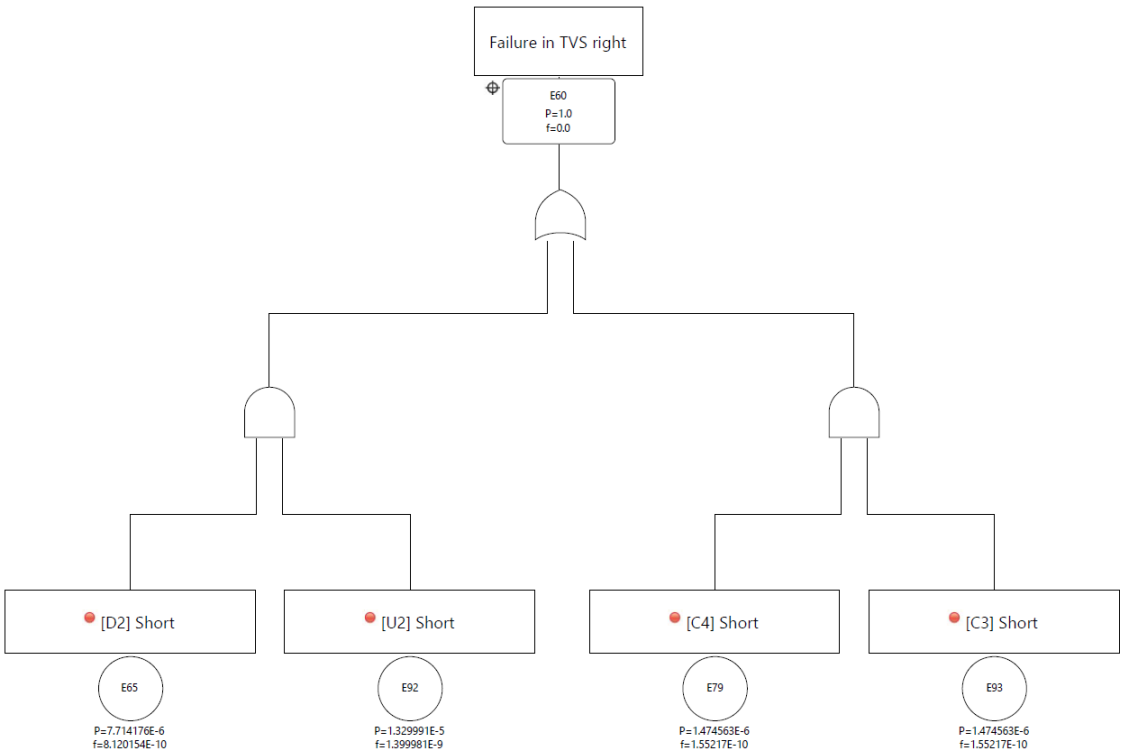


Figure 5.14: FTA of TVS Right Circuit Block

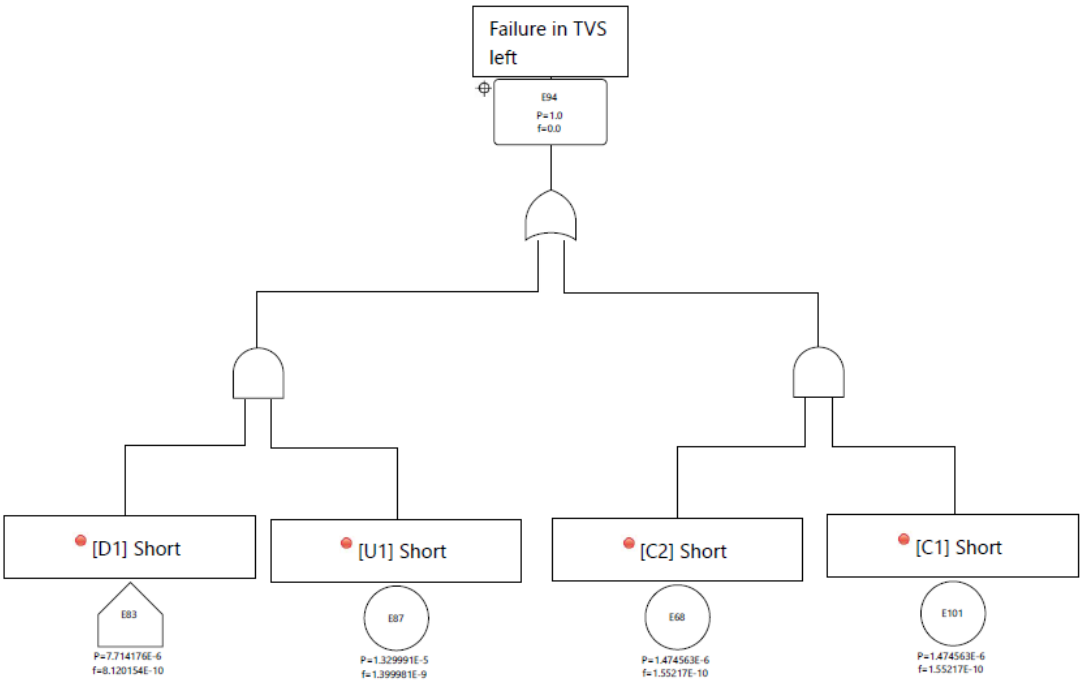


Figure 5.15: FTA of TVS Left Circuit Block

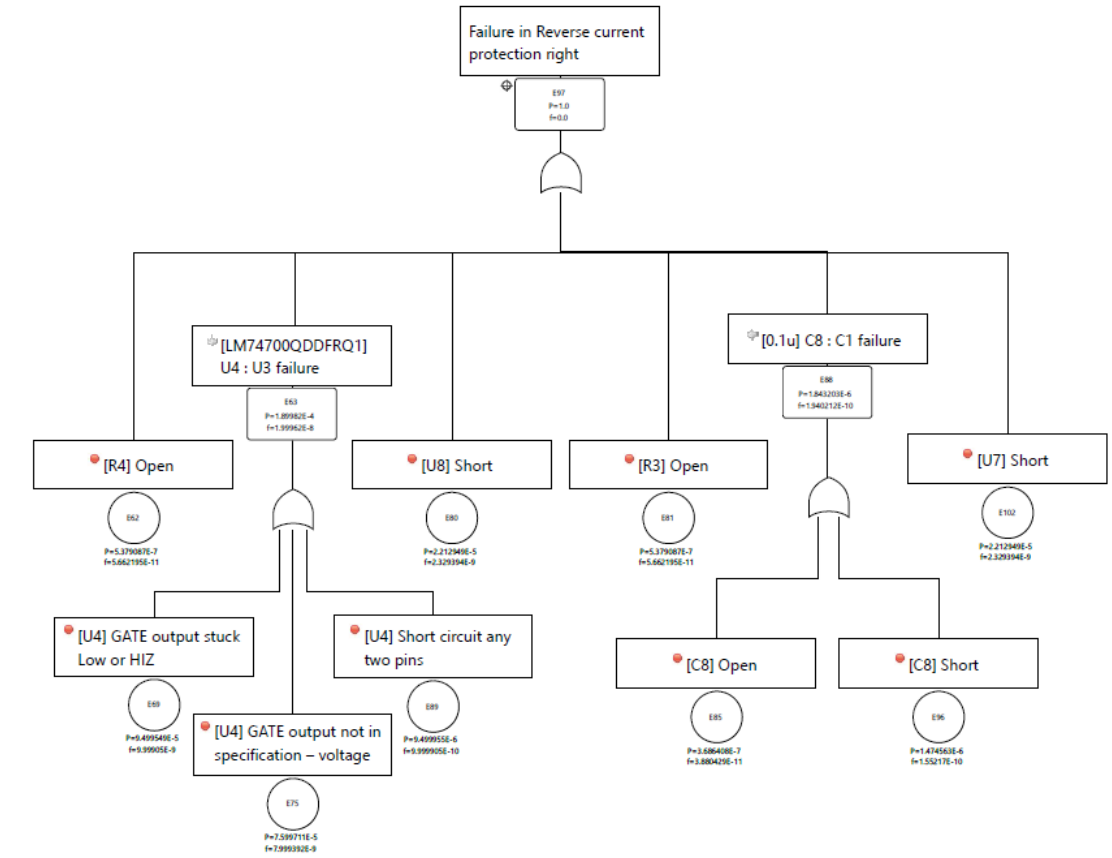


Figure 5.16: FTA of Reverse Current Protection Right Circuit Block

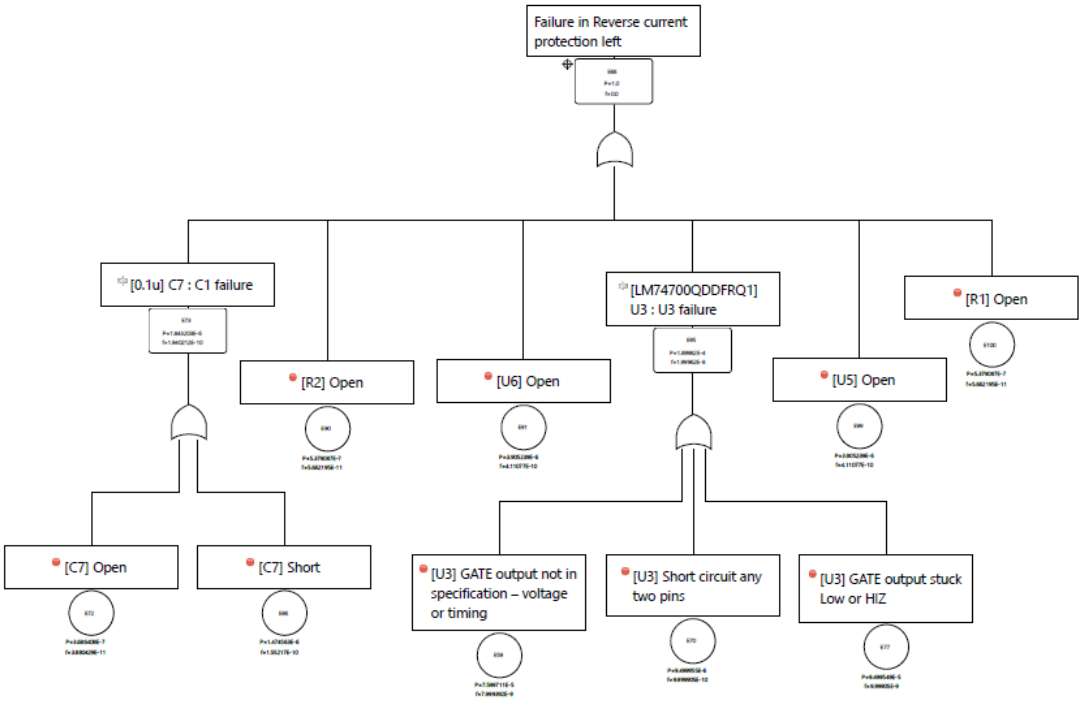


Figure 5.17: FTA of Reverse Current Protection Left Circuit Block

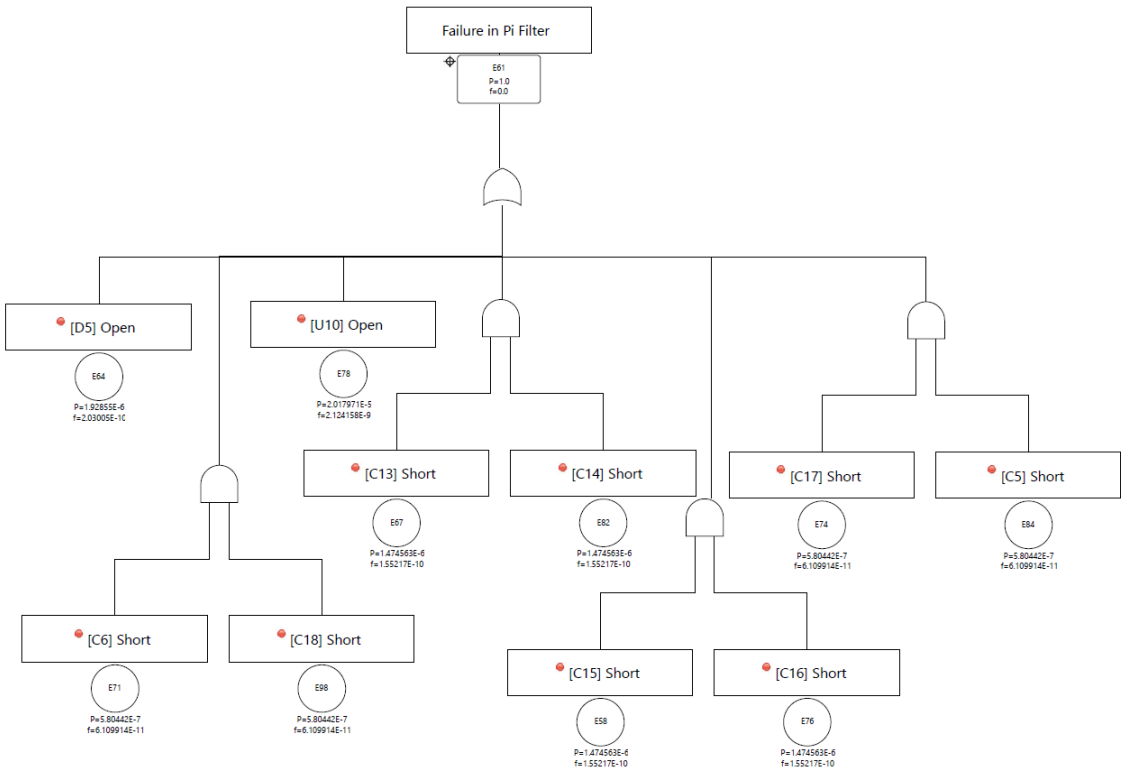


Figure 5.18: FTA of Pi-filter Circuit block

5.3 Design using ISO26262 compliant component

This section discusses the design considerations taken for the functional-safety circuit developed using ISO 26262 compliant component. The features of the ISO 26262 compliant component (STPM801), the hardware design schematic, FMEDA analysis and the FTAs for each circuit block are also discussed in this section.

5.3.1 Hardware design and failure rate allocation

The hardware circuit design using STPM801 can be seen in Figure 5.19. There are 28 capacitors used with different capacitance values, 16 resistors of different resistance values, two TPSMA18AHE3_B/I diodes and two KDZVTFTR36B Zener diodes, four MM5Z12VT1G Zener diodes, four SD0805S020S1R0 Schottky diodes, one VSSAF5M10HM3/H Schottky diode, two SQJ140EP-T1_GE3 OR-ing MOSFETs, two STH315N10F7-6 hot-swap MOSFETsz, one 100 µH/35 V choke coil and two STPM801 ideal-diode controllers. The failure rates and failure modes differ based on the type of material used for the components. The failure rates and allocation of failure modes of the components are assigned in a similar method as done for design using LM74700. This is shown under the respective component types in Figure 5.20 and Figure 5.21.

The TVS left and right, and Pi-filter implementations are the same as in the design with non-compliant component. However, the reverse-current-protection left and right differs for this design.

