Dipl.-Ing. Dipl.-Ing. Dipl.-Ing. Andreas Strasser, BSc MA

Towards Optimizing Safety-Critical Automotive Embedded Systems on Reliability for Automated Driving

DOCTORAL THESIS

to achieve the university degree of

Doktor der technischen Wissenschaften

submitted to

Graz University of Technology

Supervisor

Ao.Univ.-Prof. Dipl.-Ing. Dr.techn. Eugen Brenner

Advisor

Ass.Prof. Dipl.-Ing. Dr.techn. Christian Steger

Institute of Technical Informatics
Graz University of Technology

Graz, December 2020

Affidavit

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral dissertation.

Graz, 4. December 2020 .....

Kurzfassung

Der aktuelle Trend des vollautonomen Fahrens verändert derzeit die Automobilindustrie. Vollautonomes Fahren ist spezifiziert in den SAE (Society of Automotive Engineers) Automatisierungs Level 4 und 5 mit dem großen Wandel, dass der Fahrer zum Beifahrer wird. Momentan berücksichtigt der Sicherheitsstandard ISO 26262 den Fahrer als letzte Sicherheitsinstanz beim plötzlichen Eintritt eines unerwarteten Fehlers. In diesem Fall übergibt das Auto dem Fahrer die volle Kontrolle um das fehlerhafte Auto zum Stillstand zu bewegen. Durch den derzeitigen Wandel in der Automobilindustrie wird dieser Sicherheitsansatz nicht mehr möglich sein, weil der Fahrer über keine Möglichkeit mehr verfügt aktiv in das Fahrgeschehen einzugreifen. Der derzeitige ISO 26262 Standard verfügt nicht über geeignete Sicherheitsmethoden um Ingenieure und Sicherheitsmanager aktiv beim Umgang mit dieser neuen Situation zu unterstützen. Ein weiteres Problem, dass durch diesen Umstand entsteht ist der Bedarf an hochverfügbaren und zuverlässigen Systemen. Heutzutage werden diese Systeme mit einem speziellen Temperaturprofil entwickelt und im Falle einer Abweichung kann es im schlimmsten Fall zu einer Herabstufung des sogenannten Automotive Safety Integrity Level (ASIL) kommen. Diese Herabstufung wird aktuell nicht erkannt, aufgrund der fehlenden Regelschleife zwischen des tatsächlichen Temperaturverlaufs während des Betriebes und des theoretisch festgelegten Temperaturverlaufes. Das Ermöglichen dieser Regelschleife wird Ingenieure dabei unterstützen zukünftige Automotive Systeme auf reale Temperaturprofile hin zu optimieren und damit nicht nur die Robustheit und Zuverlässigkeit erhöhen sondern auch Kosten einsparen.

Diese Arbeit beschreibt neue Methoden wie kritische Situationen von vollautonomen Fahrzeugen gehandhabt werden können. Hierbei liegt der besondere Fokus auf Fahrzeuge die kompatibel mit den SAE Automatisierungs Leveln 4 und 5 sind. Die Methoden werden Ingenieure während des Entwicklungsprozesses dieser Systeme unterstützen und ermöglichen die Quantifizierung der Zuverlässigkeit. Diese Methoden werden es ermöglichen neue sicherheitskritische Automotive Systeme auf Zuverlässigkeit optimieren. Im Falle von Residualfehlern werden spezielle Sicherheitsmaßnahmen vorgestellt die in einem LiDAR Prototypsystem integriert wurden. Alle Methoden und Maßnahmen die in dieser Arbeit vorgestellt werden sind kompatibel mit dem aktuellen Sicherheitsstandard ISO 26262 und sind daher bestens geeignet zukünftig in automotiven Systemen eingesetzt zu werden.

Abstract

The Automotive Industry is disruptively changing with the current trend to fully-automated driving. Fully-automated driving is specified as Society of Automotive Engineers (SAE) Automation Level 4 and 5 with the big transformation of the driver that will become a passenger. Currently, the ISO 26262 safety standard of the automotive industry is using the driver as a last backup instance in case of uncontrollable failures. In case of such a failure the vehicle transfers full control back to the driver. In the next few decades the driver will have become a passenger and falling back to the driver will not be possible anymore. In the current ISO 26262 standard there are no methodologies available that support engineers and safety managers how to handle this new situation. Another problem that will arise with these vehicles is the need of highly robust and reliable systems. Nowadays, most of the systems are developed along a specific Mission Temperature Profile. In case of a mismatch between the real and the designed Mission Temperature Profile an Automotive Safety Integrity Level (ASIL) degradation can arise. This mismatch can not be evaluated nowadays due to the fact that there is limited field data available and there is no feedback loop available between the operation time and the related temperature data and its developers. But this feedback loop could support engineers in optimizing their automotive systems on real Mission Temperature Profiles and could enable their company to save costs.

This thesis describes novel methodologies on how to handle the critical situation of a driverless vehicle that is compatible with the SAE Automation Levels 4 and 5. The methodologies will support engineers during the development of these systems to be able to quantify reliability and will be a key enabler for optimizing safety-critical Embedded Systems in respect to reliability. For residual failures this thesis introduces safety enhancements for novel environmental perception systems in this case employed in a LiDAR system as prototype platform. All work presented in this thesis is compatible with the current ISO 26262 safety standard of the automotive industry and can therefore be used in the automotive domain.

Contents

List of Figures

List of Tables

Glossary

ACC Adaptive cruise control. 2

AD Automated Driving. 1, 4, 6

ADAS Advanced Driver Assistance Systems. 1, 2, 4–6, 14, 54, 55, 64, 77, 80, 84, 114, 120

AEC Automotive Electronics Council. 34

ASIC Application-specific Integrated Circuit. VIII, 21, 26, 27, 45, 76, 117

ASIL Automotive Safety Integrity Level. III, 7, 9, 11, 16, 39, 45, 52, 57, 61, 63, 64, 75, 84, 98, 107, 108, 120, 121

BCH Bose-Chaudhuri-Hocquenghem-Codes. X, 89, 91, 92

CFMEA Classification Failure Mode Effects Analysis. 53, 57, 58

CPU Central Processing Unit. 22, 43, 65, 74, 93, 102, 103, 117

ECC Error Correcting Code. X, 89, 90

ECU Electronic Control Unit. 14

ES Embedded System. 4

ESC Electronic Stability Control. 1

FIT Failure In Time. VIII–X, 8, 15, 24–27, 39, 63–65, 72–75, 84–86, 93, 94, 96–98, 107, 108, 112, 115, 117, 120–122

FMEA Failure Mode and Effects Analysis. 53

FPGA Field Programmable Gate Array. VIII, 21, 26, 27, 46, 48, 72, 76, 91

FSM Finite State Machine. 41

FTA Failure Tree Analysis. 53

GUI Graphical User Interface. XI, 85, 102, 108, 109

HARA Hazard and Risk Analysis. 16, 63, 64, 120

HDL Hardware Description Language. 22, 23, 26, 72

HTOL High-Temperature Operating Life. 34, 35, 37

IC Integrated Circuit. 35

IP Intellectual Property. IX, 23, 26, 71, 72

LDW Lane Departure Warning System. 2

LiDAR Light Detection and Ranging. III, VI–X, 4–6, 8, 9, 11, 19, 44–47, 60, 77–85, 87, 99, 102, 105, 108, 112–114, 116, 117, 120, 122

LOC Lines of Code. 14

MEMS Micro-Electro-Mechanical Systems. IX, X, 9, 19, 44–47, 77, 78, 80–83, 99, 105, 113, 116, 117

ML Machine Learning. 53, 57, 58

MOSFET Metal-Oxide-Semiconductor Field-Effect Transistor. 27

MRAM Magneto Resistive Random Access Memory. 41

MTBF Mean Time Between Failures. 4, 15, 24, 37, 38, 42, 64, 92, 112, 120

ODD Operational Design Domain. IX, 54, 55, 57, 59

OEM Original Equipment Manufacturer. 36, 38, 44, 76, 112

PLL Phase-Locked Loop. X, 80–82, 99, 116

PRYSTINE Programmable Systems for Intelligence in Automobiles. VIII, 10

Radar Radio Detection and Ranging. 6, 11

SAE Society of Automotive Engineers. III, 4, 5, 13, 54, 57, 59, 102, 105, 111, 113, 114

SEooC Safety Element out of Context. 7, 23

SEU Single Event Upset. 90

SM Smart Mobility. 1

STAMP Systems-Theoretic Accident Model and Processes. 50

STPA Systems-Theoretic Process Analysis. VI, 49–51, 57

UDP User Datagram Protocol. 85, 86

VHDL Very High Speed Integrated Circuit Hardware Description Language. 71

Chapter 1

Introduction

> *"Kelly was a seaman, and his life on the water followed a strict routine, which meant observing all the safety rules that had been written in the blood of less careful men."* - Tom Clancy, "Without Remorse"

Smart Mobility (SM), Automated Driving (AD) and Advanced Driver Assistance Systems (ADAS) are all innovative concepts of the Automotive Industry that will disruptively change well-known habits of the society, but also the design and development of novel automotive systems.

In the past, developers had the possibility to rely on the driver as a last safety instance in case of unintended occurence of failures [10]. But this will not be possible anymore in case of Automated Driving. Automated Driving means that the vehicle is able to perceive the environment, predict situations on the road, make decisions and fully control the vehicle on its own without any intervention from external parties and will transform the driver into a passenger [34]. This transformation could be disconcerting for some drivers but there are survey results available with a close majority of drivers that are open minded in respect to these novel systems [35]. The general acceptance of this technology is a good starting point for introducing novel ADAS and more advanced Automated Driving system but also involves a high responsibility. Considering the case that a single point of failure is able to trigger a car accident resulting in possible fatalities, this euphoric attitude and the overall acceptance of Automated Driving for the society but also for the government could rapidly change [36]. For that reason, automotive systems have to be developed with high safety standards.

Passenger safety is the most important target when developing a vehicle with development already started in the 1960s [37]. Over the last decades, the amount of systems that are actively supporting the driver in dangerous situations steadily increased such as the Electronic Stability Control (ESC) [38]. Nowadays, detailed safety standards are omnipresent in the automotive industry and most of them already emphasize the develop-

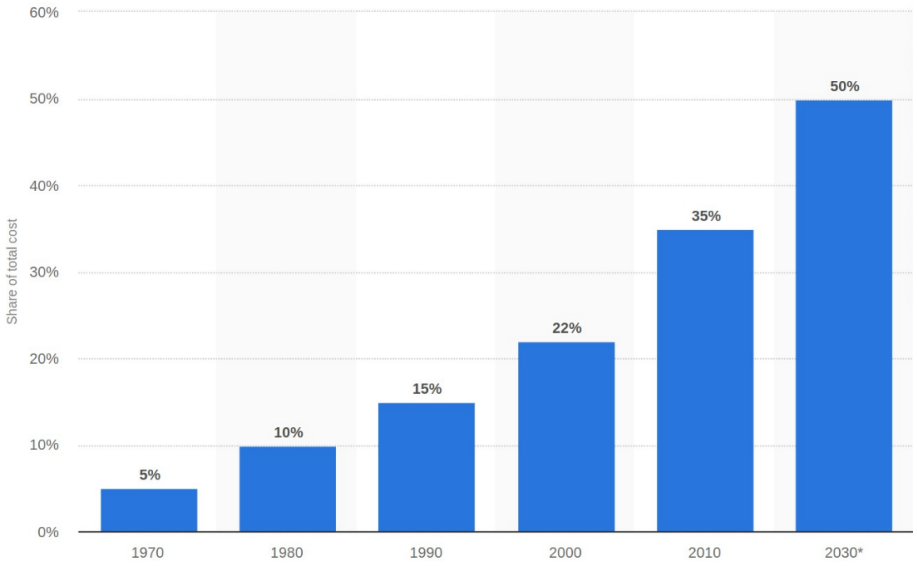

Figure 1.1: Overview of the overall costs of the Automotive electronics in percentage between 1970-2030 [1].

ment of electronic systems [10]. Comparing the early safety systems with modern systems clearly reveals that modern systems are highly integrated electronic systems that have integrated the whole logic inside software modules and these modules are executed on semiconductor devices [39].

In Figure 1.1, the relevance of electronic systems can be seen by analyzing the overall percentage rate of electronic costs in total to the car. In the 1970s, about 5% of the total car cost was spent on electronic systems and in 2010 this already increased to 35%. This significant change was triggered, among other things by steadily increasing the amount of active safety systems. In the next decade, the automotive industry is expecting that the total car cost will be determined by 50% of the electronical systems [1]. Considering current political decisions of the European Union, that vehicles released in 2022 or later have to include safety related ADAS such as the Lane Departure Warning System (LDW) or Adaptive cruise control (ACC) also support this valuation [40].

The decision of the European government that legally requires the automotive industry to introduce ADAS into every vehicle that will be released in the European Union also positively influences the development of novel ADAS and especially next generation systems that should have the ability of fully automated driving. Therefore, over the next decades the vision of automated driving could become reality and the development of these systems has already begun in the last few years and there are already examples available that are able to drive autonomously under specific circumstances such as the Tesla Autopilot [41]. In the automotive industry, the “ISO 26262 - Road Vehicle Functional Safety” [10] standard is the most important standard for developing safety relevant

electronic systems. One of the most important functional safety concepts of this standard is that a safety mechanisms is able to transit an item into a safe state or if not possible alert the driver to control the effect of the failure. But considering the fully Automated Driving scenario, there will be no driver available anymore to take full control of the vehicle. Therefore, the design principles and processes to develop a "safe" vehicle are not able cover the high complexity of future fully automated driving vehicles. This raises a need for novel approaches, especially for electronic devices, to enable safe driving for the passengers as well as other road participants.

1.1 Motivation

Mobility is one of the most important achievements of our society and enabled the age of globalization. Highways are connecting people and also enable the exchange of products and services among villages, federal states and countries. The next step is the transition from mobility to smart mobility that will enable more intelligent ways of employing vehicles, urban areas and the road infrastructure [42]. One of most important bearers of hope is the fully automated driving functionality. On one side it will allow for more recreational time during driving activities, especially for commuters, but also will decrease the amount of vehicle accidents caused by human factors such as tiredness and negligence.

The society is already awaiting this innovative step but the automotive industry is fully focused on developing industry standards for ensuring the safety for this special systems such as the ISO 21448 - Safety of the intended function [43]. Especially the novel ISO 26262 [10] from 2018, there is still the mindset that the last safety instance is the driver and also that this last instance will be responsible. Therefore, this standard is not future-proof considering fully automated driving vehicles. To prevent disastrous consequences, the suggested methodologies and approaches of this standard need to be analyzed and evaluated and novel approaches needs to be developed to improve the overall safety of fully automated driving functions.

1.2 Goals

This thesis claims to demonstrate possible capabilities in improving the overall safety of critical automotive Embedded System (ES) for Automated Driving. The main focus is on providing a base for further discussion and not on representing bullet-proof methodologies that can directly be implemented in the automotive industry for mass production. The intended goals can be partitioned in a main and a supplementary goal:

- **Main Goal**
  Introduce novel methodologies that support safety engineers in optimizing safety-critical Embedded System from the design phase up to decomposition and provide feasible results and demonstrators.

- **Supplementary Goal**
  Optimize current ADAS environment perception sensors such as Light Detection and Ranging (LiDAR) to improve the overall safety as well as to enable safety related principles such as redundancy.