The STPM801 provides wide range of functionalities that are utilized in this design. One functionality that is absent in the non-compliant design is the hot-swap feature. Hot-swap is a technique used to add, remove, or replace a component from a system while the system is still operational or powered on. The term "hot" refers to the fact that the process can be performed without the need to shut down or power off the system. The hot-swap feature ultimately serves as a mechanism to prevent high in-rush currents from damaging the circuit. This application is also used to soft start the MOSFET, which is a technique used to gradually increase the current supplied to the MOSFET during its initial power-up. In Figure 5.19, there are two STH315N10F7-6 hot-swap MOSFETs used for both power supplies. In the event of failure in one of the supplies, the other is used. The diode 'D2' and capacitor 'C5' are connected to the 'HGATE' pin of STPM801. The 'C5' capacitor charges slowly to ensure that the hot swap MOSFET is not switched on instantly, thereby enabling the soft start feature during initial power up, and also preventing high in-rush current from damaging the circuit during hot swapping.

The OR-ing functionality is common for both designs. In this design, the SQJ140EP-T1_GE3 is also used for the reverse-current-protection feature in both left and right power supplies. The functionality of the protection is similar to that in non-compliant design. The other functionality provided by STPM801 that is not implemented in the other design is over-current measuring at the output through the shunt resistors, 'R8' in left and 'R16' in right, connected to 'SENSE' input of the STPM801. Apart from this, an over-voltage and under-voltage monitoring at the

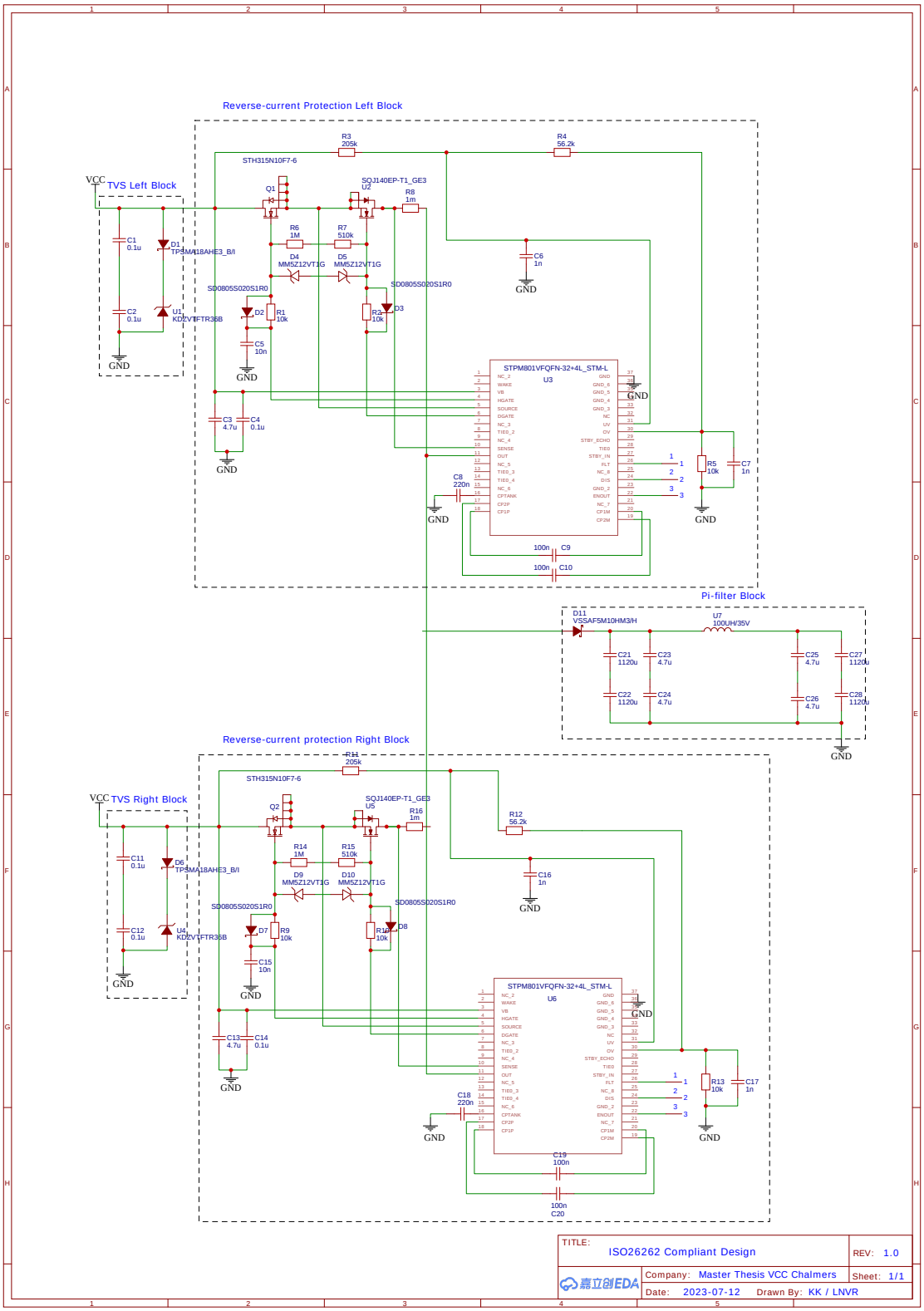


Figure 5.19: Schematic of Safety Circuit using ISO26262 compliant Ideal Diode Controller (STPM801)

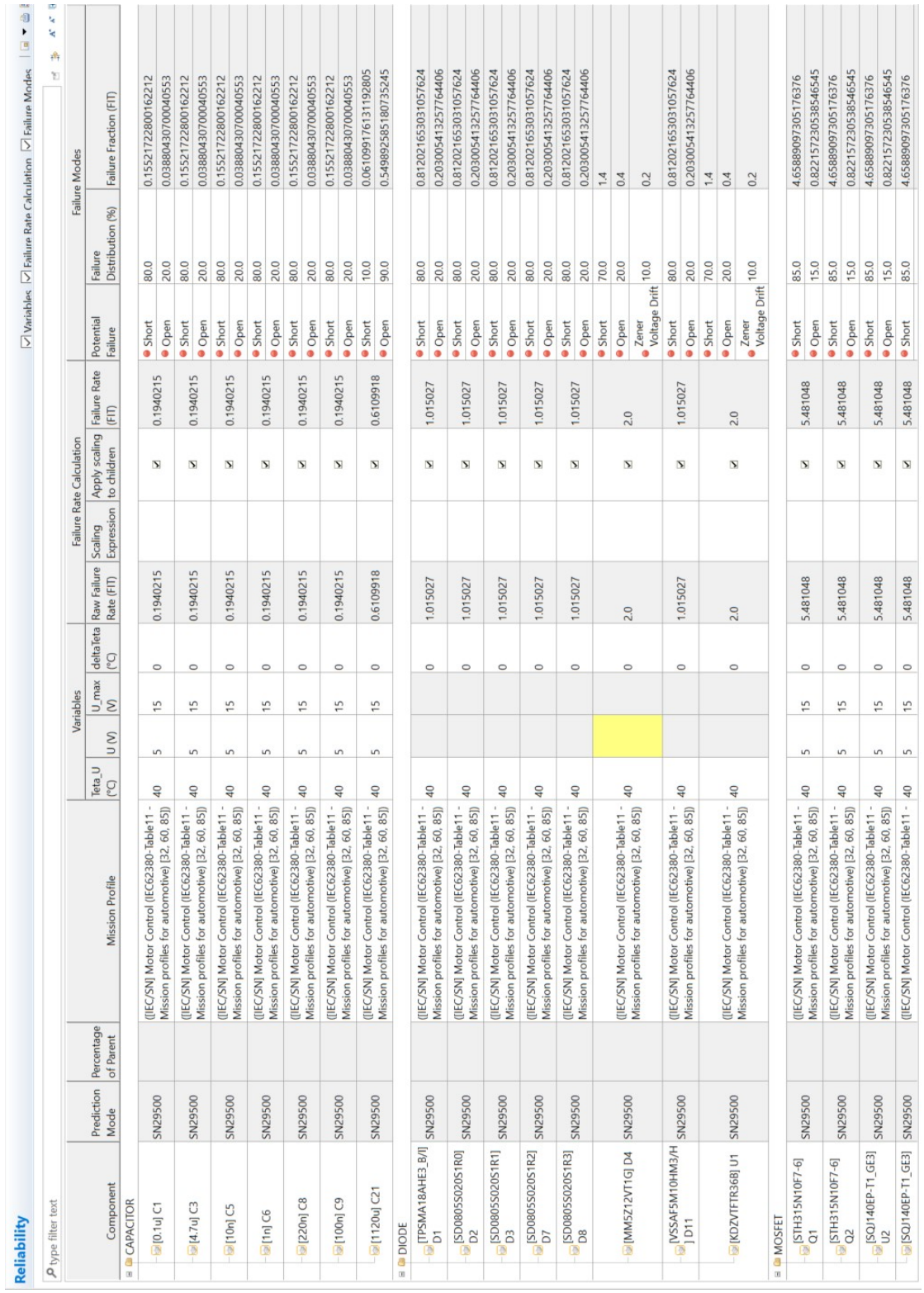


Figure 5.20: Hardware parts with their failure rates and failure modes

input is done by the STPM801. The STPM801 has inbuilt control and diagnostics unit that can also detect any failures that has occurred in the charge pump. At an event of any internal failure of the STPM801, a fault pin output, 'FLT', is set to

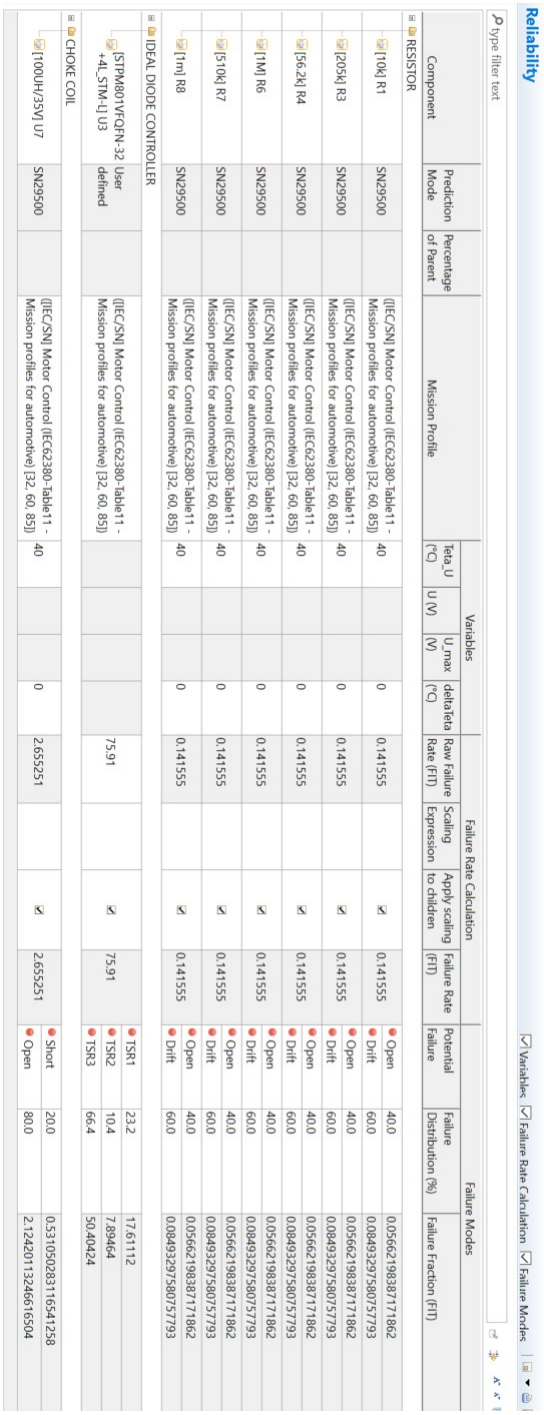


Figure 5.21: Hardware parts with their failure rates and failure modes (contd.)

low, which can be connected to an external microcontroller for handling the failure.

5.3.2 FMEDA

The FMEDA is done for the circuit in Figure 5.19 by analyzing the failure modes for different components which could potentially violate the top-level safety-goal. The safe-fault distribution for failure modes of different components is estimated by

analyzing the percentage of failures which could lead to not providing power to the control unit. In this section, only the FMEDA for the reverse-current-protection circuit block is discussed as the Pi-filter block and TVS blocks are the same for this design.

5.3.2.1 Reverse-current-protection blocks

The FMEDA for the reverse-current-protection circuits on both supplies is same since the type of components used in both the blocks are the same. The capacitors 'C3' and 'C4', ('C13' and 'C14' in right block) are connected to ground and to the input power supply 'VB' pin of the STPM801. The capacitors, when shorted, lead to a direct short between the 'VCC' and the 'GND'. This leads to a failure in powering on the STPM801 as intended.

Figures 5.22, 5.23 and 5.24 contain the information of the FMEDA for each component that contributes to the reverse-current-protection-left circuit block. The safe-fault distribution for the 'Short' in each capacitor is 50% because, only when a 'Short' failure occurs in 'C3' or 'C4', and in 'C13' or 'C14', at the same time will lead to violation of the safety-goal. As can be seen from the figures, the failure-mode distribution is 50% for the relevant failure modes of all components in the circuit blocks since they have to occur at the same time in both supply networks to violate the safety-goal. Given that the left and right circuit blocks complement each other, all failures in these blocks are considered to be part of multiple failures that violate safety-goal and not single-point failures.

FMEDA Worksheet

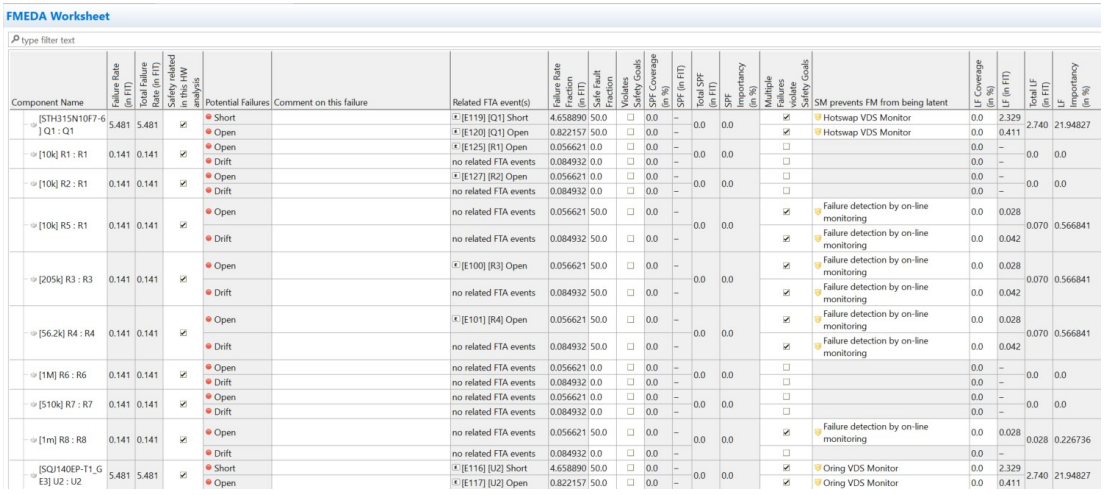
type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Comment on this failure	Related FTA event(s)	Failure Rate Fraction (in FIT)	Safe Fault Fraction	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Total SPF (in FIT)	SPF Importancy (in %)	Multiple failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
Reverse current protection Left																			
[0.1u] C4 : C1	0.194	0.194	☑	Short		no related FTA events	0.155217	50.0	☐	0.0	–	0.0	0.0	☑		0.0	–	0.077	0.62155
				Open		no related FTA events	0.038804	0.0	☐	0.0	–			☐		0.0	–		
[4.7u] C3 : C3	0.194	0.194	☑	Short		no related FTA events	0.155217	50.0	☐	0.0	–	0.0	0.0	☑		0.0	–	0.077	0.62155
				Open		no related FTA events	0.038804	0.0	☐	0.0	–			☐		0.0	–		
[10n] C5 : C5	0.194	0.194	☑	Short		[E126] [C5] Short	0.155217	50.0	☐	0.0	–	0.0	0.0	☑	Hotswap VDS Monitor	0.0	–	0.097	0.776938
				Open		no related FTA events	0.038804	50.0	☐	0.0	–			☑	Hotswap VDS Monitor	0.0	–		
[1n] C6 : C6	0.194	0.194	☑	Short		[E102] [C6] Short	0.155217	50.0	☐	0.0	–	0.0	0.0	☑	Failure detection by on-line monitoring	0.0	–	0.097	0.776938
				Open		[E103] [C6] Open	0.038804	50.0	☐	0.0	–			☑	Failure detection by on-line monitoring	0.0	–		
[1n] C7 : C6	0.194	0.194	☑	Short		no related FTA events	0.155217	50.0	☐	0.0	–	0.0	0.0	☑	Failure detection by on-line monitoring	0.0	–	0.097	0.776938
				Open		no related FTA events	0.038804	50.0	☐	0.0	–			☑	Failure detection by on-line monitoring	0.0	–		
[220n] C8 : C8	0.194	0.194	☑	Short		[E105] [C8] Short	0.155217	0.0	☐	0.0	–	0.0	0.0	☑	CP Voltage Monitor	0.0	0.1	0.194	1.553876
				Open		[E106] [C8] Open	0.038804	0.0	☐	0.0	–			☑	CP Voltage Monitor	0.0	–		
[100n] C9 : C9	0.194	0.194	☑	Short		[E108] [C9] Short	0.155217	50.0	☐	0.0	–	0.0	0.0	☑	CP Voltage Monitor	0.0	–	0.097	0.776938
				Open		[E109] [C9] Open	0.038804	50.0	☐	0.0	–			☑	CP Voltage Monitor	0.0	–		
[100n] C10 : C9	0.194	0.194	☑	Short		[E111] [C10] Short	0.155217	50.0	☐	0.0	–	0.0	0.0	☑	CP Voltage Monitor	0.0	–	0.097	0.776938
				Open		[E112] [C10] Open	0.038804	50.0	☐	0.0	–			☑	CP Voltage Monitor	0.0	–		
[SD0805S020S1R0] D2 : D2	1.015	1.015	☑	Short		no related FTA events	0.812021	0.0	☐	0.0	–	0.0	0.0	☐		0.0	–	0.101	0.812913
				Open		[E124] [D2] Open	0.203005	50.0	☐	0.0	–			☑	Hotswap VDS Monitor	0.0	0.1		
[SD0805S020S1R1] D3 : D3	1.015	1.015	☑	Short		no related FTA events	0.812021	0.0	☐	0.0	–	0.0	0.0	☐		0.0	–	0.101	0.812913
				Open		[E128] [D3] Open	0.203005	50.0	☐	0.0	–			☑	Oring VDS Monitor	0.0	0.1		
[MM5Z12VT1G] D4 : D4	2.0	2.0	☑	Short		[E98] [D4] Short	1.4	50.0	☐	0.0	–	0.0	0.0	☑		0.0	0.7	0.7	5.60615
				Open		no related FTA events	0.4	0.0	☐	0.0	–			☐		0.0	–		
				Zener Voltage Drift		no related FTA events	0.2	0.0	☐	0.0	–			☐		0.0	–		
[MM5Z12VT1G] D5 : D4	2.0	2.0	☑	Short		[E99] [D5] Short	1.4	50.0	☐	0.0	–	0.0	0.0	☑		0.0	0.7	0.7	5.60615
				Open		no related FTA events	0.4	0.0	☐	0.0	–			☐		0.0	–		
				Zener Voltage Drift		no related FTA events	0.2	0.0	☐	0.0	–			☐		0.0	–		