Based on these two goals this thesis introduces the following hypothesis:

> *Automotive LiDAR systems for Society of Automotive Engineers (SAE) Automated Level 4 upwards compatible vehicles can be optimized on reliability to extend the Mean Time Between Failures (MTBF) and any deviations can be detected in the whole lifecycle from the early development phases until decomposition.*

1.3 Research in this Thesis

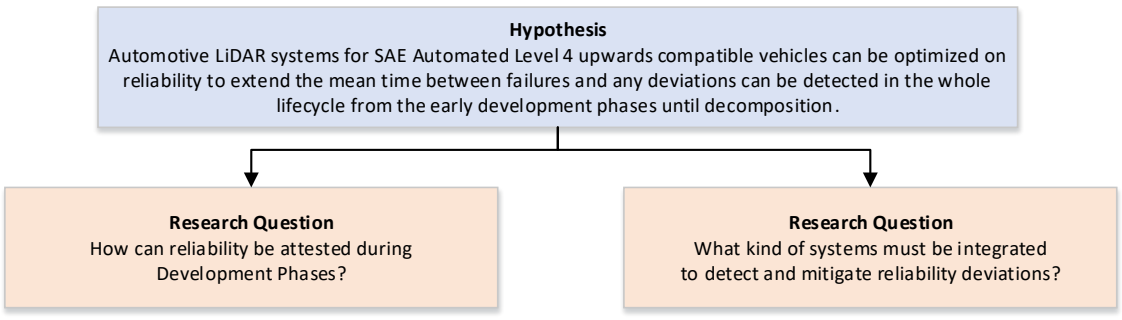

Figure 1.2: Research question and hypothesis of this thesis.

The hypothesis that was introduced in the Goals section enables the definition of the following two research questions as seen in Figure 1.2:

- **Research Question A**
  How can reliability be attested during Development Phases?

- **Research Question B**
  What kind of systems must be integrated to detect and mitigate reliability deviations?

1.3.1 Challenges

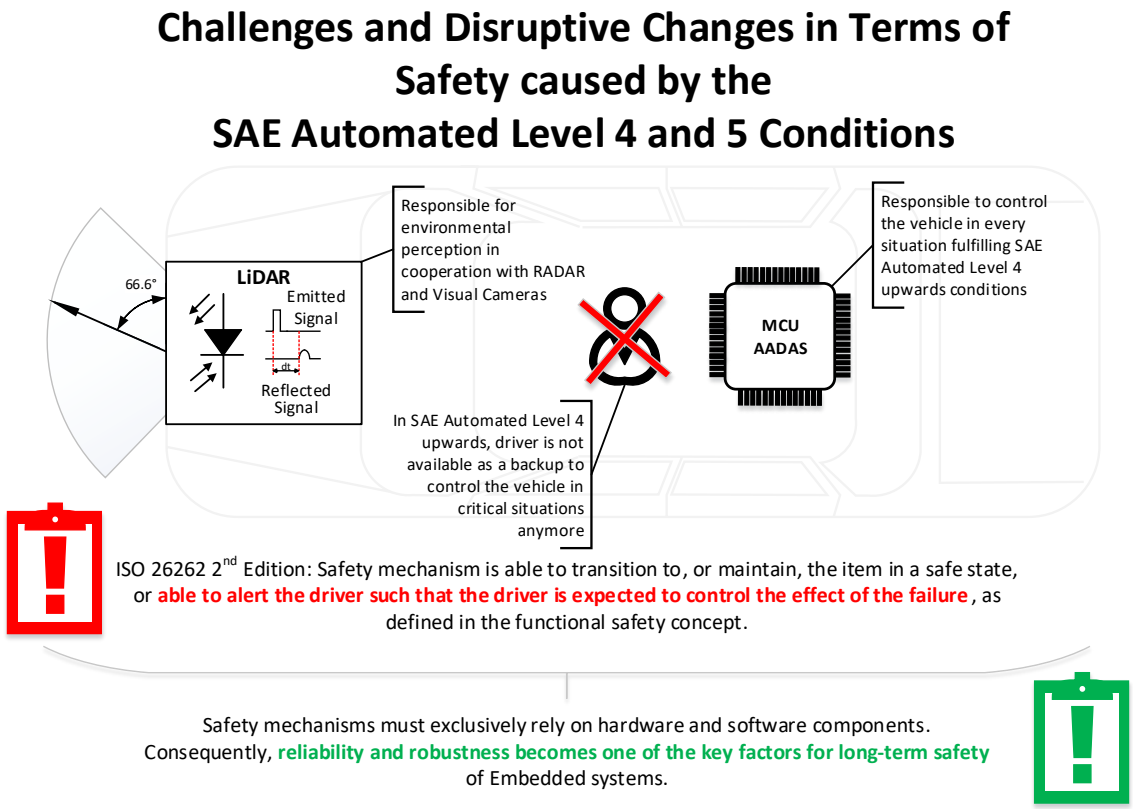

Figure 1.3: Conceptual description of novel safety challenges that will be introduced with SAE Automated Level 4 and upwards.

The transition from a traditionally controlled vehicle to an automatically controlled vehicle is mainly defined through the disappearing of the human driver that is capable of driving the vehicle on his own. In the SAE Automated Level 4 and 5 this circumstance changes and the driver becomes to a passenger. Figure 1.3 depicts this novel situation with a LiDAR system as an environmental perception system. In modern vehicles, there will be two main parts that are responsible for controlling the vehicle in a safe way: Environmental Perception Sensors and Advanced ADAS. The Environmental Perception Sensors are responsible for sensing the particular surroundings of the vehicle with specific

sensors such as LiDAR, Radar or Vision Cameras. The Advanced ADAS is responsible for processing the sensor data and controlling the vehicle in every situation. The driver will be upgraded to a passenger and will not be available anymore as a last safety instance that is able to control the vehicle in safety-critical situations. Therefore, the following challenges arise through this novel automated driving concept:

- **Disappearing Human Driver as Last Safety Instance**
  The current ISO 26262 standard [10] released in 2018 still refers to the driver as last safety instance in case of uncontrollable driving situations in case of failures.

- **ISO 26262 standard does not provide Fully Automated Vehicles focused Methodologies**
  Fully Automated vehicles completely rely on technical systems and any problem that occurs during their operation must be handled by the system on its own. This circumstance requires highly robust and reliable systems to guarantee safety. The current ISO 26262 standard [10] lacks support for focusing on optimizing novel fully automated driving systems on reliability.

- **Highly Reliable Environmental Perception Sensors**
  The Environmental Perception Sensors have the purpose to sense the surroundings next to the vehicle and can be implemented in different ways such as LiDAR, Radar, and Vision Cameras. Caused by the fact, that the processing unit of the car only can process data that is available and valid from the sensor it is necessary to continuously provide data. In case of a failure, the sensor should be able to recover from any state as fast as reasonably possible to continue driving without any sight such within a couple of centimeter.

1.3.2 Problem Statement

The development of novel safety-critical automotive systems for Automated Driving (AD) introduces novel requirements such as the full control of the vehicle in any situation caused by the omission of a driver as last safety instance. Furthermore, these novel functions will mostly be integrated in software, as described in Section 2.4, and strongly rely on the hardware of the Embedded System and are often built as highly-integrated semiconductor devices. Any fault inside these integrated circuits could directly trigger a failure on the system level that potentially leads to a total failure of the system. Through the fact that the driver was upgraded to passenger this can directly lead to an accident that could damage objects but also inflict harm on occupants and other road participants. The usage of highly integrated circuits and the transition to SAE Automation Level 4 and upwards directly leads to the following problems that this Thesis must face:

- No Hardware/Software Co-Design Development Flows that focus on optimizing systems on reliability.
- Higher cost that are related to late changes of system requirements such as safety. The later any requirement deviations or system design flaws are detected the higher becomes the effort that must be procured to eliminate these mismatches. This could lead to concealing safety issues in order to prevent these expensive changes.
- Component reliability requirements are based on mission temperature profiles that are defining in which temperature ranges the system will be operated at which specific amount of time. These temperature profiles are best practices and are based on expert judgments but are not evaluated at later stages of the lifecycle. Consequently, there could be mismatches between the desired and the actual temperature profile and this could lead to hidden ASIL degradations.
- Integrated Semiconductor components are often developed as Safety Element out of Context (SEooC) and most of the requirements are based on assumptions such as the temperature profile and usage of the component. The integrator is responsible for the safety integration, but there could be still responsibility gaps such as guarantee invocations for the supplier.
- ISO 26262 allows the "Proven in Use" argumentation for novel products that are based on previous released systems. To guarantee the effectiveness of their safety requirements it is necessary to perform an analysis of the field data that is observing the occurred incidents. In Part 11 "Guideline Semiconductor" states a constraint that this argument can be restricted caused by the fact that an effective field monitoring program can be challenging and typically the field feedback is limited. Therefore, there is a missing link between the designed mission temperature profile and the real temperature profile of the component during operation.

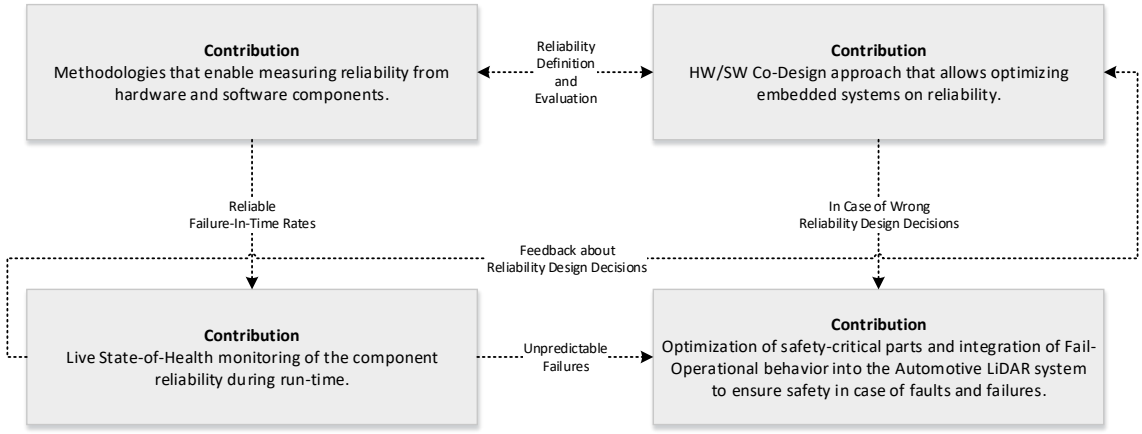

Figure 1.4: Overview of the contributions and their relations that will be provided by this thesis.

1.3.3 Contributions and Significance

This thesis provides the following contributions as seen in Figure 1.4:

1. Methodologies that enable measuring reliability of hardware and software components.
2. HW/SW Co-Design approach that allows optimizing embedded systems on reliability.
3. Live State-of-Health monitoring of the component reliability during run-time.
4. Optimization of safety-critical parts and integration of fail-operational behavior into the Automotive LiDAR system to ensure safety in case of faults and failures.

All four contributions that are provided by this thesis are related and belong to a single problem field as follows:

The methodologies that enable the measurement of reliability on hardware and software levels are directly connected the novel HW/SW Co-Design approach through the definition of the reliability in the design process and the evaluation of these requirements. This enables the optimization on reliability of the novel safety-critical Embedded Systems that are designed for SAE Automated Level 4 and upwards vehicles.

There is also a direct link between the Live State-of-Health monitoring system and the methodologies that enable measuring reliability. With these novel methodologies the safety monitor is able to measure reliable FIT Rates.

The Live State-of-Health monitoring system also enables a feedback loop between the designed reliability requirements and gives feedback about the reliability design decisions. Any deviation can be detected during operation time and actively be eliminated by

firmware or software updates. This allows to long-term comply with safety requirements such as ASIL levels and the detection of ASIL degradations.

In case of wrong reliability design decisions there must be a safety measure that is still able to control the safety-critical situation. For that reason, the last contribution is about optimizing the current safety-critical parts of the LiDAR system as well as integrating novel fail-operational behavior to ensure safety in case of faults and failures.

The last link is between the Live State-of-Health monitor and the LiDAR system. If any unintended and unpredictable failure arises than the LiDAR system will take over the control and handles the specific safety-critical situation.

1.4 Thesis Structure

This thesis is structured as follows:

- **Chapter 1** can be found on page 1 and gives an introduction into this thesis with the main motivation, goals, and research topics. The research subchapter also provides information about the research questions, challenges and the contribution.
- **Chapter 2** starts with page 11 and provides background information that is necessary to understand this thesis such as the vision of automated driving, system engineering process, SAE Automation Levels, increasing complexity of hardware and software modules, and the component reliability of hardware components.
- **Chapter 3** on page 19 provides research results in the fields of this thesis. Their are four main parts that are related: Safety in the automotive field, semiconductor reliability, 1D MEMS Micro-Scanning LiDAR and aging monitoring of electronic components.
- **Chapter 4** on page 61 describes novel methodologies and functionalities of this thesis regarding safety in the field of safety-critical Embedded Systems. The Chapter is divided in two parts: Safety enhancements for the 1D MEMS Micro-Scanning LiDAR system and Methodologies that enables optimizing safety-critical Embedded Systems on reliability.
- **Chapter 5** on page 89 provides experimental results of the safety enhancements and evaluation of the novel introduced safety methodologies.
- **Chapter 6** on page 111 gives details about the limitations and the future work that can be done as well as a conclusion about the whole thesis.

Chapter 2

Background

"Knowing is not enough; we must apply. Willing is not enough; we must do."

- Johann Wolfgang von Goethe

This section gives an overview of the most important background facts that need to be considered when reading this thesis.

2.1 Vision of Automated Driving

2.1.1 General Overview

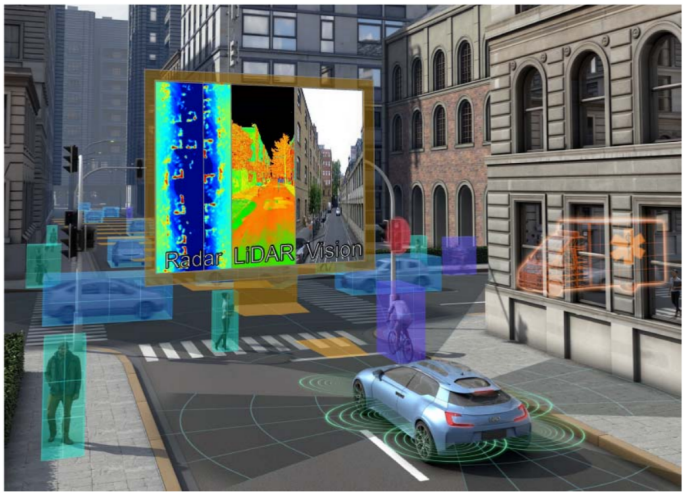

Figure 2.1: Conceptional overview of a fail-operational urban surround perception system by PRYSTINE [2].

Automated Driving is the ability of a vehicle that is capable of moving safely without any external input e.g. from a driver by perception of its environment [44]. This ability

requires a variety of sensors, as seen in Figure 2.1, to enable the environmental awareness such as [2]:

- Radio Detection and Ranging (Radar)
- LiDAR
- Vision Cameras
- Ultrasonic

2.1.2 Light Detection and Ranging

The LiDAR technology will be the base for robust and safe automated driving functionalities in modern vehicles [3].

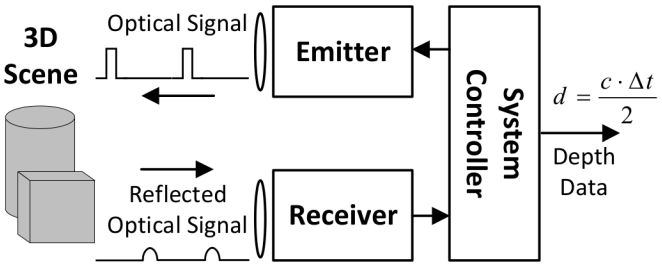

Figure 2.2: Conceptional illustration of the LiDAR principle [3].

Figure 2.2 depicts the general working principle of a LiDAR system. The LiDAR system is transmitting an optical laser signal into a 3D scenery. This signal will be reflected by obstacles that are placed inside the 3D scenery and are sensed by the receiver optics. The controller system is responsible to process the measurement results of the sensor and to compute the distance between the object on the road and the vehicle. This is done by measuring the elapsed time from transmission to reception at the speed of light (time-of-flight) [3].