Figure 5.22: FMEDA for the right reverse current protection left block

As can be seen in Figure 5.22, a 'Short' failure and 'Open' failure in capacitor 'C5' ('C15' in right block) can lead to the hot-swap MOSFET, 'Q1' ('Q2' in right block) to be turned off, which can lead to supply failure at the output. Capacitors 'C6'

and 'C7' ('C16' and 'C17' in right block) fulfill the under-voltage and over-voltage monitoring functionality. Both failure modes, 'Open' and 'Short' will lead to failure detected in STPM801 which will result in the MOSFETs turning off. Capacitors 'C8', 'C9' and 'C10' ('C18', 'C19' and 'C20' in right block) are capacitors used for the charge-pump of the STPM801. Both failure modes of these capacitors will lead to malfunction of the charge-pump, due to which the charge-pump voltage monitor will detect a failure and switch off the MOSFETs 'Q1' and 'U2' ('Q2' and 'U5' in right block). 'D2' ('D7' in right block) Schottky diode is used for the hot-swap application. A 'Short' failure is not considered as a safety critical fault as it will not lead to the violation of the safety goal. However, an 'Open' will result in a disconnection to the 'C5' ('C15' in right block) capacitor, which leads to a failure in the hot-swap application and consequently violates the safety-goal. 'D3' ('D8' in right block) diode is used for the reverse-current functionality. It is assumed that an 'Open' in this diode results in a fault detected by STPM801, as the STPM801 datasheet gives an indication that this diode is necessary but does not delve into the consequences of its failure. 'D4' and 'D5', ('D9' and 'D10' in right block) cause an issue only in cases of a 'Short' and it would result in a shorting of the 'HGATE', 'SOURCE' and 'DGATE' pins of STPM801.



FMEDA Worksheet

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Comment on this failure	Related FTA event(s)	Failure Rate Fraction (in FIT)	Safe Fault Fraction	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Total SPF (in FIT)	SPF Importancy (in %)	Multiple Failures Violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
[STH315N10F7-6] Q1 : Q1	5.481	5.481	☑	Short		[E119] [Q1] Short	4.658890	50.0	☐	0.0	–	0.0	0.0	☑	Hotswap VDS Monitor	0.0	2.329	2.740	21.94827
				Open		[E120] [Q1] Open	0.822157	50.0	☐	0.0	–			☑	Hotswap VDS Monitor	0.0	0.411		
[10k] R1 : R1	0.141	0.141	☑	Open		[E125] [R1] Open	0.056621	0.0	☐	0.0	–	0.0	0.0	☐		0.0	–	0.0	0.0
				Drift		no related FTA events	0.084932	0.0	☐	0.0	–			☐		0.0	–		
[10k] R2 : R1	0.141	0.141	☑	Open		[E127] [R2] Open	0.056621	0.0	☐	0.0	–	0.0	0.0	☐		0.0	–	0.0	0.0
				Drift		no related FTA events	0.084932	0.0	☐	0.0	–			☐		0.0	–		
[10k] R5 : R1	0.141	0.141	☑	Open		no related FTA events	0.056621	50.0	☐	0.0	–	0.0	0.0	☑	Failure detection by on-line monitoring	0.0	0.028	0.070	0.566841
				Drift		no related FTA events	0.084932	50.0	☐	0.0	–			☑	Failure detection by on-line monitoring	0.0	0.042		
[205k] R3 : R3	0.141	0.141	☑	Open		[E100] [R3] Open	0.056621	50.0	☐	0.0	–	0.0	0.0	☑	Failure detection by on-line monitoring	0.0	0.028	0.070	0.566841
				Drift		no related FTA events	0.084932	50.0	☐	0.0	–			☑	Failure detection by on-line monitoring	0.0	0.042		
[56.2k] R4 : R4	0.141	0.141	☑	Open		[E101] [R4] Open	0.056621	50.0	☐	0.0	–	0.0	0.0	☑	Failure detection by on-line monitoring	0.0	0.028	0.070	0.566841
				Drift		no related FTA events	0.084932	50.0	☐	0.0	–			☑	Failure detection by on-line monitoring	0.0	0.042		
[1M] R6 : R6	0.141	0.141	☑	Open		no related FTA events	0.056621	0.0	☐	0.0	–	0.0	0.0	☐		0.0	–	0.0	0.0
				Drift		no related FTA events	0.084932	0.0	☐	0.0	–			☐		0.0	–		
[510k] R7 : R7	0.141	0.141	☑	Open		no related FTA events	0.056621	0.0	☐	0.0	–	0.0	0.0	☐		0.0	–	0.0	0.0
				Drift		no related FTA events	0.084932	0.0	☐	0.0	–			☐		0.0	–		
[1m] R8 : R8	0.141	0.141	☑	Open		no related FTA events	0.056621	50.0	☐	0.0	–	0.0	0.0	☑	Failure detection by on-line monitoring	0.0	0.028	0.028	0.226736
				Drift		no related FTA events	0.084932	0.0	☐	0.0	–			☐		0.0	–		
[SQJ140EP-T1_GE3] U2 : U2	5.481	5.481	☑	Short		[E116] [U2] Short	4.658890	50.0	☐	0.0	–	0.0	0.0	☑	Oring VDS Monitor	0.0	2.329	2.740	21.94827
				Open		[E117] [U2] Open	0.822157	50.0	☐	0.0	–			☑	Oring VDS Monitor	0.0	0.411		

Figure 5.23: FMEDA for the right reverse current protection left block (contd.)

Figure 5.23 shows the failure modes of the hot-swap MOSFET 'Q1' ('Q2' in right block), all resistors in the circuit, 'R1' to 'R8' ('R9' to 'R16' in right block), and the OR-ing MOSFET 'U2' ('U5' in right block). For 'Q1' MOSFET, both failure modes, 'Short' and 'Open' can prove to be critical. A 'Short' failure can be critical during initial wake up of the system and during hot swapping. in this case, a high inrush current cannot be prevented from damaging the circuit. An 'Open' failure will not activate the circuit and that results in low output voltage. The resistors 'R1' and 'R2' ('R9' and 'R10' in right block) are not considered to be violating the safety-goal, as a path always exists through the 'D2' and 'D3' diodes ('D7' and 'D8' in right block).

'R3', 'R4' and 'R5' ('R11', 'R12' and 'R13' in right block) resistors are used for the over-voltage and under-voltage detection. The STPM801 can detect a false

positive fault if these resistors 'Open' or have a high 'Drift' in its resistance value. A fault in the shunt resistor, 'R8' ('R16' in right block) could lead to faulty current measurement at the output that could cause the STPM801 to interpret a failure and turn off the MOSFETs.

For 'U2' MOSFET, both failure modes, 'Short' and 'Open' can prove to be critical. A 'Short' failure can be critical in cases when left power-supply is lower than the right. In this case, the power-supply would be considered from right block and the left STPM801 turns off or opens the 'U2' MOSFET. But if the MOSFET does not open due to a 'Short', then the reverse-current passes through to from right to left power-supply, which could potentially damage the system. An 'Open' failure will be an issue when the left supply is the primary supply. In this case, the MOSFET is expected to be turned on, but an 'Open' failure will lead to low voltage at the output.

FMEDA Worksheet

type filter text

Component Name	Failure Rate (in FIT)	Total Failure Rate (in FIT)	Safety related in this HW analysis	Potential Failures	Comment on this failure	Related FTA event(s)	Failure Rate Fraction (in FIT)	Safe Fault Fraction	Violates Safety Goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)	Total LF (in FIT)	LF Importancy (in %)
[STPM801VFQFN-32+4L_STM-L] U3 : U3	75.91	75.91	☑	TSR1	The SPF, LFM and PMHF values provided by supplier cannot be directly imported they do not provide the total safety related FIT of the component. However, this can be determined based on the relationship between the metrics. The FIT of 17.61 was derived by calculating the safety related failure using the SPFM, LFM and PMHF equations and substituting the values provided by supplier.	[E30] [U3] Violation of TSR1	17.61112	50.0	☐	99.0	–	☑	Voltage Monitor - POR Clock Monitor CP Voltage Monitor Oring VDS Monitor CRC on Safety Relevant OTP data runtime Chopper Monitor / Analog BIST Redundancy among CRC gen and CRC check circuits Clock Monitor Self Test	99.0	0.088	0.323	2.592528
				TSR2	The SPF, LFM and PMHF values provided by supplier cannot be directly imported they do not provide the total safety related FIT of the component. However, this can be determined based on the relationship between the metrics. The FIT of 7.89 was derived by calculating the safety related failure using the SPFM, LFM and PMHF equations and substituting the values provided by supplier.	[E31] [U3] Violation of TSR 2	7.89464	50.0	☐	99.84	–	☑	Voltage Monitor - POR Clock Monitor CP Voltage Monitor Hotswap VDS Monitor Chopper Monitor / Analog BIST Clock Monitor Self Test	99.84	0.006		
				TSR3	The SPF, LFM and PMHF values provided by supplier cannot be directly imported they do not provide the total safety related FIT of the component. However, this can be determined based on the relationship between the metrics. The FIT of 50.40 was derived by calculating the safety related failure using the SPFM, LFM and PMHF equations and substituting the values provided by supplier.	[E32] [U3] Violation of TSR 3	50.40424	50.0	☐	99.09	–	☑	Voltage Monitor - POR Clock Monitor Oring VDS Monitor CRC on Safety Relevant OTP data runtime Chopper Monitor / Analog BIST Redundancy among CRC gen and CRC check circuits Clock Monitor Self Test	99.09	0.229		

Figure 5.24: FMEDA for the right reverse current protection left block (contd.)

Figure 5.24 shows the failure modes of the STPM801 itself. Since the controller has been developed as per ISO26262, STM Electronics have provided three TSRs that they have been implemented along with the failure metrics for each TSR. These failure metrics have been determined by by ST Microelectronics through an extensive failure analysis and implementation of internal safety mechanisms. The SPFM, LFM and PMHF have not been directly used, as the Medini Analyze tool requires the safety related failures along with their SPF and latent fault (LF) coverage. The SPF coverage and LF coverage give an indication to the percentage of safety-related faults that have been covered by the safety mechanisms implemented within the controller. As two STPM801 is used in this use case, the SPF of the STPM801 now becomes LF at a system level. Therefore, in the figure, the STPM801 failure modes are also chosen as multiple failures that violate safety goals.

5.3.3 Quantified fault tree analysis

The top-level event failure is same for both the designs. The FTA for the ISO 26262 compliant design differs only in the reverse-current-protection left and right circuit blocks. The truth table in Figure 5.12 is applicable for this design as well. Since the STPM801 provides a number of features that are used in the design, the FTA is more extensive than in the design using LM74700. As shown in Figure 5.25, the number of components involved are more and there are sub-trees for hot-swap failure and Ideal-diode failure which can be seen in Figure 5.26 and Figure 5.27 respectively.

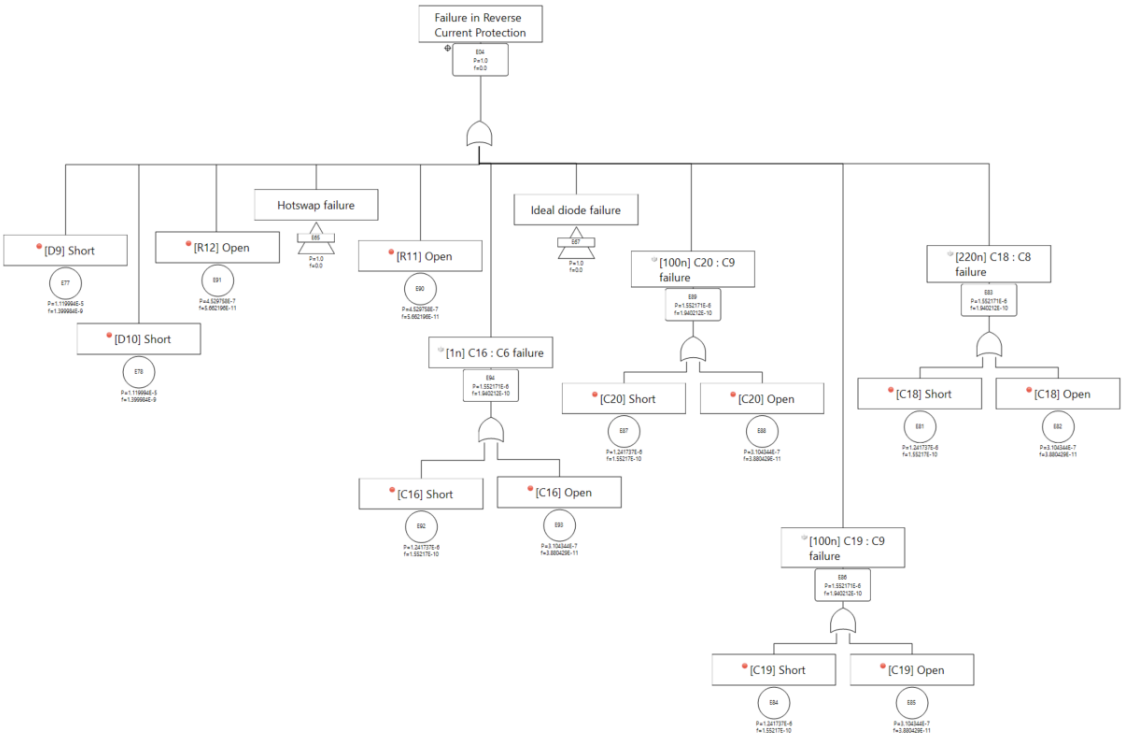


Figure 5.25: FTA of Reverse Current Protection Right Circuit Block

The method of performing the FTA is similar as in the previous design. The failure modes of components from the FMEDA are used to form the root of the tree. By analysing the circuit, the failure modes are traced to the top level event through 'OR' and 'AND' combinations. In Figure 5.26 and Figure 5.27, the FTA is designed based on the components involved in fulfilling the hot-swap and OR-ing functionality. As many safety mechanisms are in place for the STPM801, only a double failure (failure of the safety mechanism and the components involved) would lead to failure of the Hot-swap and OR-ing failure events.

The FTA for the reverse-current-protection-left block is similar to the reverse-current-protection-right block. Figure 5.28, Figure 5.29 and Figure 5.30 show the FTAs derived for the reverse-current-protection-left block.