Nowadays LiDAR can not be found in middle-class vehicles yet, due to the fact that these systems are too expensive. For that reason, Druml et al. have developed a novel 1D MEMS Micro-scanning LiDAR platform that is based on a micro-mechanical structure with the target to decrease the costs of the overall LiDAR system to about 200$ as well as to support Automotive Safety Integrity Level (ASIL) C [3].

2.2 Systems Engineering Process

A system can be summarized as a set of hardware, software, people and facilities to reach a specific goal. The engineering process of a system contains the whole lifecycle from

the development of the system until the decomposition and disposal of the individual components [45].

2.2.1 V-Model

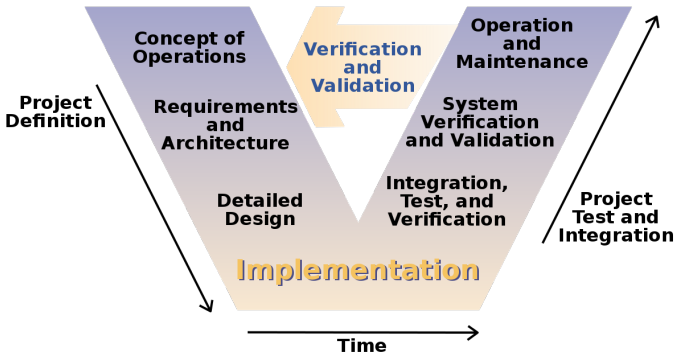

Figure 2.3: Overview of the V-Model of the Systems Engineering Process [4].

The V-Model, as seen in Figure 2.3, is the defacto standard for systems engineering in the automotive industry and is also integrated in the ISO 26262 standard [10]. The left branch represents the system definition and the right branch the integration and testing. Below is the basis that represents the implementation of the system. The system definition starts at a high level of representation and is systematically becoming rich in detail when moving forward on this branch. After the implementation, the project is climbing up the right branch and is validating and verifying the system requirements on different levels [5].

2.2.2 Development Costs

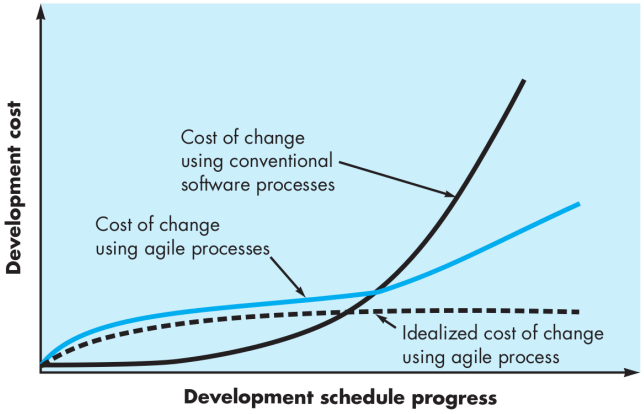

Figure 2.4: Increasing Development costs with increased time [5].

One of the biggest challenges in developing systems is the cost of change. In general, using traditional systems engineering processes the fact will arise that with advanced time the amount of work that has to be spent for making changes is growing exponentially over time. By using agile processes this exponential trend can be partly compensated, but the amount of costs is still rising continuously [5].

2.3 Automation Levels

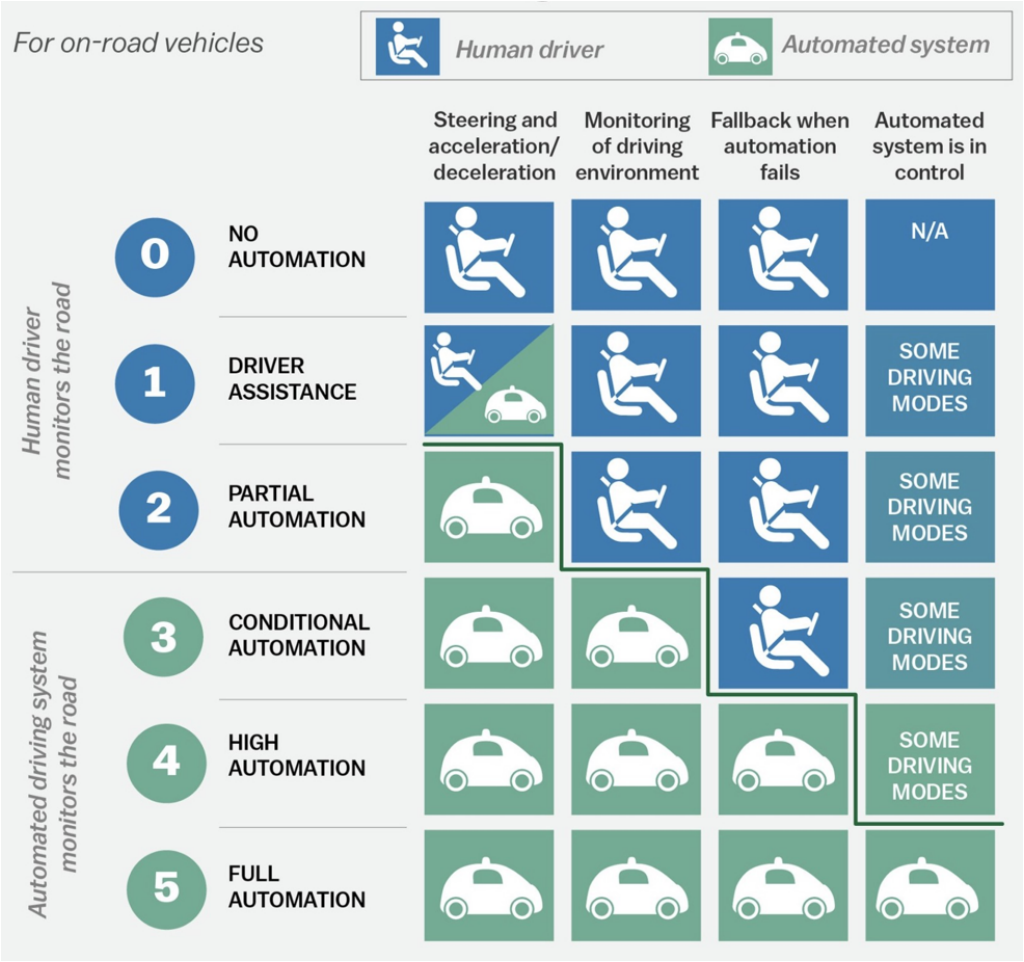

Figure 2.5: Overview of the five different SAE Automation Levels of driving [6].

The Society of Automotive Engineers has defined five different automation levels for on-road vehicles as seen in Figure 2.5. In the first and second class, the vehicle is able to support the driver with steering and acceleration, but monitoring the system and safety fallback must be handled by the driver. From class three onwards, the automated driving systems should be able to fully monitor the driving environment as well as handle steering

and acceleration. Only in the fourth and fifth class is the vehicle able to perform as a fallback in case of failed functions. In the last class, the automated vehicle is able to take over the control for every situation and does not rely on the driver as a last safety instance [34, 6].

2.4 Increased Hardware and Software Complexity

Modern vehicles are steadily integrating novel features such as ADAS and therefore the amount of Electronic Control Unit (ECU) are also steadily increasing. Nowadays, a modern, luxury car already contains about 150 ECUs [46].

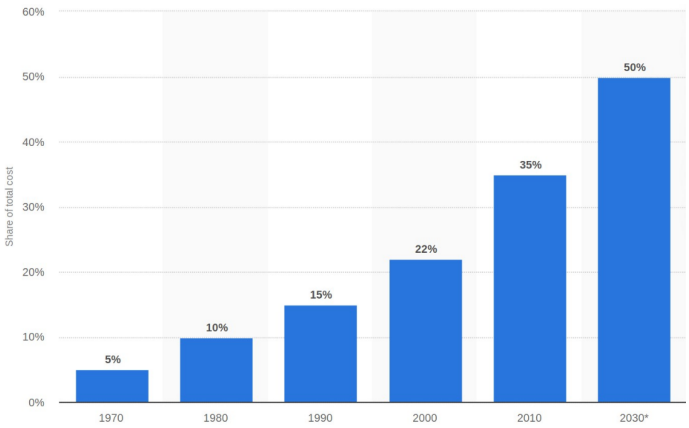

Figure 2.6: Electronic costs percentage of the overall car between 1970 and 2030 [1].

In modern vehicles, the amount of functionalities that are getting electrified is steadily increasing since the 1970s as seen in Figure 2.6. The reason for this trend is the electrification of certain mechanical functionalities such as steering, but also caused by the fact that more and more safety related ADAS are integrated into a modern car. In the next decade, this trend will be continued [1, 46].

Simultaneously with the increasing amount of ECUs there is also the trend of increasing Lines of Code (LOC). For fully automated vehicles this trend will continue, consider Googles Self-Driving car that already contains about 2 Billion LOC [47].

2.5 Component Reliability

2.5.1 Bathtub Curve

Electronic components usually fail at the beginning and at the end of their operational time. This is also known as bathtub curve as seen in Figure 2.8. The amount of time between the beginning of the operation time and the first failure is described as Mean

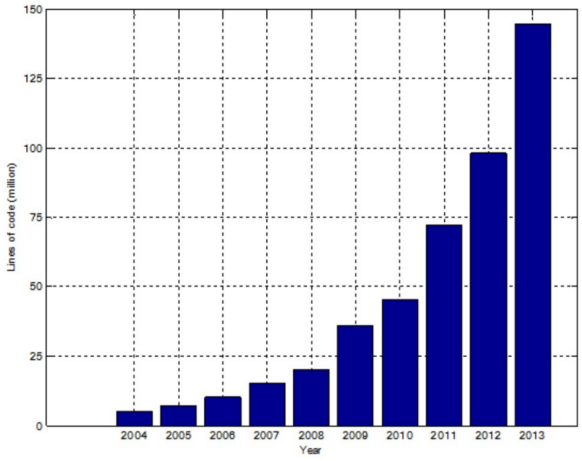

Figure 2.7: Lines of Code from a vehicle between 2004 and 2013 [7].

Time Between Failures (MTBF). The reciprocal value of the MTBF, commonly used in the automotive domain, is described as the Failure In Time (FIT) [10].

2.5.2 Degradation

The MTBF value is not a fixed value that is only determined by the physical structure of the semiconductor device. Instead, the MTBF value can change dynamically according to the physical temperature stress as seen in Figure 2.9. Higher temperature directly influences the reliability of electronic components. As a rule of thumb it can be said that with every 10°C more, the expected lifetime of the component will be halved [9]. The derating factor that is influencing the lifetime can be calculated by using the Arrhenius equation [9]:

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \tag{2.1}$$

where:

DF is De-rating Factor

$\mathbf{E_a}$ is Activation Energy in eV

k is Boltzmann Constant (8.167303 x 10^{-5} ev/K)

$\mathbf{T_{use}}$ is Use Junction Temperature in K

$\mathbf{T_{stress}}$ is Stress Junction Temperature in K

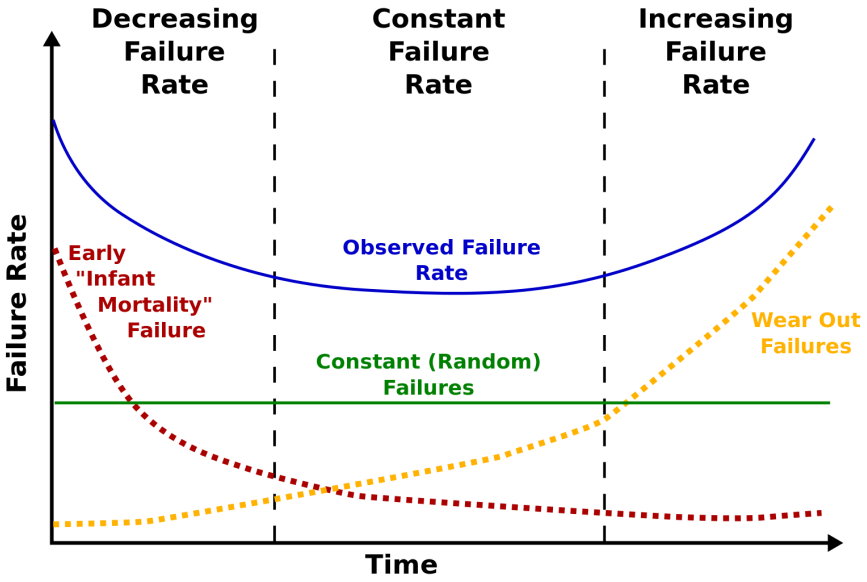

Figure 2.8: Bathtub curve that represents the probability of a failure over time of an electronic device [8].

2.6 Automotive Safety Integrity Level

The Automotive Safety Integrity Level is defined in the ISO 26262 standard [10] and is one out of four specific safety levels that specify the necessary requirements of the item as well as the safety measures with the goal to avoid unreasonable risks [10].

The ASIL level is derived from the Hazard and Risk Analysis and is determined through the three dimensions: Severity, Exposure and Controllability. The rating of the ASIL level can be looked up inside a table and is always specified by the judgment of a safety expert [10].

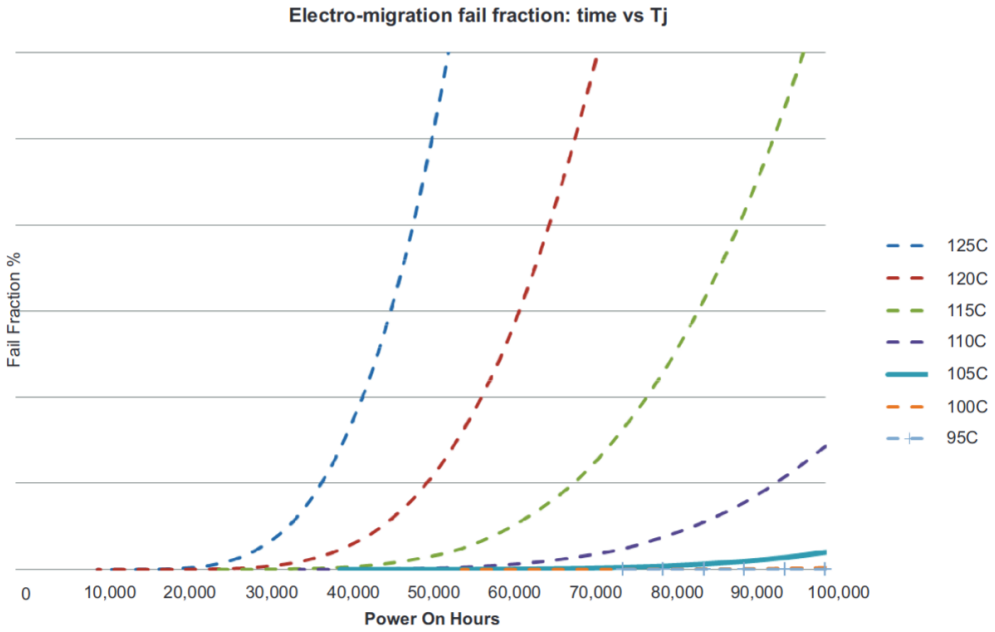

Figure 2.9: Impact of temperature on hardware failures [9].

Chapter 3

Related Work

> *"Dicebat Bernardus Carnotensis nos esse quasi nanos gigantum umeris insidentes, ut possimus plura eis et remotiora videre, non utique proprii visus acumine, aut eminentia corporis, sed quia in altum subvehimur et extollimur magnitudine gigantea."* - Johannes von Salisbury (Metalogicon)

This chapter provides an overview of the latest scientific and industrial work that is related to this thesis. The main topics are safety in the automotive domain, semiconductor components reliability, 1D Micro-Electro-Mechanical Systems (MEMS) Micro-Scanning LiDAR platform for enabling continuous environmental perception of the close surrounding of a vehicle, and common approaches to continuously monitor the live state-of-health of the overall system considering reliability.

Hint: Section 3.1.2 about semiconductor safety starts on page 21 and Section 3.2 starts on page 24 containing information and research results that were gathered in the "Selected Topics Embedded and Automotive Systems" seminar [12].