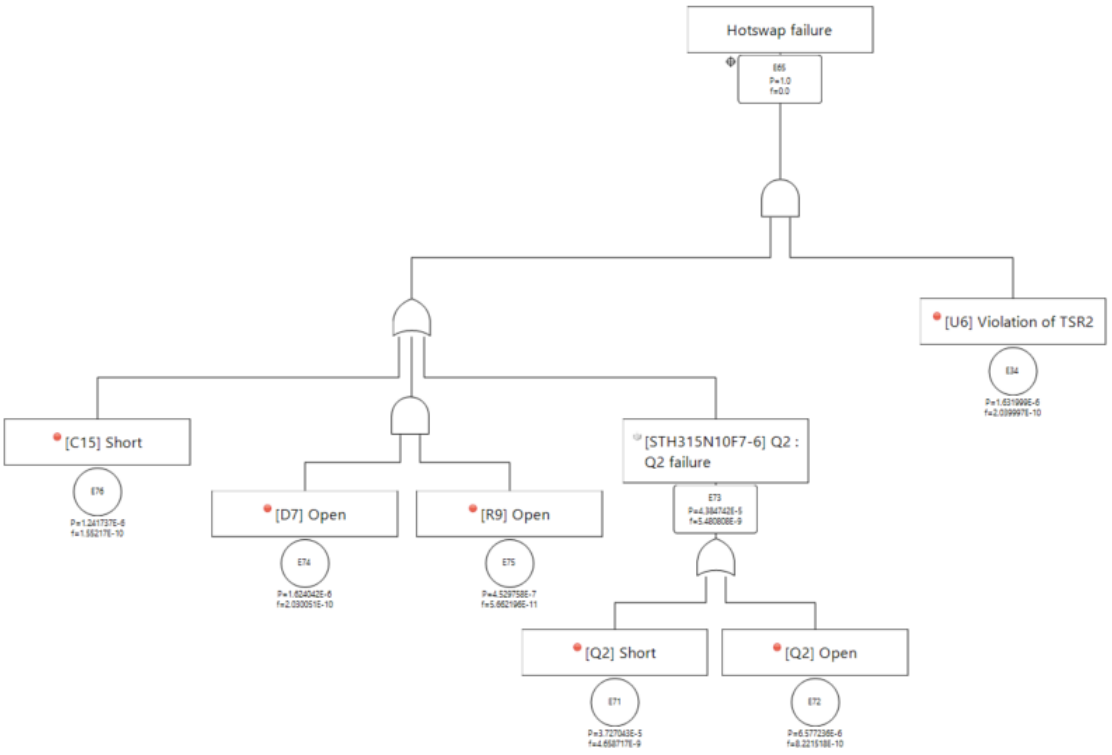


Figure 5.26: FTA of hot-swap failure Right

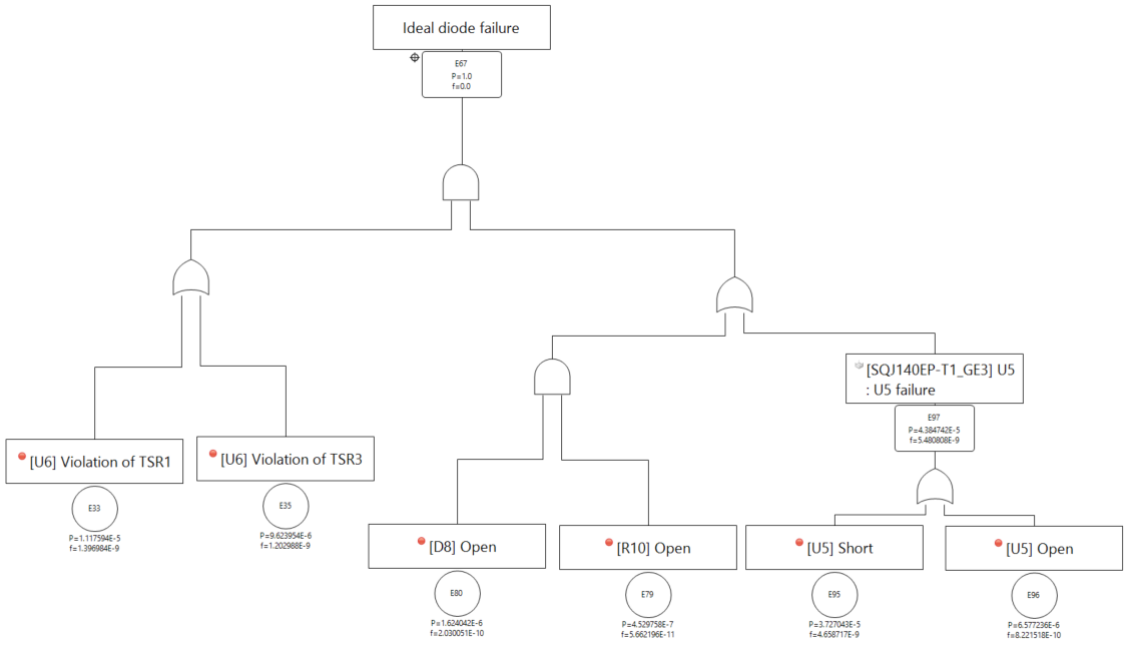


Figure 5.27: FTA of Ideal diode failure Right

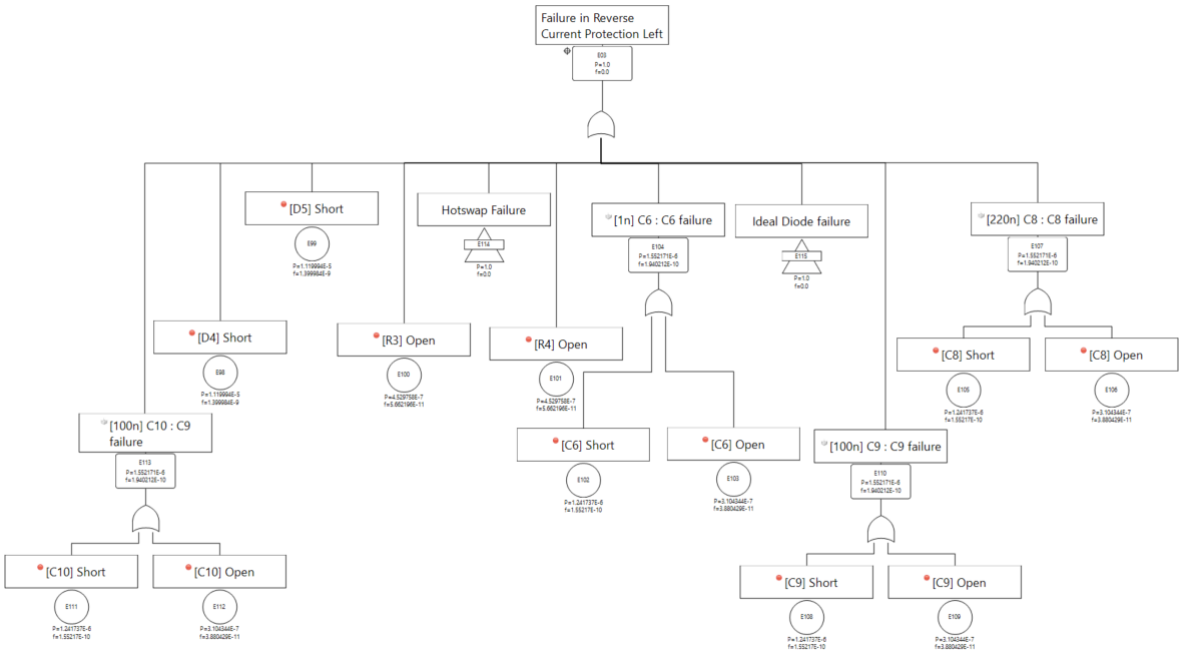


Figure 5.28: FTA of Reverse Current Protection Left Circuit Block

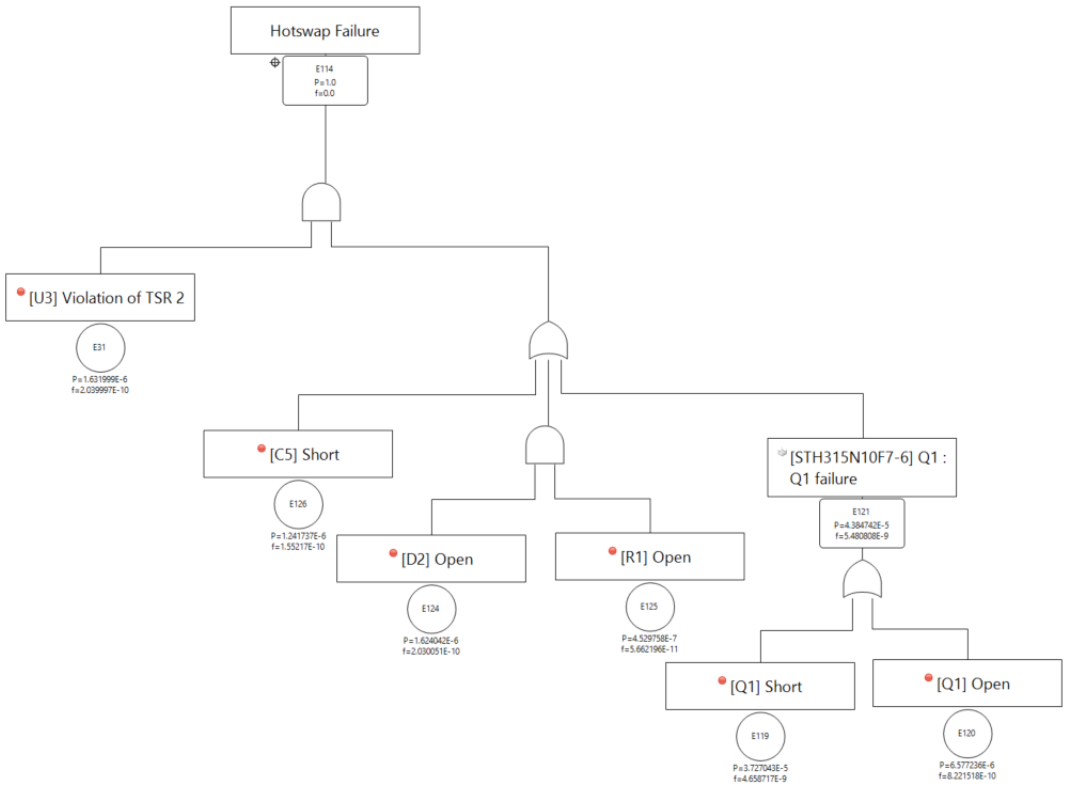


Figure 5.29: FTA of hot-swap Failure Left

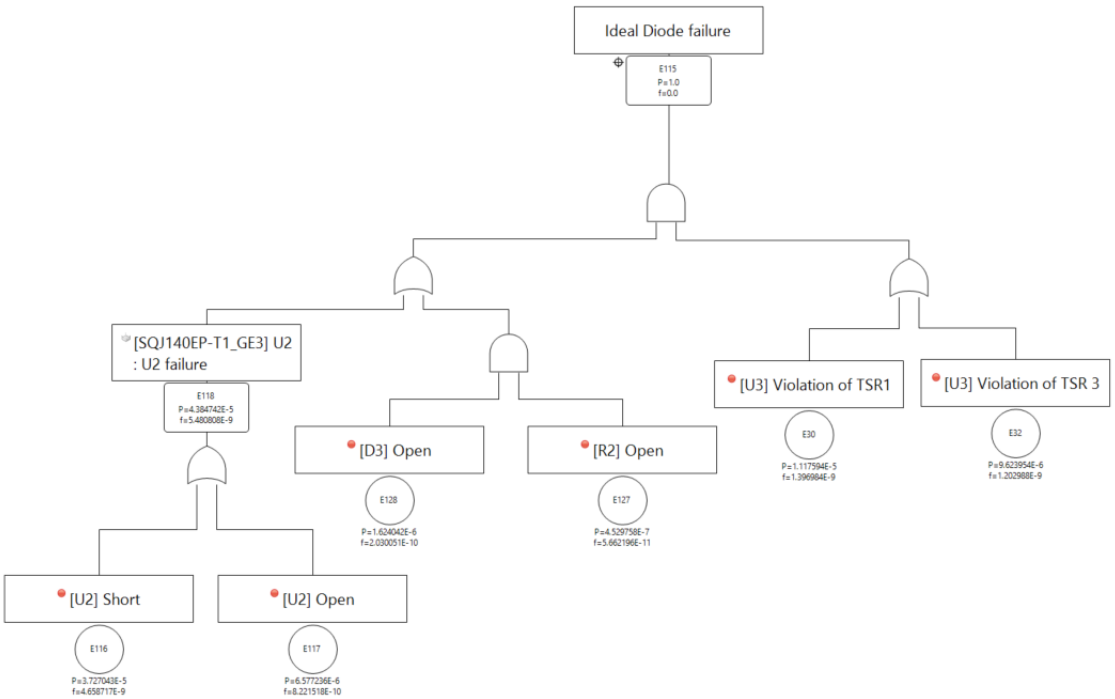


Figure 5.30: FTA of Ideal Diode failure Left

6

Results

This section shows the results obtained after performing the functional-safety analysis for the designs using the ISO 26262 non-compliant device and the ISO 26262 compliant device. A comparison between the hardware metrics for the circuit using ISO26262 compliant device and the circuit using ISO26262 non-compliant device is discussed.

6.1 Failure analysis results for circuit with ISO 26262 non-compliant component

Diagnostic Coverage Worksheet for DC_NonISO26262

ID	Safety Goal	ASIL	SPF Metric Target Value	99.0%
G001	SG001	D	LF Metric Target Value	90.0%

Total		Single-Point		Latent	
Failure Rate (in FIT)	66.3889E0	Total Failure Rate (in FIT)	2.32721E0	Total Failure Rate (in FIT)	25.3079E0
Safety Related (in FIT)	66.3889E0				
Not Safety Related (in FIT)	0.0E0	Fault Metric	96.49%	Fault Metric	60.49%

Figure 6.1: FMEDA results overview for circuit using ISO 26262 non-compliant component.

Figure 6.1 shows the SPF (Single-Point Failure) and the LFM (Latent-Fault Metric) of the circuit designed (Shown in Figure 5.19) with non-compliant component. The total SPF and LF obtained are 2.327 FIT and 25.308 FIT (Failure In-Time)

respectively. This corresponds to an SPFM (Single-Point-Fault Metric) of 96.49% and an LFM of 60.49%. The results indicate that the ASIL D target metrics are not met with the current design. Based on these results, it is clear that the usage of non-compliant component without any safety mechanisms can lead to a less reliable design in safety-critical applications. This analysis is necessary to understand the extent of external safety mechanisms needed to be implemented in order to compensate for the unreliability of a component.

Part No.	VSSAF5M10HM3/H	Component Name	D5									Failure Rate (in FIT)	Total Failure Rate (in FIT)
Safety related in this HW analysis	all SGs	Container Path	*Pi Filter*									1.01503E0	1.01503E0
Potential Failure Modes	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Evaluation Group	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of safety goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)
Open	20	0.203	all SGs	0.0%	203.005E-3	x		0.0%	203.005E-3	-		0.0%	
Short	80	0.812	all SGs	0.0%	812.022E-3	-		0.0%		-		0.0%	

Part No.	100UH/35V	Component Name	U10									Failure Rate (in FIT)	Total Failure Rate (in FIT)
Safety related in this HW analysis	all SGs	Container Path	*Pi Filter*									2.65525E0	2.65525E0
Potential Failure Modes	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Evaluation Group	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of safety goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)
Open	80	2.124	all SGs	0.0%	2.1242E0	x		0.0%	2.1242E0	-		0.0%	
Short	20	0.531	all SGs	0.0%	531.05E-3	-		0.0%		-		0.0%	

Figure 6.2: Main contributors to SPFM.

The reason for SPFM being lower than the target value is due to the VSSAF5M10-HM3/H Schotkky diode (D5) and the choke coil 100 µH/35 V (U10) in Pi-filter block. From Figure 6.2, it can be seen that total SPF is due to 'Open' failure mode of both D5 and U10. These two components do not have a redundancy or any other mechanism that can mitigate the effects of the SPF. A possible solution to improve the SPFM is by having two choke coils in parallel and having two Schottky diodes in parallel. By doing this, the single-point failures would be converted to multiple-point failures which would in turn increase the SPFM value, but would result in reduction in LFM value.

Figure 6.3 and Figure 6.4 shows the failure-rate contribution of LM74700 in reverse-current-protection left and right circuit block, respectively. The total FIT contribution by each LM74700 is 10 FIT. From Figure 6.1, it can be seen that the total LFM in FIT is 25.307, and the combined FIT contribution from both LM74700 accounts to 20 FIT, which is responsible for approximately 80% of the total latent failures in the circuit. Since an in-depth analysis of the systematic failures and their effects has not been done by the supplier, no safety mechanisms are in place addressing the

Part No.	LM74700QDDFRQ1	Component Name	U3	Failure Rate (in FIT)	Total Failure Rate (in FIT)
Safety related in this HW analysis	all SGs	Container Path	*Reverse current protection Left*	20E0	20E0

Potential Failure Modes	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Evaluation Group	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of safety goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)
GATE output not in specification – voltage or timing	40	8	all SGs	50.0 %	4.0E0	-		0.0%		x		0.0%	4.0E0
GATE output stuck Low or HIZ	50	10	all SGs	50.0 %	5.0E0	-		0.0%		x		0.0%	5.0E0
GATE output stuck on Hi	5	1	all SGs	50.0 %	500E-3	-		0.0%		x		0.0%	500E-3
Short circuit any two pins	5	1	all SGs	50.0 %	500E-3	-		0.0%		x		0.0%	500E-3

Figure 6.3: FMEDA results for the circuit using LM74700 in left

Part No.	LM74700QDDFRQ1	Component Name	U4	Failure Rate (in FIT)	Total Failure Rate (in FIT)
Safety related in this HW analysis	all SGs	Container Path	*Reverse current protection Right*	20E0	20E0

Potential Failure Modes	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Evaluation Group	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of safety goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)
GATE output not in specification – voltage or timing	40	8	all SGs	50.0 %	4.0E0	-		0.0%		x		0.0%	4.0E0
GATE output stuck Low or HIZ	50	10	all SGs	50.0 %	5.0E0	-		0.0%		x		0.0%	5.0E0
GATE output stuck on Hi	5	1	all SGs	50.0 %	500E-3	-		0.0%		x		0.0%	500E-3
Short circuit any two pins	5	1	all SGs	50.0 %	500E-3	-		0.0%		x		0.0%	500E-3

Figure 6.4: FMEDA results for the circuit using LM74700 in right

failures within the component. The latent failures are high in the current system due to the lack of monitoring, diagnostic and safety mechanisms, which could mitigate the effects of these failures. To satisfy ASIL D requirements, the failures in the LM74700 need to be addressed through external monitoring and safety mechanisms that ensure a safe reaction in case of a failure.

The result obtained for PMHF from Medini Analyze tool can be seen in Figure 6.5. The FTA evaluated by the tool is not performed specifically to calculate the PMHF. The evaluation also provides other information that is useful while performing risk analysis. As shown in the figure, the parameters evaluated by the tool are unavailability, unreliability, probability of Failure-in-Demand (PFD), conditional failure intensity (CFI) average, and PMHF. However, out of these parameters, only PMHF is of interest for this thesis project. The PMHF obtained is 2.33 FIT which is well within the ASIL D target PMHF value. The consolidated safety-goal analysis for the circuit with the non-compliant component is shown in Figure 6.6.

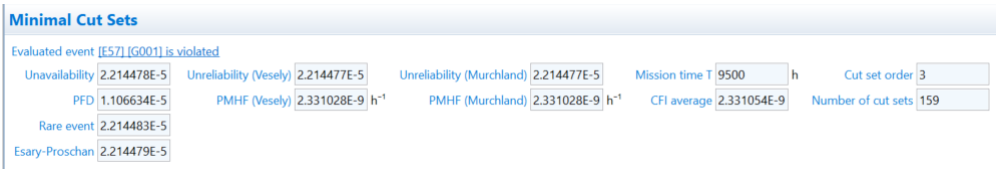


Figure 6.5: FTA results for the circuit using ISO 26262 non-compliant component (LM74700)

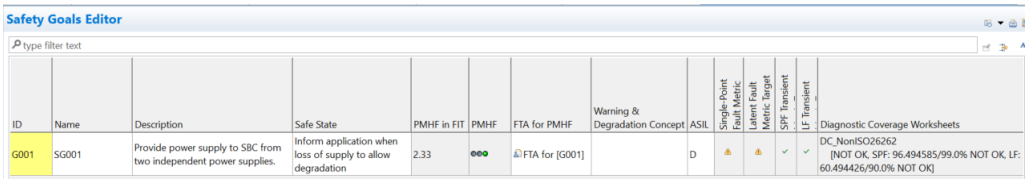


Figure 6.6: Safety goal analysis for the circuit using ISO 26262 non-compliant component (LM74700)

6.2 Failure analysis results for circuit with ISO 26262 compliant component

The overall result of the FMEDA analysis performed on the circuit (See Figure 5.19) with the ISO 26262 compliant component is shown in Figure 6.7.

Diagnostic Coverage Worksheet for DC_ISO26262

ID	Safety Goal	ASIL	SPF Metric Target Value	99.0%
G001	SG001	D	LF Metric Target Value	90.0%

Total		Single-Point		Latent	
Failure Rate (in FIT)	204.87E0	Total Failure Rate (in FIT)	2.32721E0	Total Failure Rate (in FIT)	12.4863E0
Safety Related (in FIT)	204.87E0				
Not Safety Related (in FIT)	0.0E0	Fault Metric	98.86%	Fault Metric	93.84%

Figure 6.7: FMEDA analysis for the circuit with the compliant component

The SPFM and LFM for this design is found to be 98.86% and 93.84%, respectively. The SPFM does not satisfy the requirement for ASIL D although the LFM satisfies ASIL D target metrics. The reason for the 98.86% SPFM is due to the Schottky diode VSSAF5M10HM3/H (1.015 FIT) and the choke coil 100 µH/35 V (2.655 FIT).

The SPFM can be improved the same way as suggested for the previous design for the Pi-filter, as this block is the same for both designs.

The FMEDA analysis for the STPM801 gives a consolidated report of the safety mechanisms and the latent failure for each failure mode as shown in Figure 6.8 and Figure 6.9. The failures are latent faults with the safety mechanisms covering 99%, 99.84% and 99.09% for 'TSR1', 'TSR2' and 'TSR3' failures respectively. It can be observed that a single STPM801 unit contributes to a 0.323 FIT out of the total 12.426 FIT latent faults as shown in Figure 6.7. From this it can be inferred that, the compliant component with all the internal safety mechanisms implemented, is able to sufficiently mitigate the effects of the potential latent faults that can occur in this design.

Part No.	STPM801VFQFN-32+4L_STM-L	Component Name	U3	Failure Rate (in FIT)	Total Failure Rate (in FIT)
Safety related in this HW analysis	all SGs	Container Path	*Reverse current protection Left*	75.91E0	75.91E0

Potential Failure Modes	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Evaluation Group	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of safety goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)
TSR1	23.2	17.611	all SGs	50.0 %	8.8055 6E0	-	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Oring VDS Monitor	99.0 %		x	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Oring VDS Monitor, CRC on Safety Relevant OTP data runtime, Chopper Monitor / Analog BIST, Redundancy among CRC gen and CRC check circuits, Clock Monitor Self Test	99.0 %	88.055 6E-3
TSR2	10.4	7.895	all SGs	50.0 %	3.9473 2E0	-	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Hotswap VDS Monitor	99.84 %		x	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Hotswap VDS Monitor, Chopper Monitor / Analog BIST, Clock Monitor Self Test	99.84 %	6.3157 1E-3
TSR3	66.4	50.404	all SGs	50.0 %	25.202 1E0	-	Voltage Monitor - POR, Clock Monitor, Oring VDS Monitor	99.09 %		x	Voltage Monitor - POR, Clock Monitor, Oring VDS Monitor, CRC on Safety Relevant OTP data runtime, Chopper Monitor / Analog BIST, Redundancy among CRC gen and CRC check circuits, Clock Monitor Self Test	99.09 %	229.33 9E-3

Figure 6.8: FMEDA report for STPM801 used in reverse current protection left

The quantitative FTA is evaluated based on the FTA design in Section 5.3.3. The result of the evaluation of the FTA is shown in Figure 6.10. The PMHF obtained is 2.327 FIT for the design. This value is less than 10 FIT which is the recommendation for an ASIL D design.

Part No.	STPM801VFQFN-32+4L_STM-L	Component Name	U6	Failure Rate (in FIT)	Total Failure Rate (in FIT)
Safety related in this HW analysis	all SGs	Container Path	*Reverse current protection Right*	75.91E0	75.91E0

Potential Failure Modes	Failure Rate Distribution (in %)	Failure Rate Fraction (in FIT)	Evaluation Group	Safe Fault Fraction (in %)	Remaining Safety Related Failure Rate (in FIT)	Violates Safety Goals	SM prevents FM from violation of safety goals	SPF Coverage (in %)	SPF (in FIT)	Multiple Failures violate Safety Goals	SM prevents FM from being latent	LF Coverage (in %)	LF (in FIT)
TSR1	23.2	17.611	all SGs	50.0 %	8.80556E0	-	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Oring VDS Monitor	99.0 %		x	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Oring VDS Monitor, CRC on Safety Relevant OTP data runtime, Chopper Monitor / Analog BIST, Redundancy among CRC gen and CRC check circuits, Clock Monitor Self Test	99.0 %	88.056E-3
TSR2	10.4	7.895	all SGs	50.0 %	3.94732E0	-	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Hotswap VDS Monitor	99.84 %		x	Voltage Monitor - POR, Clock Monitor, CP Voltage Monitor, Hotswap VDS Monitor, Chopper Monitor / Analog BIST, Clock Monitor Self Test	99.84 %	6.3157E-3
TSR3	66.4	50.404	all SGs	50.0 %	25.2021E0	-	Voltage Monitor - POR, Clock Monitor, Oring VDS Monitor	99.09 %		x	Voltage Monitor - POR, Clock Monitor, CRC on Safety Relevant OTP data runtime, Chopper Monitor / Analog BIST, Redundancy among CRC gen and CRC check circuits, Clock Monitor Self Test, Oring VDS Monitor	99.09 %	229.339E-3

Figure 6.9: FMEDA report for STPM801 used in reverse current protection right

The consolidated result of the safety-goal using quantitative failure analysis is shown in Figure 6.11.