3.1 Safety in the Automotive Field

The main standard for safety in the automotive field is ISO 26262: Road vehicles - Functional safety standard [10]. The latest version was released in 2018 that, among other things added a novel part about semiconductor safety called: "Part 11 - Guideline on application of ISO 26262 to semiconductors".

3.1.1 Overview ISO 26262 Standard

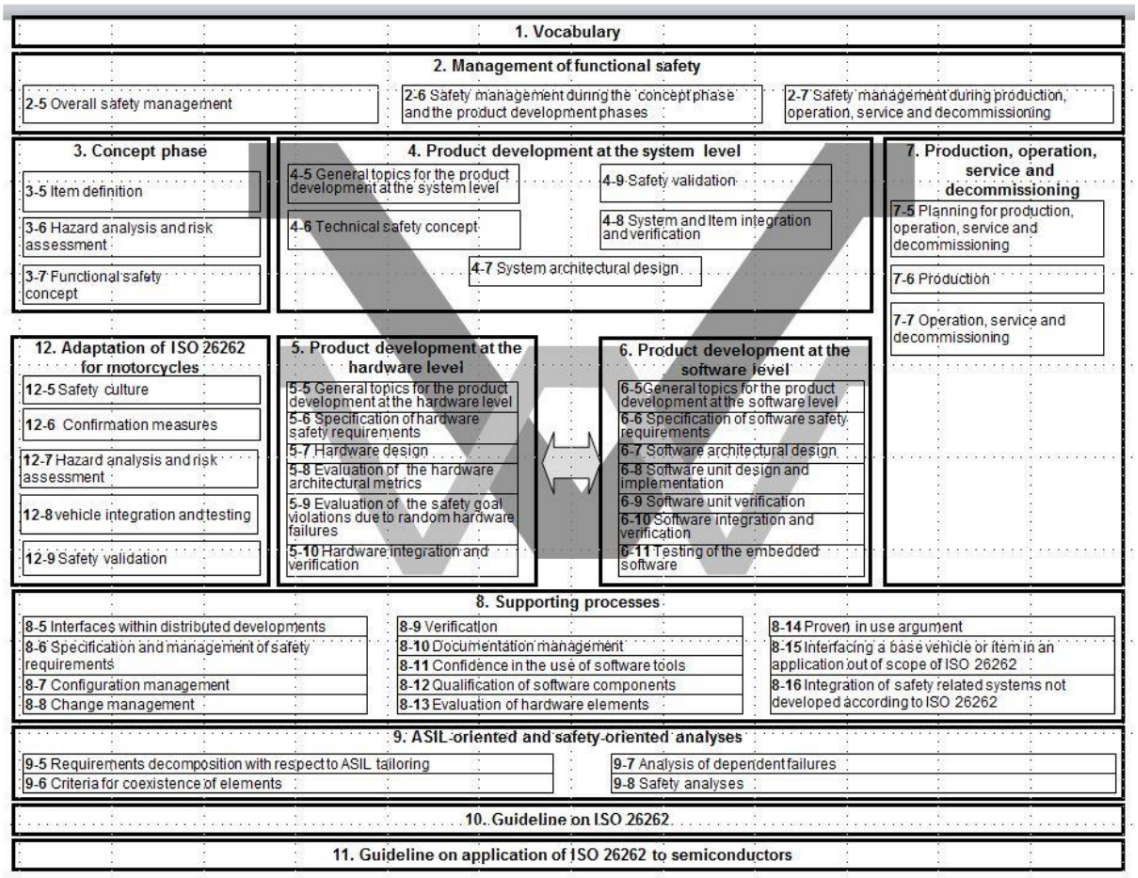

Figure 3.1: Overview of the ISO 26262 Standard and the relations between the individual parts [10].

The ISO 26262 standard, depicted in Figure 3.1 is intended to support developers and manufacturers of safety-related electronic and electrical systems for mass production road vehicles [10].

The main focus of this standard is to provide solid methodologies to analyze possible hazards that are caused by malfunctioning behavior of safety-critical parts of the electrical or electronic system. The standard especially focuses on the complex interaction between

individual systems and the related possible malfunctions [10].

Figure 3.1 clearly shows the strong interaction and collaboration of the particular lifecycle phases from the concept phase of the component up to the supporting processes that include the verification and documentation. Another important fact is that the whole standard provides a management process that includes the definition and introduction of novel key words that can be found in the Part 1 Vocabulary section [10].

3.1.2 Guideline on Semiconductor Safety

In 2018, the ISO 26262 standard released a best practice part about the application of the ISO 26262 on semiconductor devices to support the safety process of these devices.

Semiconductor Technologies

Semiconductor devices are a heterogeneous group of electronic components that are highly integrated components for a specific function implemented in silicon, germanium and gallium. These semiconductor devices can be implemented as an Application-specific Integrated Circuit (ASIC) chip or synthesized into an Field Programmable Gate Array (FPGA) [11, 48, 49, 12].

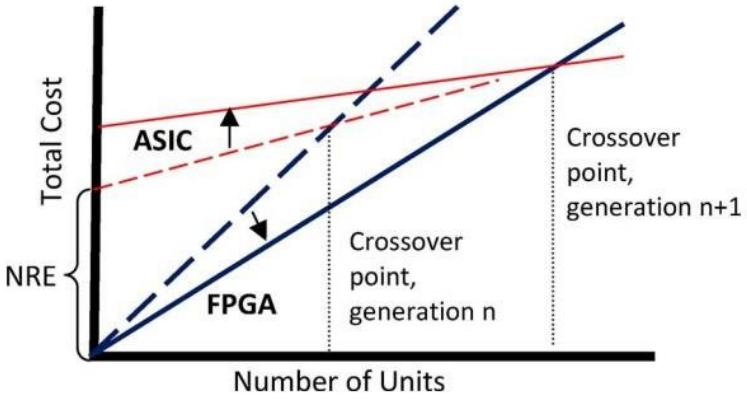

Figure 3.2: Relation between the total costs and the number of units between ASIC and FPGA [11, 12].

The decision between FPGA or ASIC that will be used for an electrical component is on the one hand related to the specific design of the circuit because for analog circuits there are no industrial proofed FPGA boards that can synthesize massive integrated analog circuits. Therefore, just for digital circuits a decision between both technologies is necessary. On the other hand the decision is always a tradeoff between the unit cost, performance and power consumption as seen in Figure 3.2 [50, 12].

Overview ISO 26262 Part 11

Applying the ISO 26262 standard on semiconductor devices can be a hard challenge considering the heterogeneous technology and the rapid change of the semiconductor scale. Additionally, semiconductor safety challenges the engineers in an extraordinary way considering the fact that there are also design flows in which black box components are integrated on the logical gate level as encrypted Hardware Description Language (HDL) or on the physical layer as chip layout. Consequently, the ISO 26262 Part 11 does not represent a bullet proof standard that can directly be applied in every project. Instead the standard provides information and an overview about the general challenges and best practices how to face and control these challenges [10, 12].

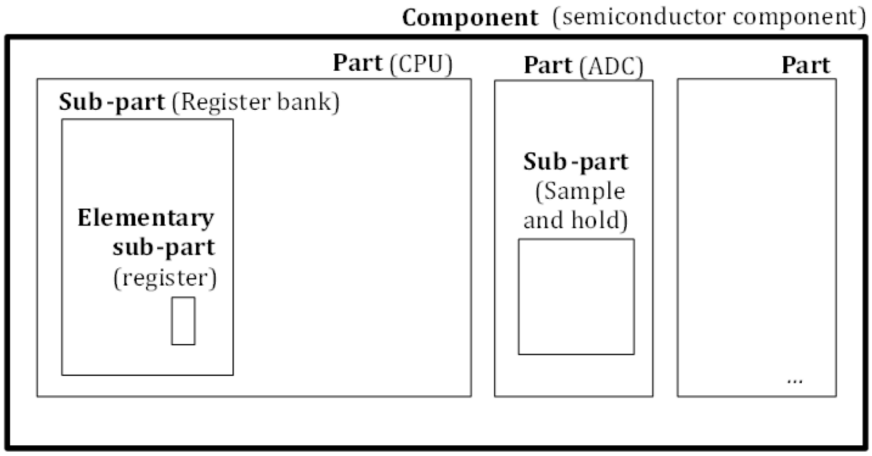

Figure 3.3: Partitioning of a semiconductor device specified in the ISO 26262 standard [10].

Semiconductor Partitioning is an important step to define the general language. This step is necessary to build an unified picture for all engineers and safety managers. Figure 3.3 depicts the general partitioning of the semiconductor device as described by the ISO 26262 standard. The whole device is called component and consists of individual parts such as the Central Processing Unit (CPU). These parts consist of several sub-parts such as the Register bank, which is a set of elementary sub-parts, in this case registers. The smallest entity is represented by the elementary sub-part and enables analyzing the device on different layers [10, 12].

Hardware Faults, Errors and Failures are logically connected inside integrated circuits as seen in Figure 3.4. Based on the definition of the semiconductor partitioning a Fault is triggered inside a physical unit of the elementary sub-part and triggers an Error on that logical level. This Error will be propagated to a Failure of the component and

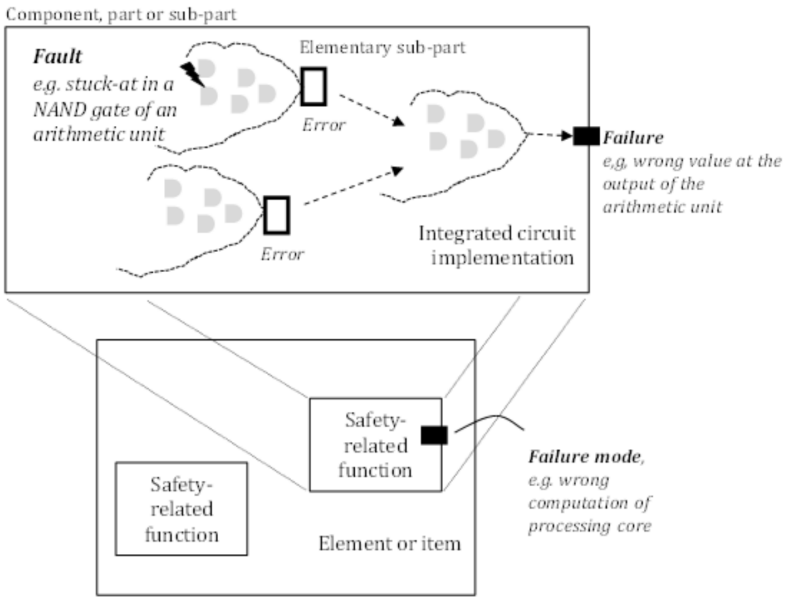

Figure 3.4: Relationship between hardware faults and failure modes [10].

triggers a specific Failure mode on the item level [10]. The most important fact is the understanding that a single Fault inside an elementary sub-part can trigger a Failure mode on item level. Therefore, the reliability of each component directly influences the overall safety level of the item [12].

Intellectual Property (IP) is describing the process of reusing existing design blocks that are implemented on logic level as HDL or on physical level as the chip layout. Most of the time, the design blocks are developed as SEooC, but there is also the possibility of using existing IP cores and support the reliability and safety claims with the "Proven In Use" argumentation [10, 12]. Nevertheless, the standard declares that the "Proven In Use" argumentation should not be applied because of the following reason [10]:

> *The conditions surrounding the validity of the "proven in use" argument can be restricting. Ensuring that an effective field monitoring program described in ISO 26262-8:2018, 14.4.5.3 is in place can be challenging due to the typically limited field feedback from designs incorporating IP or due to differences in IP configuration.*

This statement clearly describes the serious challenge of long term reliability and safety of semiconductor components. Currently, there is not enough field feedback available to evaluate the overall reliability of the components [12].

3.2 Semiconductor Component Reliability in the ISO 26262

The reliability of semiconductor components is measured in Mean Time Between Failures or in the automotive domain also described by the Failure In Time Rate that represents the reciprocal MTBF value. These values describe the amount of failures after a specific amount of time, in general one billion hours (10^9), and represents an indicator for reliability. The reliability of a component is directly connected to safety because a single fault inside an elementary sub-part such as a stuck NAND gate can trigger a Failure mode on item level [10, 12].

3.2.1 Failure Rate Estimation

The FIT Rate must be calculated using additional standards such as IEC TR 62380 [51]. This standard provides information about calculating the specific values by strict mathematical models that require the input of specific semiconductor process parameters and technology usage as well as the amount of elements that are used. But there is also the possibility to derive these values using field tests and statistical models such as the Chi-Quadrat test [10, 51, 12].

3.2.2 Temperature-Correlated Reliability

From a reliability point of view the temperature has the biggest impact on the overall reliability of the component. Higher temperatures actively degrade the overall FIT Rate of the component. In general is the FIT Rate represented at a specific temperature and is listed in the datasheet of the specific component. This specific FIT Rate can be adapted to other temperature ranges with the Arrhenius Equation as seen in (2.1) [10, 51, 12].

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \tag{3.1}$$

where:

DF De-rating Factor

E_a Activation Energy in eV

k Boltzmann Constant (8.167303 x 10^{-5} eV/K)

T_{use} Use Junction Temperature in K

T_{stress} Stress Junction Temperature in K

As seen in Equation (3.1) the temperature is stressing the reliability of the component in an exponential way. If we consider developing a novel safety-critical system for the automotive domain in which the temperature range is between $-40°C$ - $140°C$ degrees and we would have to think about the worst case scenario, the engineer has to use the highest temperature for dimensioning the physical semiconductor components. But this approach would lead to high cost and would be not realistic because the device is not operating at this high temperature all the time. For this purpose, the industry has introduced Mission Temperature Profiles [10, 51, 12]

3.2.3 Mission Temperature Profiles

Ambient Temp (T_A) in °C	% Time	De-Rated Fit (1)	FIT × % Time
-5	2%	0.01	0.0002
5	8%	0.03	0.0024
15	10%	0.08	0.008
25	15%	0.21	0.0315
35	20%	0.5	0.1
45	18%	1.15	0.207
55	15%	2.5	0.375
65	5%	5.2	0.26
75	5%	10.36	0.518
85	2%	19.88	0.3976
			1.8997

Figure 3.5: Mission Temperature Profile table that is provided as an example in an Application Report of Texas Instruments [13].

The Mission Temperature Profile is a division of the operation time in temperature ranges and the related amount of time as percentage that is related to a specific temperature. An example is depicted in Figure 3.5. The amount of time and the ambient temperature is specified from an expert and represents an expert judgment. The De-Rated FIT Rate is calculated with Equation (3.1) from the last Sub-Section. The total FIT Rate at the specific Mission Temperature Profile can be calculated by summing up the individual rates that are a multiplication between the De-Rated FIT Rate and the amount of time at that specific temperature range [10, 51, 12].

One problem that occurs with this model is about dealing with the power-on and power-off times of the system. In general, this consideration should be specified inside the employed industry standard such as the IEC TR 62380 [51, 12].

3.2.4 Base Failure Rate Calculation

The FIT Rate that was introduced before represents the final value that is mostly provided in the component related datasheet. This value is mostly calculated using the industrial

reliability standard IEC TR 62380 that is also used inside Part 11 of the ISO 26262 standard. First of all, the standard is differentiating between ASIC and FPGA implementations. The reason for these two groups is based on the fact that inside an FPGA there are already all transistors and complementary circuits placed and based on the logical HDL that is synthesized a specific amount of gates are used to represent this logic. For ASICs this approach is not feasible and the engineers have to calculate everything on their own, starting with the amount of transistors, used semiconductor materials and their used process [10, 51, 12].

FPGA FIT-Rate Estimation

Figure 3.6 depicts a table from the ISO 26262 standard of an FPGA with the related resources that are provided by the platform. In this example, the FPGA provides about 1000 logical blocks, a user memory of 16 Kilobyte and also fixed functions that are integrated as IP cores that provide additional co-processors such as microcontrollers. All these resources could be used after synthesis [10, 12].

Element	Resources	Assumed IEC 62380 category
Logic blocks	1000	CPLD (EPLD, MAX, FLEX, FPGA, etc.)
User memory	16 kb	Low-consumption SRAM
Fixed function IP	20 k gates	Digital circuits, microcontroller, DSP
Configuration technology	10 kb	Low-consumption SRAM
NOTE For the Logic blocks, the CPLD entry of IEC TR 62380 has been used as example. For modern volatile FPGA devices, the LCA (RAM based) entry can be preferable.		

Figure 3.6: FPGA overview of the resources that are provided by this specific platform [10].

Element	λ_1	N	α	λ_2	Base FIT	De-rating for temp	Effective FIT
Logic blocks	$2{,}0 \times 10^{-5}$	100000 (100 transistors per macrocell)	10	34	34,0604	0,17	5,7903
User memory	$1{,}7 \times 10^{-7}$	98304 (6 transistors/bit for a low-consumption SRAM)	10	8,8	8,8005	0,17	1,4961
Fixed function IP	$3{,}4 \times 10^{-6}$	80000 (4 transistors / gate)	10	1,7	1,7082	0,17	0,2904
Configuration technology (based	$1{,}7 \times 10^{-7}$	61440 (6 transistors/bit for a	10	8,8	8,8003	0,17	1,4961

Figure 3.7: Calculating the FIT Rate for an FPGA [10].

The elements that are provided by the FPGA are integrated as analog components such as transistors and must be considered as physical representation. Figure 3.6 shows the internal representation of the FPGA elements. The Logical blocks are internally rep-

Element	Resource usage	Effective FIT
Logic blocks	23 %	1,3318
User memory	10 %	0,1496
Fixed function IP	100 %	0,2904
Configuration technology (based on SRAM)	15 %	0,2244
Sum		1,9962

Figure 3.8: Summarizing the used resources and the related effective FIT Rate of the FPGA example [10].

resented as 100 transistors per macrocell on the physical level and therefore an amount of 100000 transistors. The Base FIT Rate is derived from two λ values that represent different transistor types such as Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET) and the degree of coping with the specific technology. The α value represents the time difference from the actual year to the year 1998 [10, 51, 12].

In the last step of the FPGA calculation the process is reducing the FIT Rate to the amount of resources that are really used by the provided function. In the example of Figure 3.8 it can be seen that from the 100 logical blocks there are just 23% used and therefore the effective FIT Rate is reduced to this specific amount. The reason for this approach is that if there is an Fault inside one of the non-used Logical blocks than this does not represent a safety issue because these blocks are not used for safety-critical computation or signal processing. This approach will be applied to all elements and the used resources [10, 51, 12].

ASIC FIT-Rate Estimation

In comparison to the FPGA, the ASIC example is reduced to the steps in which the FIT Rate of the physical representation is calculated. In Figure 3.9 the whole calculation formula is shown. As already stated in the previous subsection is the FIT Rate defined by the amount of elements that can be represented by transistors or resistors and the specific technological values λ and α [10, 51, 12].

$$\lambda_{die} = \left\{ \sum_{elements} \left(\lambda_{1,element} \times N_{element} \right) \times e^{-0{,}35 \times \alpha} + \max(\lambda_{2,element}) \right\} \times \sum_{elements} \left\{ \left\{ \frac{\sum_{i=1}^{y} \left(\pi_{t,element} \right)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right\} \times \frac{N_{element}}{N_{total}} \right\}$$

Figure 3.9: Calculating the FIT Rate of an ASIC [10].

3.3 General Reliability Assessment for Electronic Devices

Component Reliability basics were already described in the Background Section of this Thesis. This Subsection describes a general overview of the Industrial approaches, the challenges and the limitations of these current approaches. In general, reliability is one of the most important factors for complex systems. The beginning of reliability engineering started in the 1940s with Wernher von Braun and the improvement of the V-1 rocket. Von Braun created the first documentation about predictive reliability modeling. The first publically available handbook was the Military Handbook 217 which was published in 1965 [52]. The handbook is outdated and several publications declare that its reliability methodologies should not be used anymore [52, 53, 14]. Due to wrong outcomes as well as the U.S. Army stating that the approaches are unreliable and lead to wrong reliability predictions [52]. For that reason, several new standards were written to advance the basic MIL-HDBK-217 standard and to improve these shortcomings.

Procedural method	Last updated year	Country of origin	Status
MIL-HDBK-217	1995	USA	Active
GJB/Z 299	2006	China	Active
Telcordia SR-332	2016	USA	Active
PRISM	2000	USA	Active
RDF-2000	2000	France	Active
217Plus	2015	USA	Active
FIDES	2009	France	Active
Siemens SN29500	2013	Germany	Active
NTT Procedure	1985	Japan	Canceled
British Telecom HRD-5	1994	UK	Canceled

Figure 3.10: Reliability Handbooks that are mostly based on the MIL-HDBK-217 [14].

Pandian et al. [14] state in their publication that most of these novel handbooks, as seen in Figure 3.10, are based on the MIL-HDBK-217 and that they have similar shortcomings than the original handbook. In 2018, most of them were still used by the Industry. The common basis of all these standards is the calculation of the component failure rate using failure models created with field data and statistical models [14].

3.3.1 The Mythos of Failure Models

Pandian et al. describe that the reliability estimation of the handbooks can be mathematically described in the following function form [14]:

$$F(t) = f(T)f(P)f(V)f(Q)f(E) \tag{3.2}$$

Equation 3.2 is calculating the Failure Rate using Temperature, Power Dissipation, Voltage, Quality and Environmental Conditions. Pandian et al. emphasize that the handbook is using a linear correlation between all input parameters, which is simply wrong. Furthermore the handbooks does not consider the variation of each factor such as temperature cycles [14].

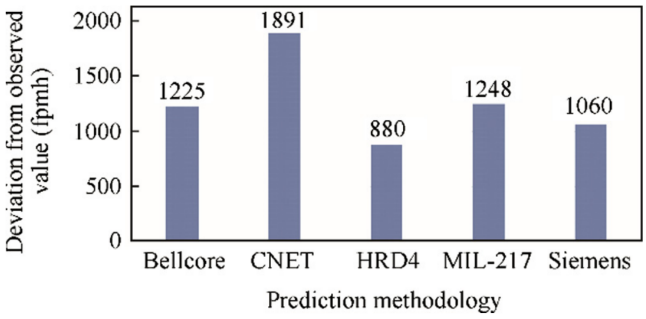

Figure 3.11: Prediction Deviations from different Reliability Handbooks and real field data [14].

In the 1950s, engineers started to use exponential models for their failure calculations. These models simplified the mean time between failure calculation which lead to a quick spread of these methodologies into the reliability community. Pandian et al. describe that the community shared reliability models of specific components such as capacitors and resistors and that they are still widely used without considering that these models are based on specific manufacturer components and can not be generalized for other components. Therefore, Pandian et al. emphasize that each manufacturer should create their own reliability models with real data [14].

Figure 3.11 gives an overview of the deviation between real failure data from the field and the predicted data. It can be seen that all standards have under-estimated the failure rate and that the components have lasted longer than expected [14].

3.3.2 The Holy Grail of Temperature Factors

Pandian et al. describe that in the reliability handbooks the influence of the temperature is always expressed with the Arrhenius Equation [14]. The Arrhenius Equation is also used in the Automotive Industry e.g. within ISO 26262, already described in Section 3.2.

$$\text{Siemens} \quad \Pi_T = A \exp\left[11.605 E_{a,1}\left(\frac{1}{T_{j,1}} - \frac{1}{T_{j,2}}\right)\right] + (1 - A)\exp\left[11.605 E_{a,2}\left(\frac{1}{T_{j,1}} - \frac{1}{T_{j,2}}\right)\right]$$

$$\text{SAE PREL} \quad \Pi_T = \exp\left[-A\left(\frac{1}{T_j + 273} - \frac{1}{287}\right)\right]$$

$$\text{Telcordia GR332} \quad \Pi_T = \exp\left[-\frac{E_A}{R}\left(\frac{1}{313} - \frac{1}{T_j + 273}\right)\right]$$

Figure 3.12: Different forms of the Arrhenius Equation used in different reliability handbooks [14].

Figure 3.12 shows differences between Arrhenius Equations from different reliability handbooks. Pandian et al. emphasize, because the exponential form of the equations lead to a high sensitivity to the Activation Energy E_a. They describe that even a small deviations of the energy value such as 0.05 can result in higher Acceleration Factors such as a multplication of 5 of the original value.

Therefore different reliability handbooks can result in completely different temperature factors due to small deviations in the assumed Activation Energy as seen in Figure 3.13 [14].

Failure mechanism	Activation energy
Metal corrosion 4	0.3–0.6 eV 0.77–0.81 eV 0.9 eV 0.6–0.7 eV
Metallization migration	1 eV 2.3 eV
Ionic contamination (surface, bulk)	0.6–1.4 eV 1.4 eV
Gate-oxide breakdown	0.3–0.4 eV 0.3 eV
ESD	0.3 eV 2.1 eV
TDDB	0.3–1.0 eV 2 eV
Surface-charge spreading	1.0 eV 0.5–1.0 eV
Au-A1 intermetallic growth at wire bonding	0.5 eV 1.0 eV 1.1 eV 2.0 eV

Figure 3.13: Deviations of the Activation Energy based on the failure mechanism [14].

3.3.3 Alternatives To Handbook Based Reliability Estimations

Pandian et al. describe that since the 1980s the MIL-HDBK 217 was called into question doubting its usability and accuracy. Therefore, the Industry in Europe started to develop alternatives with the ability to consider the complexity of novel electronic designs as well as the manufacturing technology. These new approaches should be able to provide real reliability data for each vendor-specific designs and technology [14]. Pandian et al. describe five different alternatives to the Handbook based reliability estimations [14]:

1. **Physics of Failure Model Based Prediction**
   The Semiconductor Industry is continuously improving their manufacturing processes and is shrinking the analog semiconductor manufacturing processes. Breaking the 100nm technology will introduce novel failures which are not design related but physical based such as utilization. High utilization causes mechanical and electrical stress as well as thermal effects and chemical interactions. To analyze these failures and to allow for predictions about future advanced technologies, the Industry uses the Physics of Failure Model Based Prediction [14]. There are several publications in the field of the Electrical Engineering domain related to this approach [54, 55, 56, 57, 58]. But also in the Mechanical Engineering domain [59, 60, 61]. The Physics of Failure Model Based Prediction is focusing on the Electrical Engineering domain in detail, the mechanical stress of the components such as bonding wires and interconnections of electronic modules.

2. **Data-Driven Prognostics**
   Data-Driven Prognostics one monitors the health of a specific system and derives the Remaining Useful Lifetime. This approach is calculating the degradation of the system with evaluating deviations of the designed state of the system [14].

3. **Similarity Analysis-Based Prediction**
   The Similarity Analysis-Based Prediction is analyzing the performance of a system by comparing it to its digital twin. The idea is to detect certain patterns in the data. The digital twin is analyzed with specific Computational Intelligence technologies such as Machine Learning (Supervised and Unsupervised Learning), Deep Learning or Neural Networks [14]. The usage of Similarity Analysis-Based Prediction is mostly used in the Information Technology domain on higher Abstraction Layers such as the Application Layer [62, 63, 64]. But there are also holistic approaches such as predicting the reliability of a lithography machine [65]. Yang et al. describe that one of the biggest problems related to this field is the need of large data sets from the specific machine which often is not possible. Especially for novel machines [65].

4. **Field Data-Based Prediction**
   The Field Data-Based Prediction method is using data from systems that are already in service and therefore represents the real performance of the system in the specific operational environment under the real conditions. This approach enables the reliability estimation of systems that are already in service [14].

5. **Test Data-Based Prediction**
   The Test Data-Based Prediction is similar to the Field Data-Based Prediction with the difference that the systems are running inside a test environment. Based on the results of failed and still working systems the reliability can be measured. One big concern is sugarcoating of the real environmental conditions to enhance the reliability data [14]. Nowadays Test Data-Based Prediction is one of the most common approaches for evaluating the reliability of novel systems. Also the ISO 26262 suggests the Chi-squared test for reliability estimations [10] and there is the Automotive Electronics Council as a Technical Committee which started to define qualification requirements in the 1990s [15]. Also other domains widely employ the Test Data-Based Prediction method [66, 67, 68, 69].

For this thesis, the Data-Driven Prognostics and Field Data-Based Prediction are the most important approaches for advancing the current reliability estimations in the Automotive Industry. Therefore, the following Subsections will provide more information regarding these approaches.

Data-Driven Prognostics

Data-Driven Prognostics can be an alternative to Handbook based reliability estimations. Pandian et al. describe that Prognostics and Health Management is monitoring the actual health of the product and is estimating the residual lifetime, also called the Remaining Useful Life. In this approach, the product is evaluated with an ideal state of the product and the real usage of this product. This methodology is using real operation conditions, the load on the system and aging symptoms that are related to expect damages. Using the Prognostics and Health Management approach Pandian et al. emphasize that it offers numerous advantages like [14]:

- Premature Failure Warnings
- Minimized Unscheduled Maintenance
- Longer Intervals between Maintenance Cycles
- Improved System Availability

- Reduction in Life Cycle Costs by minimizing Downtime and Inspection Costs
- Improved Qualification and Assisting in the Design and Logistical Support of Fielded and Future Systems

The actual health of the specific system is evaluated using different real-time monitored indicators such as the voltage of the device. Based on this idea several monitors have been developed to evaluate the state-of-health of a system in real-time. The health of a system is evaluated by the monitor with checking specific components inside the system such as the resistance or voltage of the device [14]. Pandian et al. listed the following prognostic possibilities [14]:

- **Fuses and Canaries**
  Are used to sense damage to the system preventing further failures which are caused by these preliminary faults.
- **Monitoring Failure Precursors**
  Specific system indicators are monitored continuously in real-time and any deviation will be evaluated with possible system failures or degradations.
- **Monitoring Environmental and Usage Profiles**
  Data of these Usage Profiles is used to generate a digital twin of the system and to evaluate possible down-times or degradation of the system caused by faults.

Pandian et al. describe that the previous prognostic possibilities are widely used in the Industry for evaluating the Remaining Useful Lifetime such as predicting failures in the Lithium Ion Batteries inside the Boeing 787. Pandian et al. [14] also describes approaches with Bayesian based covariant identification [70], Auto-Regressive models [71] and Gaussian Process Regression [72].

Field Data-Based Prediction

Field Data-Based Prediction is related to collecting data from real systems in the field to estimate the reliability of the system under real environmental and operational conditions. This allows for the observation of systems already in service [14]. This approach requires the following data to work correctly [14]:

- Initial Operation Time
- Life Cycle History and Operating Profile
- Failure Time

Pandian et al. describe that the collection process of the data is the most crucial part, because it requires manual or automatic collection. Though most of the products already have many built-in sensors, which could be used to collect this data. This information is collected and stored in databases. Based on these databases specific statistics can be derived such as failure reportings, operating profile and the operational environmental conditions [14].

3.3.4 High-Temperature Operating Life

In 2014, the Automotive Electronics Council (AEC) released their novel AEC-Q100 standard called Failure Mechanism Based Stress Test Qualification for Integrated Circuits. The standard is divided in 12 parts [15]:

- AEC-Q100-001: Wire Bond Shear Test
- AEC-Q100-002: Human Body Model Electrostatic Discharge Test
- AEC-Q100-003: Machine Model Electrostatic Discharge Test
- AEC-Q100-004: IC Latch-Up Test
- AEC-Q100-005: Non-Volatile Memory Program/Erase Endurance, Data Retention, and Operational Life Test
- AEC-Q100-006: Electro-Thermally Induced Parasitic Gate Leakage Test
- AEC-Q100-007: Fault Simulation and Test Grading
- AEC-Q100-008: Early Life Failure Rate
- AEC-Q100-009: Electrical Distribution Assessment
- AEC-Q100-010: Solder Ball Shear Test
- AEC-Q100-011: Charged Device Model Electrostatic Discharge Test
- AEC-Q100-012: Short Circuit Reliability Characterization of Smart Power Devices for 12V Systems

Most of these are related to the Physics of Failure Based Prediction methods such as the Wire Bond Shear Test, Electrostatic Discharge Tests, IC Latch-Up Test and Solder Ball Shear Test. But there is also a Test Data-Based Prediction Method such as the Non-Volatile Memory Program/Erase Endurance, Data Retention, and Operational Life Test which is using the High-Temperature Operating Life (HTOL) approach.