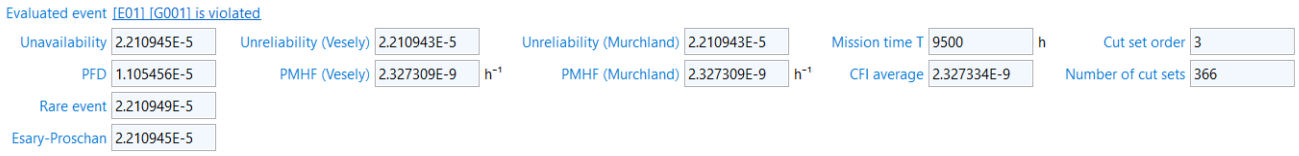


Figure 6.10: Quantitative FTA evaluation of the design with STPM801

ID	Name	Description	Safe State	ASIL	Single-Point Fault Metric Target Achieved	Latent Fault Metric Target Achieved	SPF Transient Metric Target Achieved	LF Transient Metric Target Achieved	Diagnostic Coverage Worksheets	PMHF in FIT	PMHF	FTA for PMHF
G001	SG001	Provide power supply to SBC from two independent power supplies.	Inform application when loss of supply to allow degradation	D	⚠	✓	✓	✓	DC_ISO26262 [NOT OK, SPF: 98.864056/99.0% NOT OK, LF: 93.835234/90.0% OK]	2.33	●●●	FTA for [G001]

Figure 6.11: Safety goal analysis for the circuit using ISO 26262 compliant component.

6.3 Discussion

Based on the results obtained for non-compliant component, LM74700, it is observed that the component is responsible for 80% of the latent faults that could occur in the design. Furthermore, the results indicate that without analysing the failure probability of the components being used, the system being designed can have unknown failures that would remain unaddressed. In safety-critical applications, the margin for error should be very low, therefore, it is essential to know the reliability of components.

When comparing the obtained safety metrics for the design using compliant component and design using non-compliant component, it is noted that both designs have the same cause of single-point failures. However, the SPFM for design using STPM801 is higher (98.6%) than that of design using LM74700 (96.43%). This is mainly due to the difference in the total number of safety-related failures in both designs. As the design using STPM801 consists of more components, the total number of safety-related failures is higher (204.87 FIT) than the design using LM74700 (66.39 FIT), which has fewer components. From this result, it can be inferred that while the usage of the components in question are done with redundancy, they impact the SPFM indirectly due to their contribution to the total safety-related failures.

The results obtained for the LFM in both the designs show a striking difference of about 33% with the LFM for the design with LM74700 being 60.49% while the LFM for the design with STPM801 being 93.84%. This is due to the fact that most of the latent failures are mitigated by the implementation of safety mechanisms within the STPM801 component while there are no safety mechanisms to protect the design with LM74700 from latent faults.

The results for the design with the non-compliant component raises a pertinent question: Why use non-compliant components if the results indicate higher probabilities of failures?

1. Firstly, when using compliant components the total number of safety related

failures may increase due to the number of components involved in implementing the safety mechanisms. While these safety mechanisms are in place to mitigate the effect of the failures, it has to be noted that using more components introduce more possibilities of failures in the system. Using a non-compliant component can be beneficial in these cases, if the failure detection and safety mechanism implementations are implemented externally with high ASIL integrity microcontrollers. In these cases, the less complexity of non-compliant components along with the external safety mechanisms may result in a lower total safety related failures and also achieve the target metrics.

2. Secondly, to achieve ISO 26262 compliance, the standard requires you to cover for all SPFs and LFs within the component, which results in various internal safety mechanisms implemented by supplier based on assumed use-cases and assumed safety-requirements. While the components fulfill the main goal of OEM, some of these assumed use-cases and requirements may not necessarily align completely with OEM's design. For example, STPM801 provides hot-swap feature for ensuring high inrush currents do not damage the system. This issue could be dealt differently by OEM on a higher level outside of the functional safety circuit explored in this thesis project.
3. Finally, due to these internal safety features and mechanisms implemented by suppliers, the OEMs are restricted in implementing a more design specific solution for their use case. In such situations, non-compliant components, along with the relevant documentation providing justification for its use in safety applications may prove to be a more flexible option.

7

Conclusion

One of the aims of this thesis project was to assess the impact of component reliability while designing a safety-critical electronic system. Based on an initial literature survey, it was found that there is a lack of research papers addressing the reliability of components being used while designing safe system. To explore this, a safety scenario was put forth by Volvo Cars that focused on addressing a reverse current between two power supplies in a power-distribution solution. To understand the effects of component reliability in this scenario, a design with ISO 26262 non-compliant ideal-diode controller, LM74700, and a design with ISO 26262 compliant ideal-diode controller, STPM801, are considered. A comprehensive failure analysis was performed to evaluate the random hardware failure metrics on both these designs. The failure analysis involved performing an FMEDA (Failure Mode Effect and Diagnostic Analysis) and FTA (Fault-Tree Analysis) on the hardware designs to calculate the safety hardware metrics defined in ISO 26262, namely the SPFM (Single Point Failure Metric), LFM (Latent Fault Metric) and PMHF (Probabilistic Metric for random Hardware Faiure), which indicate the probability of components to fail and their effects on the whole system.

The overall result indicated that the non-compliant component, without safety mechanisms in place, is indeed less reliable compared to the compliant component. The obtained results indicated that, the design using LM74700 had a slightly lower SPFM as compared to the design with STPM801, while there was a significantly large difference in LFM between the designs. This is mainly attributed to redundancy in using the components addressing the reverse-current protection. As only a failure in both components occurring at the same time will result in violating the safety goal, the effects of the ideal-diode controller directly impacted the LFM and indirectly impacted the SPFM. The LFM for design using LM74700 was significantly lower as it did not contain any safety mechanisms to cover for the latent faults in the design. In contrast, the LFM for the design with STPM801 met the necessary targets as most of the latent faults were covered by the internal safety mechanisms.

The rationale behind using non-compliant components, even when results suggest a higher likelihood of failures, is worth considering. The decision to opt for such components in safety applications, is based on the specific use case of each component within the safety system. This choice considers several key factors. Firstly, compliant components can introduce complexity due to the multiple internal safety mechanisms, which, may increase the number of safety-related failures. Non-compliant components, when paired with external monitoring systems for failure detection and

safety mechanisms, can simplify the system and lead to fewer safety-related failures, and also align with target metrics set for that system. Secondly, ISO 26262 compliance by suppliers mandates internal safety mechanisms in components, often based on assumed use cases and requirements that may not perfectly match with OEM's specific design needs. Lastly, the internal safety features implemented by suppliers can constrain OEMs in tailoring solutions for their unique use cases. In such scenarios, non-compliant components, substantiated by suitable documentation justifying their safety use, offer a more adaptable alternative. Ultimately, the choice hinges on the intricacies of the safety application and the need for flexibility within the design process.

Although this thesis project encompassed an examination of a non-compliant component lacking internal safety mechanisms and a compliant component equipped with built-in safety mechanisms, within the context of a particular power distribution scenario, the findings and conclusions drawn from this study can still hold relevance and applicability to a broader spectrum of safety-critical applications. In future investigations, it may be advantageous to extend the scope by comparing a non-compliant design incorporating externally implemented safety mechanisms against a design utilizing a compliant component. Such an approach would enable a comprehensive assessment of component reliability from a system-level perspective. Another prospective avenue for research involves the practical realization of hardware designs followed by verification tests. The aim is to ascertain whether the empirical outcomes align with the theoretical values derived in this thesis.

In conclusion, the outcomes of this study provide useful insights to engineers, designers, and stakeholders seeking to balance safety considerations with hardware design. The study contributes to the ongoing discourse on hardware design, component failure and reliability in safety engineering within the framework of ISO 26262 compliance.

Bibliography

[1] A. Ismail and W. Jung, "Research trends in automotive functional safety," in *2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)*, 2013, pp. 1–4.

[2] https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries.

[3] "ISO26262: 2018 - Road Vehicles - Functional Safety," in *ISO*, 2018.

[4] ISO, "Road vehicles - Functional safety - Part 5: Product development at the hardware level," 2018, iSO 26262-5:2018.

[5] K.-L. Lu and Y.-Y. Chen, "ISO 26262 ASIL-Oriented Hardware Design Framework for Safety-Critical Automotive Systems," in *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*, 2019, pp. 1–6.

[6] A. Nardi and A. Armato, "Functional safety methodologies for automotive applications," in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2017, pp. 970–975.

[7] M. Chaari, W. Ecker, C. Novello, B.-A. Tabacaru, and T. Kruse, "A model-based and simulation-assisted fmeda approach for safety-relevant e/e systems," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1–6.

[8] R. Letor and R. Crisafulli, "Smart Power devices and new electronic fuses compliant with new E/E architecture for autonomous driving," in *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, 2019, pp. 1–6.

[9] P. Kilian, O. Koller, P. Van Bergen, C. Gebauer, and M. Dazer, "Safety-Related Availability in the Power Supply Domain," *IEEE Access*, vol. 10, pp. 47 869–47 880, 2022.

[10] P. Kilian, A. Köhler, P. Van Bergen, C. Gebauer, B. Pfeufer, O. Koller, and B. Bertsche, "Principle Guidelines for Safe Power Supply Systems Development," *IEEE Access*, vol. 9, pp. 107 751–107 766, 2021.

[11] ISO, "Road vehicles - Functional safety - Part 8: Supporting Processes," 2018, ISO 26262-8:2018.

[12] ——, "Road vehicles - Functional safety - Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses," 2018, ISO 26262-9:2018.

[13] ——, "Road vehicles - Functional safety - Part 4: Product development at the system level," 2018, ISO 26262-4:2018.

[14] R. Dardar. (2013) Building a safety case in compliance with iso 26262 for fuel level estimation and display system. [Online]. Available: http://mdh.diva-portal.org/smash/get/diva2:690954/FULLTEXT01.pdf

[15] "Bathtub curve." [Online]. Available: https://blog.ucsusa.org/dlochbaum/the-bathtub-curve-nuclear-safety-and-run-to-failure/

[16] N. Das and W. Taylor, "Quantified fault tree techniques for calculating hardware fault metrics according to ISO 26262," in *2016 IEEE Symposium on Product Compliance Engineering (ISPCE)*, 2016, pp. 1–8.

[17] "Infineon FuSA." [Online]. Available: https://www.infineon.com/cms/en/product/promopages/functional-safety-ISO26262/

[18] "TI FuSA." [Online]. Available: https://www.ti.com/technologies/functional-safety.html

[19] "TÜV SÜD." [Online]. Available: https://www.tuvsud.com/en-us/resource-centre/stories/iso-26262

[20] "IEC." [Online]. Available: https://webstore.iec.ch/publication/6946

[21] ISO, "Road vehicles – Functional safety – Part 11: Guidelines on application of ISO 26262 to semiconductors," 2018, iSO 26262-11:2018.

[22] "LM74700." [Online]. Available: https://www.ti.com/product/LM74700-Q1

[23] "STPM801." [Online]. Available: https://www.st.com/en/automotive-analog-and-power/stpm801.html

[24] "STPM801." [Online]. Available: https://www.eenewseurope.com/en/integrated-asil-d-hot-swap-and-ideal-diode-controller/

[25] "LM74700." [Online]. Available: https://www.ti.com/document-viewer/lm74700-q1/datasheet