High-Temperature Operating Life is used as a reliability testing method for Integrated Circuit (IC). This test method is operating the IC on higher temperature conditions to evaluate the impact of the stress on the specific device [15]. This testing method is also widely used in the manufacturing process to pick out early failing devices as seen in the Bathtub curve in the first section as described in Section 2.5.1.

	Temp [°C]	Use Time [h]	Eq. time @ 150°C	Eq. time @ 175°C
Operation	150	100	100.0	39.9
Operation	120	900	256.2	102.2
Operation	110	5000	896.1	357.6
Operation	90	6000	394.9	157.6
	Total Op:	12000	1647	657
Non-op	90	1000	65.8	26.3
Non-op	40	118400	287.0	114.5
	Total Non-Op:	119400	353	141
	Total [h]:	**131400**	**2000**	**798**

Figure 3.14: High Temperature Storage Life Equivalent Bake Time [15].

The HTOL approach is trying to age the semiconductor device under specific conditions to simulate the operation time at specific temperature conditions. For this purpose, the operational temperature will be increased to a specific point to stress the device which is assumed to be equivalent to a specific amount of time at a common operational temperature. The main idea is to shorten the testing time from several thousand hours to a few hundreds. Figure 3.14 describes an example of the AEC Q100 standard, which is calculating the equivalent "baking" time of a device with a specific Mission Temperature Profile. The statistical Use Time would be 131400 hours under normal operational conditions and with the HTOL approach the testing time could be reduced to 798 hours by heating up the device for example to a operation temperature of 110°C degrees up to 175°C. This reduces the testing time from 5000 hours to 357.6 hours [15]. The test requires the selection of several samples to achieve statistical confidence [10].

3.3.5 Blind Spot Analysis Reliability Estimation

This Subchapter described the general Reliability Estimation of Electronic Products, which are used in different Industries such as Consumer Electronics. The base for all different domains is the usage of the Reliability Handbooks. The main Reliability Handbook is represented by the Military Handbook 217 that was first published in 1965. As already described there are many publications which are declaring that this handbook should not be used anymore caused by the fact that many relations are not physically correct such as the linear coherence of the different physical effects such as temperature, voltage and others. But there are still many handbooks available that are a derived version from this first handbook such as the 217Plus Handbook that was last updated in 2015 as well as the ISO 26262 standard that was revised in 2018 and are still using concepts from the base Handbook. This raises the question why so many standards reference this root handbook and still use its methodologies. Because there are already alternative methods that can be used such as the Data-Driven Prognostics, Field Data-Based Prediction and Test Data-Based Prediction. Lets analyze all of them from the view of the Automotive Industry.

The usage of Data-Driven Prognostics is not really applicable for calculating the foreseeable operation time of a specific system. Based on the fact that the Data-Driven Prognostics roots in the detection of misalignment between the designed operational specifications and the real specifications. To detect overheat conditions the Industry is using Canaries. But the Canaries can be seen as Sensors that trigger a specific strategy, such as adapting the Frequency of a system to counteract on the higher temperature. Therefore, these monitors can be used as detection sensors that can trigger a system degradation to enable fail-operational behavior instead of running into a total failure of a system.

The second approach is the Field Data-Based Prediction that is collecting real data from system in the field to estimate reliability of the real operational conditions. In my opinion this is the key to improve the statistical reliability data of the OEM as well as from Tier-1 and Tier-2 suppliers. The reason is that the Design is always an estimation, which can be wrong or can be sugarcoated. The strategy of determining the reliability is always connected to the Mission Temperature Profile. The Mission Temperature Profile is a strong parameter to reduce cost caused by the fact that higher Mission Temperature Profiles demands higher quality materials. In a highly competitive industry such as the Automotive Industry this option could be used to stay ahead of other competitors. In the end, the consumer has to settle this bill caused by lower quality materials that will fail sooner than expected. The real border will always be the statutory requirements of the guarantees. The compulsory collection of real Field Data such as Temperature Profiles will force the Automotive Industry to design their systems on real Mission Temperature

Profiles, which will optimize the systems on the real operational occurrences. The ISO 26262 standard is criticizing their own industrial approach by stating in its own document that there is a lack of real Field Data. Therefore more approaches should use real Field Data. Instead of real Field Data the standard is referencing the evaluation with Test Data-Based Prediction methods. The Test Data-Based Prediction Methods are defining test cases in which the Components, Systems and Items are tested such as in the AEC Q-100 standard. This standard is providing approaches which can be used to perform HTOL test cases in which systems are running at higher operational temperature conditions to simulate longer durations at lower temperatures. The ground base of this approach is the Arrhenius Equation that is widely used in all different Industrial domains for calculating the Acceleration or Derating Factor of systems that are operating at higher temperatures. The Arrhenius Equation mathematically describes the relationship between the MTBF and the temperature as an exponential relation. The physical background is well known and accepted but there are also differences of opinion as already described in the Sub-Section about the "Holy Grail of Temperature Factors". One of the biggest problem is the Activation Energy factor. If there are small changes in the Activation Energy than the result of the Arrhenius Equation can be significantly higher or lower. Therefore, this Activation Energy could be used to sugarcoat the reliability estimation with the goal of minimizing cost. Therefore Test Data-Based Prediction methods that are using the Arrhenius Equation to calculate specific run-times to evaluate reliability of their components are not objective enough for an independent analysis.

As a result of the reliability analysis of different methodologies it can be seen that Test Data-Based Prediction can not be sufficient for evaluating reliability of safety-critical Automotive Systems. One of the biggest concerns is the usage of optimistic input data to provide reliability verification of specific design decisions. Even if most of the Industry is using real or pessimistic data, it could be the case that newcomer companies are abusing this industry standard approaches to lower the cost of their products. Especially in the field of Fully-Automated Driving systems there are many new competitors that are already widely known from the Software Industry such as Google that are trying to achieve high market shares in this new market. This could lead to economical conflicts that have a negative impact on the customer. Especially from a safety point of view, e.g. the rollout of Teslas Summon function that was far from a reliable fully-automated function. Backed by the fact that there are several videos available that clearly show damage on the car and surrounding facilities [73]. This case clearly shows the hard fight in this domain to gain market share and to become the industry leader. In this specific case, the missing safety was easy to spot for a customer and customers had the possibility to pass on this convenience function. But regarding the reliability of specific semiconductor devices, customers are not able to make any decisions at all. Therefore higher standards are

needed to force newcomers in evaluating the reliability of their system on real operational conditions such as with the Field Data-Based Prediction methods.

Lastly one problem that still exists is the identification of the base Failure Rate because before the Industry can draw from real Field data it requires a first estimated Failure Rate. So this is a chicken-and-egg problem and thus hard to overcome the critical Handbook methods of deriving reliability data. But the consensus of the Industry is that the Arrhenius Equation and the Handbook based reliability estimations can provide a specific Failure Rate which could prove wrong. But what does it mean for this value to be wrong? If we think of this value as an exact value such as a MTBF time of 100 hours, in which the system will statistically fail at the exact point of 100 hours than yes this value is wrong. This value must be regarded as a statistical value with a specific deviation. Lets assume that the deviation is about 50 hours. Than we could statistically evaluate if all test samples will work as expected at least for 50 hours. This is good enough for a first shot, but the Industry should not stop here and advance their methods by using a second methodology such as the Field Data-Based Prediction method. Because the Field Data-Based Prediction method could be used to detect deviations from the designed Mission Temperature Profile. It can be seen that one of the most crucial input parameter of the whole reliability estimations is the Mission Temperature Profile. Therefore to advance the current methodologies and to provide highly safe systems future Fully-Automated Automotive Systems should be advanced with:

1. Conservative Handbook Based Reliability Estimations for a first Failure Rate
2. Test Data-Based Prediction Methods to Evaluate the Failure Rate
3. Dynamic Adaption of the Failure Rate with real Field Data

The first two requirements are already fulfilled by the ISO 26262 standard. The last is one of the most complicated issues, due to the Industry having to collect this data from the whole fleet already in service. Over the last few years collection of this data was not possible in a practical manner caused by the lack of vehicle connectivity. But this limitation will be gone in the next few years with the upcoming Vehicle-To-Infrastructure connections that will enable a permanent communication between the vehicle and the OEM. This will also enable the collection of real-time operational condition data such as temperature and can be used as a feedback loop for the Handbook Based Reliability estimations regarding Mission Temperature Profiles. But we have to introduce this Field Data-Based methodologies in several steps to avoid impairment of the industry. Therefore, I suggest to start with the collection of Field data that can be easily integrated in the current Automotive products and thus mainly by sampling the temperature data. The reason for collecting the temperatures is because almost all Automotive semiconductor

devices already are equipped with a temperature sensor. This would allow us to easily integrate a Field-Data Based monitoring system with the following requirements:

- Continuously calculate the current utilization with the Failure In Time Rate as the main indicator
- Usage of the integrated temperature sensors of the Automotive semiconductor devices
- Dynamic Adaption of the Failure In Time Rate to detect Safety Anomalies regarding ASIL Level
- Semiconductor area optimized approach

To fulfill these requirements, the next subchapter gives an excerpt of State-of-the-Art Live State-of-Health monitors regarding aging detection for hardware systems.

3.4 Live State-of-Health Monitor for Electronic Components

3.4.1 General Overview

The detection of stressed Electronic components is very difficult in comparison to the classical mechanic domain. Mechanical parts that are highly stressed are changing their structure and this leads to visible characteristics such as fissures but also changes the audible frequency range of the component and this allows observation of differences. The electrical domain instead is working flawlessly up to a certain point at which the whole component fails and all of a sudden the functionality is not provided anymore [74]. This circumstance has been handled by using the driver as a last backup distance in case of failures [10]. Over the next few decades automated driving vehicles will fully control all possible driving situations and this leads to the requirement that any fault must be detected apriori to prevent failures during operation that could lead to deadly accidents.

The detection of stressed electronic components and related failures is an important research topic that can be seen by the numerous publication in this specific field [16, 75, 76, 77, 78, 79, 80, 17, 81, 18, 82, 83, 84, 19]. Most of the publications are using a temperature sensor for detecting aging and reliability losses. This is directly related to the Arrhenius Equation that was introduced in Section 2.5.2.

In the next few subsections the most important aging monitors are described with respect to this thesis.

3.4.2 An FPGA-based monitoring system for reliability analysis (Saab Group)

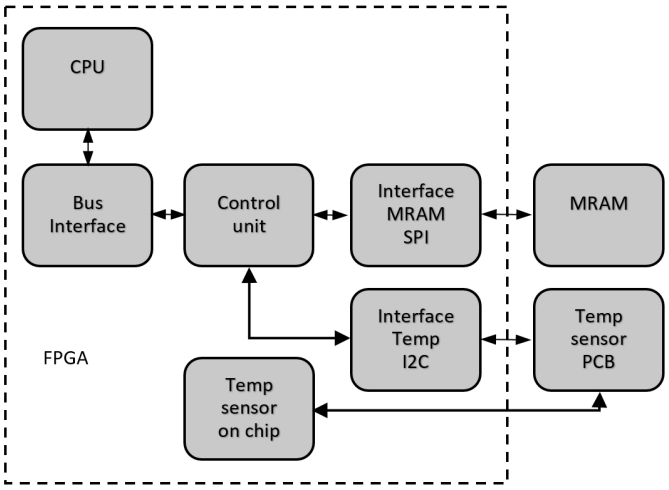

Figure 3.15: Block diagram that gives on overview of the aging monitor system of Johansson et al. [16].

Johansson et al. [16] describe an FPGA-based monitoring system for reliability analysis in their publication. Their system consists of a temperature monitor that is implemented in VHDL and uses several temperature sensors together with non-volatile memory for storing these values for long-term evaluation. Figure 3.15 depicts the aging monitor as block diagram. The main part of the system is implementing the temperature measurement as a Finite State Machine (FSM) and is permanently saving these samples inside an external Magneto Resistive Random Access Memory (MRAM). Their current system is using standard communication protocols to allow a fast adaptation to other systems [16].

In their test run, Johansson et al. simulated a steep temperature change between 20°C and 93°C and the monitor measured the current temperature with a interval rate of 15 seconds. During their test run they detected that applying this thermal stress profile would result in a shortening of the component lifetime from 6.4 years to 1.9 years [16].

The FPGA-based monitoring system can be used as a continuous logger of temperatures during the whole operation time. Johansson et al. emphasizes the big advantage of using these data in external reliability tools for estimating the remaining useful lifetime [16].

3.4.3 Mission Profile Recorder: An Aging Monitor For Hard Events (STMicroelectronics)

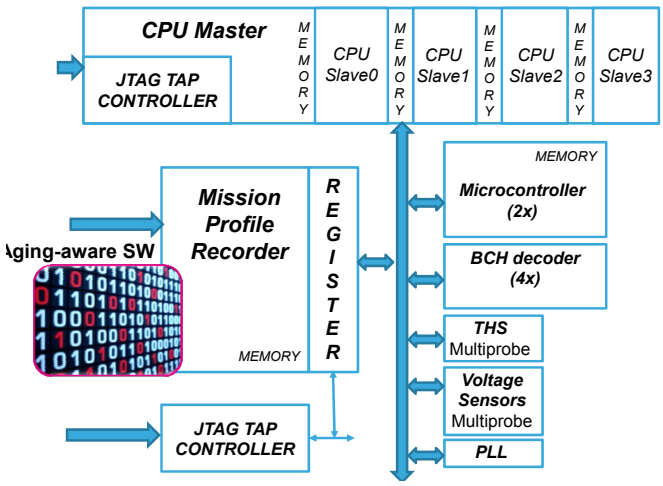

Figure 3.16: System Architecture of the Mission Profile Recorder [17].

Mhira et al. [17] introduced a novel demonstrator for recording mission profiles to cope with degradation due to oxide breakdown and electromigration. Their main goal was to support the design process for hardening their products by using real workloads [17].

Figure 3.16 gives an overview of the system architecture of the Mission Profile Recorder.

The monitor is working by recording the usage of the chip and computing the remaining lifetime. For this purpose, the monitor is measuring the elapsed time of the executed instruction, current voltage, and the related thermal junction temperature. An algorithm is calculating the remaining time by using these three input parameters. Mhira et al. implemented their prototype on a 40nm testchip and evaluated the feasibility of their approach [17].

3.4.4 Reliability and Field Aging Time Using Temperature Sensors (Cisco)

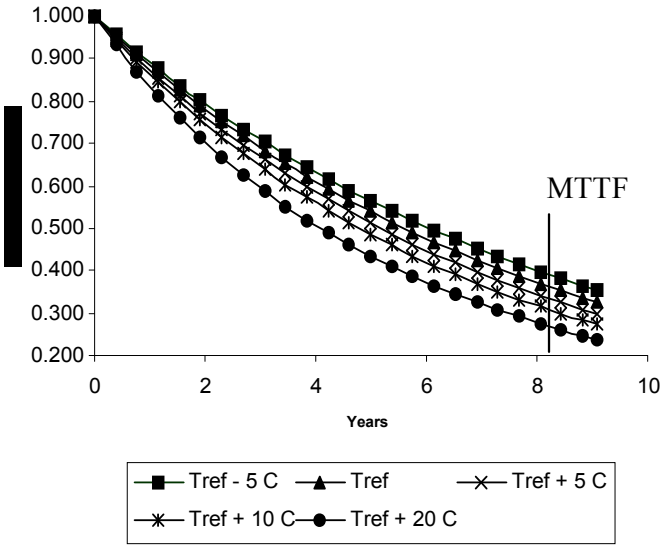

Figure 3.17: Experimental results of Civilini describing the reliability deviations in comparison to different temperatures [18].

Civilini [18] describes in his publication a novel approach to make a transition from statistical reliability evaluation to a real endpoint-specific definition. Figure 3.17 clearly shows that higher temperatures directly influence the MTBF. The main work represented in this paper is mathematical formulas about their approach. The main idea is to use the existing temperature sensors which are already placed inside their critical infrastructure hardware [18].

3.4.5 Wear-out stress monitor utilizing temperature and voltage sensitive ring oscillators (Renesas Electronics Corporation)

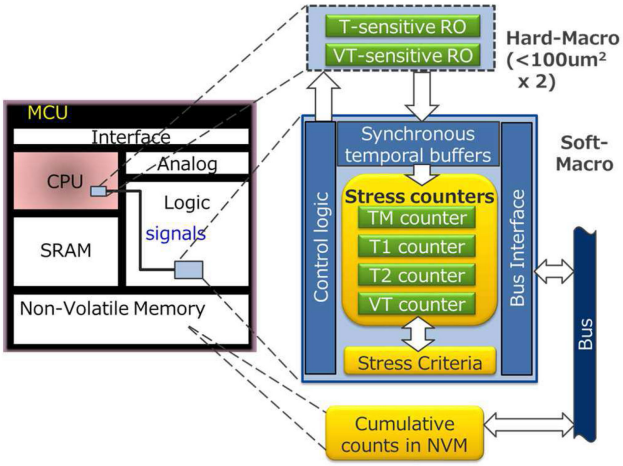

Figure 3.18: System architecture of the wear-out stress monitor [19].

Takeuchi et al. [19] implemented an on-chip wear-out monitor that is considering the environmental conditions of the digital chip as seen in Figure 3.18. Their main focus was on emulating real stress with different ring oscillators with the goal of hardening automotive microcontrollers on reliability. The monitor is working with four counters that are increased with every triggered stress incident. The main controller is totally independent and therefore is not interrupting the operations on the CPU. Takeuchi et al. implemented their novel monitor on a 28nm testchip to evaluate feasibility [19].

3.5 1D MEMS Micro-Scanning LiDAR

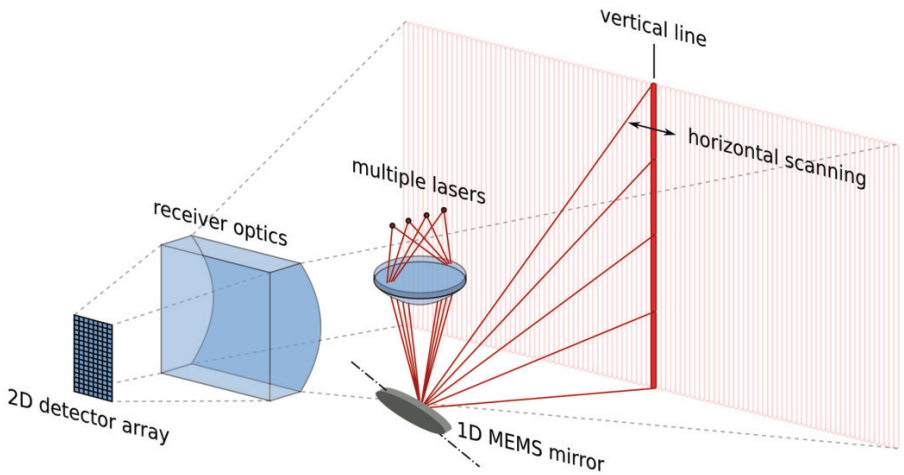

Figure 3.19: Conceptual illustration of the 1D MEMS Micro-Scanning LiDAR platform [3].

In the Background Section the concept of the LiDAR technology has already been introduced and is depicted in Figure 3.19. The main idea behind LiDAR is to sense the front area of the sensor by using a laser that emits an optical signal into the scenery, reflected by obstacles and as a last step received by a 2D detector array. The Point Cloud of the scenery can be derived from these signals. This is achieved by processing the time differences between the signal that was sent and the signal that was received. The time directly depends on the overall distance of the platform and the object inside the scene [3].

3.5.1 Requirements

Druml et al. [3] introduced a novel concept of the LiDAR technology called the 1D MEMS Micro-Scanning LiDAR system. This technology has its specific focus on providing a robust and safe LiDAR system that is also automotive certified. One of the most challenging things about the LiDAR technology are the high cost caused by the complexity of these systems. The novel approach of Druml et al. emphasizes highly integrated components such as the mechanical parts that are integrated as Micro-Electro-Mechanical Systems. Druml et al. describes that the main requirements on a long-range LiDAR sensor are from Original Equipment Manufacturer (OEM) perspective [3]:

- 120° horizontal field-of-view and 16° vertical field-of-view
- 20cm distance resolution, 0.1° horizontal and 0.5° vertical resolution
- 200m measurement range

- 20 frames per second of field-of-view's point cloud
- 200$ system costs
- ASIL-C and laser class 1 guaranteeing functional-, eye-, and skin-safety
- High robustness against shocks and vibrations

3.5.2 System Architecture

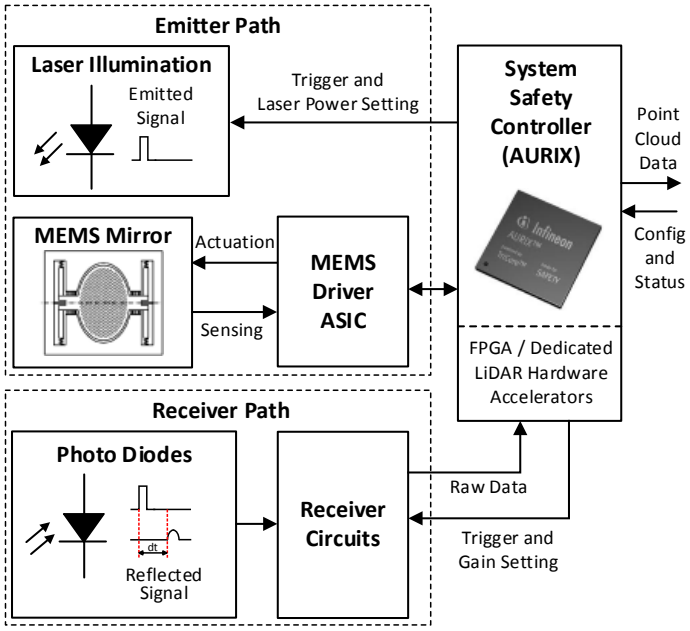

Figure 3.20: System architecture of Druml et al. 1D MEMS Micro-Scanning LiDAR platform [3].

Figure 3.20 gives an overview of the 1D MEMS Micro-Scanning LiDAR platform on system level. The system consists of three main parts [3]:

- **Emitter Path**
  The Emitter Path is responsible to emit the Laser signal and all related control systems. This path gets configured and triggered by the system Safety Controller and the Laser Illumination is actively sending out the Laser signal. For controlling the laser in the horizontal direction the MEMS mirror is responsible. The mirror is actuated by the MEMS Driver ASIC and also receives control signals from the MEMS mirror. These signals are evaluated and any faults will be reported to the System Safety Controller [3].

- **Receiver Path**
  The Receiver Path consists of an array of Photo Diodes that are receiving the optically reflected laser signal. The Receiver Circuits are sending these raw data signals to specific FPGA implemented LiDAR hardware accelerators [3].

- **System Safety Controller**
  The System Safety Controller is responsible for controlling and monitoring the Emitter and Receiver Path. Additionally this controller is also receiving the raw data from the Receiver Path, processing this data to Point Cloud Data and sending them to other items [3].

3.5.3 MEMS Mirror

Figure 3.21: MEMS mirror of the 1D MEMS Micro-Scanning LiDAR platform [3].

The MEMS Mirror is an essential part of the whole LiDAR system because it enables the possibility of moving the laser in a horizontal line. Figure 3.21 depicts the mirror inside a case that is hermetically sealed with the pins on the bottom side which are necessary to control and sense the structure. The mirror is moved by an electrostatic comb and is oscillating with a high Q factor. The oscillation is driven through application of 100V to the electrostatic comb that is moving the rotor to the zero position by the electrostatic force [3].

Non-linear Harmonic Oscillator

The MEMS Mirror of the LiDAR system shows a mechanical behavior of a non-linear harmonic oscillator that can be depicted in Figure 3.22. When the mirror starts moving

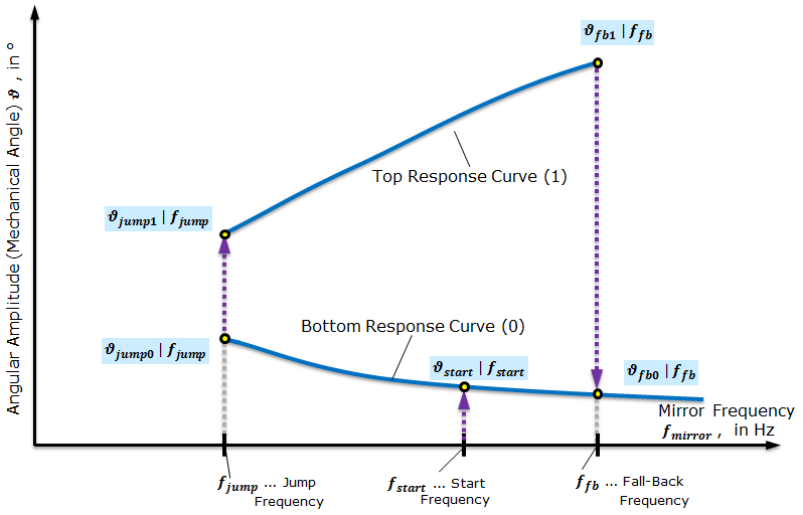

Figure 3.22: The response curve of the LiDAR system that's representing a non-linear harmonic oscillator [3].

due to the electrostatic force then the mirror starts with the frequency f_{start}. This operational point can be moved upwards and downwards along the curve by changing the actuation frequency of the voltage. If we lower the actuation frequency until f_{jump} then the operation point is moving from the Bottom Response Curve to the Top Response Curve. The normal operation must be on the Top Response Curve. because in this scenario the actuation voltage follows the mirror and its zero crossing and with increasing frequency the mirror's deviation angle also increases [3].

3.5.4 Prototype Platform

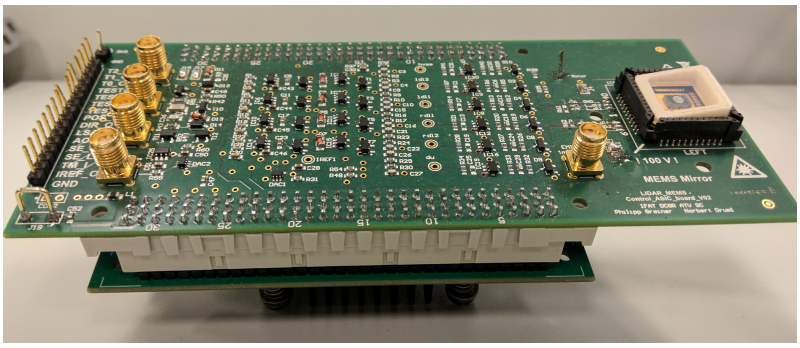

Figure 3.23: 1D MEMS Micro-Scanning LiDAR prototype platform.

The prototype platform that was provided by our project partner is shown in Figure 3.23. The platform consists of an analog circuit board that contains the measurement circuits and actuation circuits for the MEMS Mirror as well as the mirror itself. The

control system is implemented on a ZYNQ 7000 platform that consists of an Artix-7 FPGA and a dual-core ARM Cortex-A9 processor.

3.6 Handling the Complexity of Automated Driving

This Section describes the handling of complexity related to Automated Driving. Automated Driving spans several ranges of subjects from the technological aspects to the social aspects [85]. In general, there is already a well advanced awareness that the transition from semi-automated to fully-automated driving requires a rethinking of the current safety standards and processes [86, 24, 87, 23, 22, 21, 20, 85, 88, 89, 90, 91, 92, 93, 94, 95].

3.6.1 Safety Issues Caused By Automated Driving

Noy et al. [85] published a paper about the current safety blind spots of Automated Driving. In their work, they emphasized the sociotechnical complexity of Automated Driving. One of the biggest falsities is the pursuit of automated driving to decrease car accidents due to the fact that most of them are caused by human errors. But Noy et al. described that most car accidents are based on vehicle controls with not valid assumptions even if these assumptions are based on the traffic system rules. They mention the accident of the autonomous Google car in 2016 in which the car was making the assumption that the other driver will slow down on the lane to let the Google car pass. But the driver did not slow down and a collision occurred. After the crash the human driver inside the autonomous Google car stated that he would have made the same decision as the car. Based on the fact that there will be no Big Bang and suddenly all other vehicles will be driven from autonomous vehicle we have to work with a mix of traditional, semi-automated and fully-automated vehicles and the interim period will likely last a couple of decades. This will introduce a novel sociotechnical complexity that must be handled by all road participants. Noy. et al. also emphasizes that decisions from technical system can not be flawless. Software failures are ubiquitous and often induced by external influence factors such as unrealistic or inarticulate project goals, inaccurate estimates of needed resources, incomplete system requirements, unmanaged risks and commercial pressure. Therefore it is an important aspect to understand that even the best algorithms are fallible [85]. Noy et al. introducing new level of crash cause factors [85]:

- Software Failures
- Failures due to a mix of automated and non-automated vehicles
- Failures due to inadequate transfer of control

Noy et al. also describes that in the past the Automotive Industry was mostly characterized by traditional mechanical engineering companies and methodologies. But this has changed with the upcoming automated driving trend in which digital companies such as Google are entering this market. This is disruptively changing the design, usability and utility of motor vehicles and will be an extension of the ubiquitous digital world [85].

3.6.2 STPA Based Approach

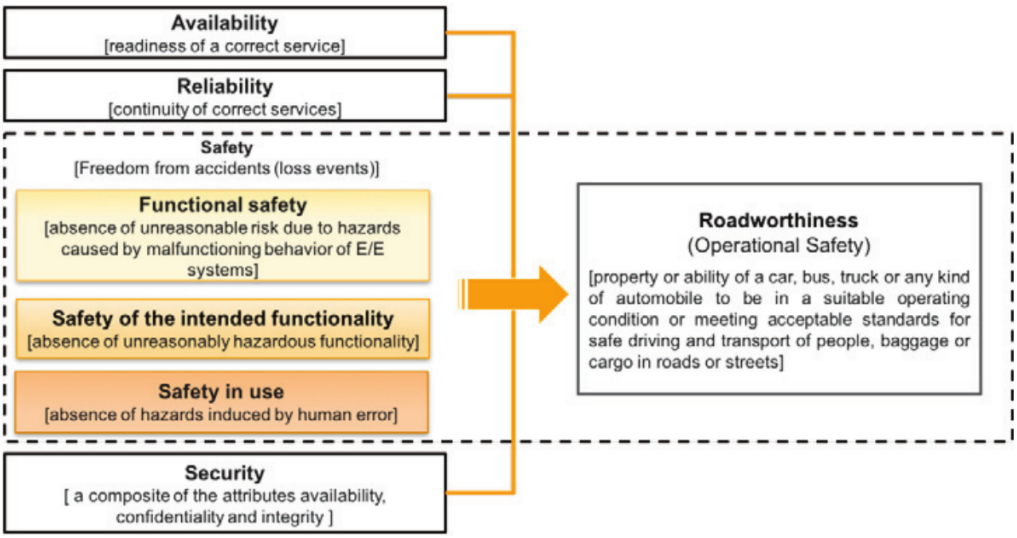

Figure 3.24: Overview of operational safety attributes related to vehicles with the ability of fully-automated driving [20].

Abdulkhaleq et al. [20] describes in their publication that operational safety depends on three different attributes as seen in Figure 3.24 [20]:

- **Availability**
  The availability describes the probability or degree of a system that is in a specific operable state of a random amount of time. The value is mostly given in a percentage such as 99.99%.

- **Reliability**
  Reliability describes the ability of a system to perform as intended for a specific amount of time that is determined at the design phase of the system.

- **Security**
  Security describes the protection of computer systems and networks against damage and disruption of their service by third parties.

These attributes are partly covered by the ISO 26262 safety standard but their focus is not aligned to fully-automated driving vehicles. For this purpose, Abdulkhaleq et al. developed a novel safety process that is aligned to fully-automated driving vehicles and are based on the Systems-Theoretic Process Analysis (STPA). The STPA is based on the Systems-Theoretic Accident Model and Processes (STAMP) model and considers accidents as a chain of events. This point of view allows for treating accidents as a control problem of complex dynamic processes in which humans are interacting with machines. These approaches are able to detect more possible hazards such as unsafe interactions among components and misunderstandings between complex software systems and the operators [20].

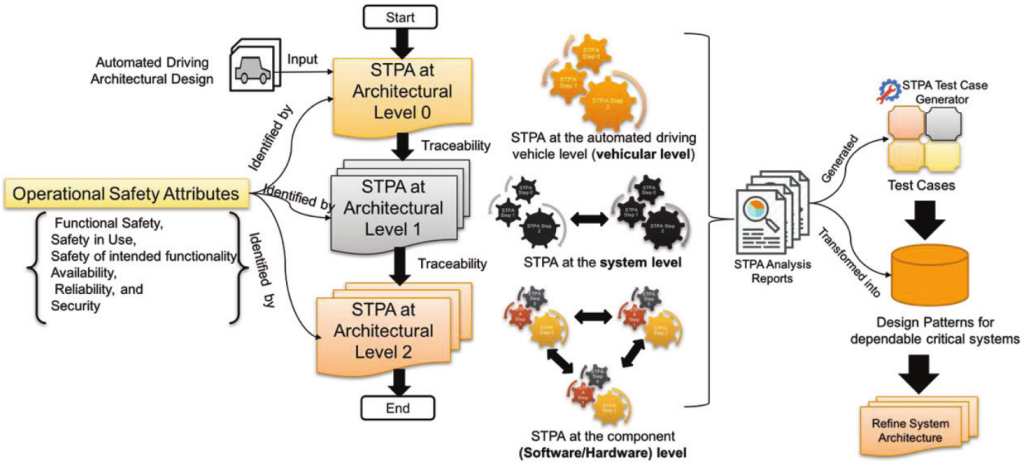

Figure 3.25: STPA based safety approach for handling the safety complexity of automated driving [20].

The process of Abdulkhaleq et al. is depicted in Figure 3.25. The process is divided in five major steps [20]:

- **Decomposing the architecture of the fully-automated driving vehicle**
  The system architecture can be decomposed into three levels: autonomous vehicular level, system level and component level. Every abstraction layer addresses specific problems [20].

- **Applying the STPA approach at different architecture levels**
  The STPA approach is applied on all different decomposition levels. The main focus is on defining traceability between the different decomposition level hazards [20].

- **Developing operational safety concepts for the fully-automated driving vehicle**
  This step identifies the associated risks of each property and derives the result into a novel architecture design [20].

- **Generating test cases to evaluate the architectural design**
  Tests are derived from the STPA results and supports the verification engineers to test the fully-automated driving architecture prototypes [20].

- **Developing design patterns for dependable critical systems**
  The last step is for improving future development of fully-automated driving vehicle systems and derives design patterns and best practices of the current developing process [20].

Abdulkhaleq et al. used the widely employed STPA approach to identify fully-automated driving safety requirements. Their approach is to divide complex systems into three abstraction layers and is focusing on the interaction of different components. They emphasize that reliability is one of the most important key factors for safety, but did not address this in their process.

3.6.3 Statistical Reference Model

Berk et al. [21] describe in their publication a novel approach to determine sensor reliability from statistical models that are based on comparing the output of redundant sensors.

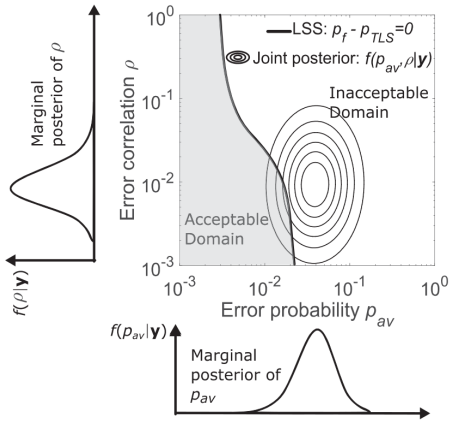

Figure 3.26: Illustration of the system reliability verification of Berk et al. [21].

The approach of the system reliability verification process that is depicted in Figure 3.26 has the main advantage that a statistical reference model can be developed without extensive testing. The statistical reference model is continuously improving due collecting reliability data from all vehicles in the fleet. Their work clearly shows that their approach is feasible but they also address some challenges that still must be solved such as inadequate statistical models that can lead to pseudo interference [21].

3.6.4 Dynamical Tactical Safety

Khastgir et al. [22] emphasizes that with the transition from traditional fail-safe vehicles of SAE Automation Level 0-3 to fully-automated vehicles is a changing nature of interactions between the environment and the system. These novel interactions require a continuous real-time evaluation of the current ASIL level. In their publication they describe a novel framework which demonstrates the feasibility of their novel approach. Their initial point is a Dynamic Risk Analysis which updates the accident and the failure probabilities. Based on these values the framework calculates a health status of the specific system [22].

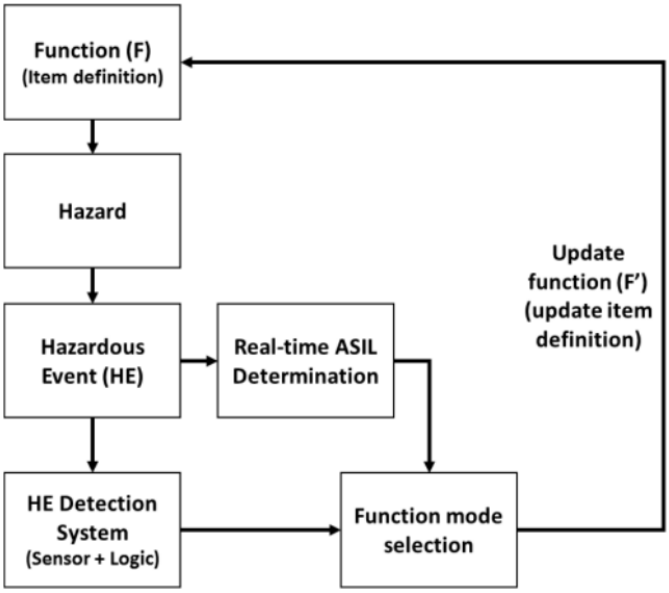

Figure 3.27: Dynamical Tactical Decision Making Framework [22].

The framework, as seen in Figure 3.27, has a process which is separated into five steps:

- Item Definition
- Hazardous event detection system
- Objectification of Automotive HARA
- Real-time ASIL determination
- Decision and Control for countermeasure (updating item definition to lower the ASIL

The main advantage of this novel approach is that the current HARA process of the ISO 26262 is very static and does not consider environmental changes. With this approach the overall system becomes dynamic and enables the degradation of the ASIL level during runtime [22].

3.6.5 Classification Failure Mode Effects Analysis

Salay et al. [23] describes in their work that traditional safety analysis methodologies such as the Failure Tree Analysis (FTA) or Failure Mode and Effects Analysis (FMEA) are struggling with Machine Learning (ML) algorithms. For this purpose, their publication is introducing a novel approach called the Classification Failure Mode Effects Analysis (CFMEA). This approach enables an assessment of the classification-based perception of the novel automated driving system [23].

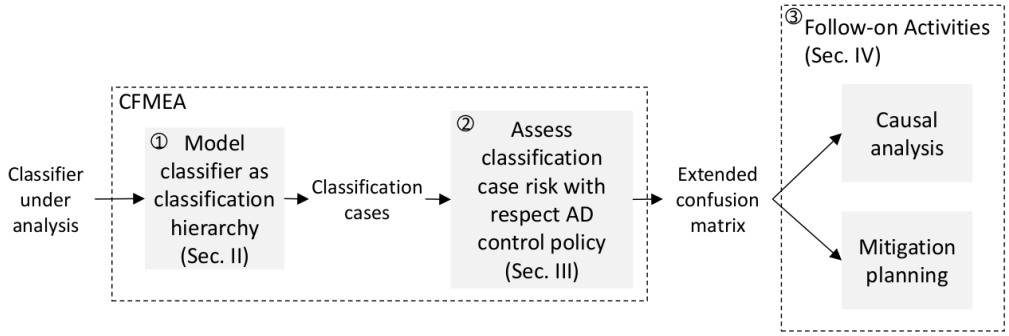

Figure 3.28: Classification Failure Mode Effects Analysis [23].

The process, as seen in Figure 3.28, is divided into three main parts [23]:

- **Model Classifier as Classification Hierarchy**
  The first step is abstracting the classifier and mapping it into a hierarchy to detect the possible perception problem as well as their subclass relationships.
- **Assess Classification Case Risk with respect Autonomous Driving Control Policy**
  The second step is about estimating the risk that is based on the specific hierarchy and classification level. The risk is based on the severity, the effect and the controllability. These three characterization points are already well known through the ISO 26262 safety standard.
- **Follow-on Activities**
  The third and last step is about identifying high risk cases and planning specific mitigation strategies.

Their current work is evaluated with simulations which are clearly depicting the feasibility of their approach.

3.6.6 Operational Design Domain

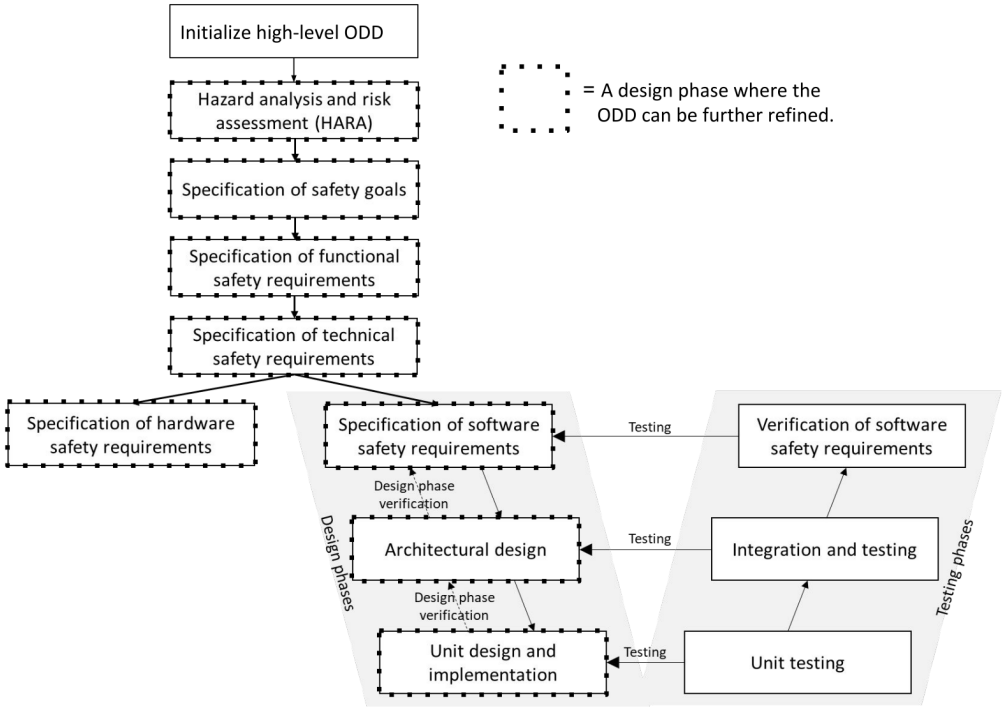

Figure 3.29: Integration of the ODD approach into the design process [24].

SAE has introduced the Operational Design Domain (ODD) approach to handle fully-automated driving vehicles on SAE Automation Level 3 upwards [87]. This approach is monitoring the current driving situation and considers road type, environmental conditions, road participants during run-time and is analyzing if the ADAS systems are in a valid state to handle the specific situation. Therefore, this approach can also be seen as a functional system boundary that is specified during the design phase of the system. The monitor is triggered by boundary violations and is triggering a Dynamic Driving Task fallback. In the SAE Automation Level 3 this fallback can be handled by the driver, but in the other Automation Levels the ADAS system must handle this specific situation on its own [24]. In general the ODD domain focuses on the following three tasks [24]:

- **Design Process**
  The Design Process focuses on identifying the safety-critical driving situations that must be handled by the ADAS systems.

- **Testing and Verification**
  This step is providing generated test cases to verify the correct functional boundaries of the system and to validate the Dynamic Driving Task fallbacks.

- **Online Monitoring**
  The ODD approach enforces the system to permanently monitor the current driving situation and evaluates the current scenario with the internal designed functional boundaries. The Dynamic Driving Task fallbacks would be instantly activated in case of boundary violations.

Figure 3.29 depicts the integration of the ODD approach into the widely used V-Model Design approach of the Automotive Industry. The approach is supporting a top-down and a bottom-up approach. This enables an iterative improvement of the overall design. On top of the process is the high-level ODD. The high level ODD specifies the limitations of the physical vehicle values in specific situations based on road structure, road users, animals, other obstacles, environmental conditions and the current vehicle behavior. During the safety process that is based on the traditional safety assessment of the ISO 26262 safety standard is the ODD further refined [24]. One of the biggest challenges in this approach is to monitor the actual driving situation and the evaluation and actuation of the Dynamic Driving Task fallback. For this purpose, Colwell et al. [24] introduced a feasibility on the monitoring task and introduced a novel ODD monitor as seen in Figure 3.30.

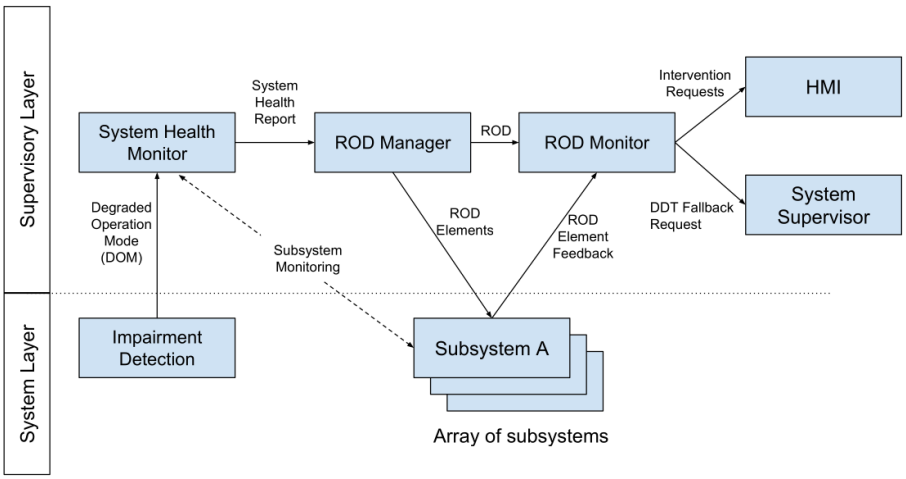

Figure 3.30: System Architecture of the ODD System Monitor [24].

The monitor system is divided into two parts [24]:

- **System Layer**
  The System Layer is activating the Dynamic Driving Task in case of functional boundary violations.

- **Supervisor Layer**
  The Supervisor Layer is monitoring the whole ADAS system and is actively interacting with the System Layer.

3.6.7 Blind Spot Analysis Operational Safety Attributes

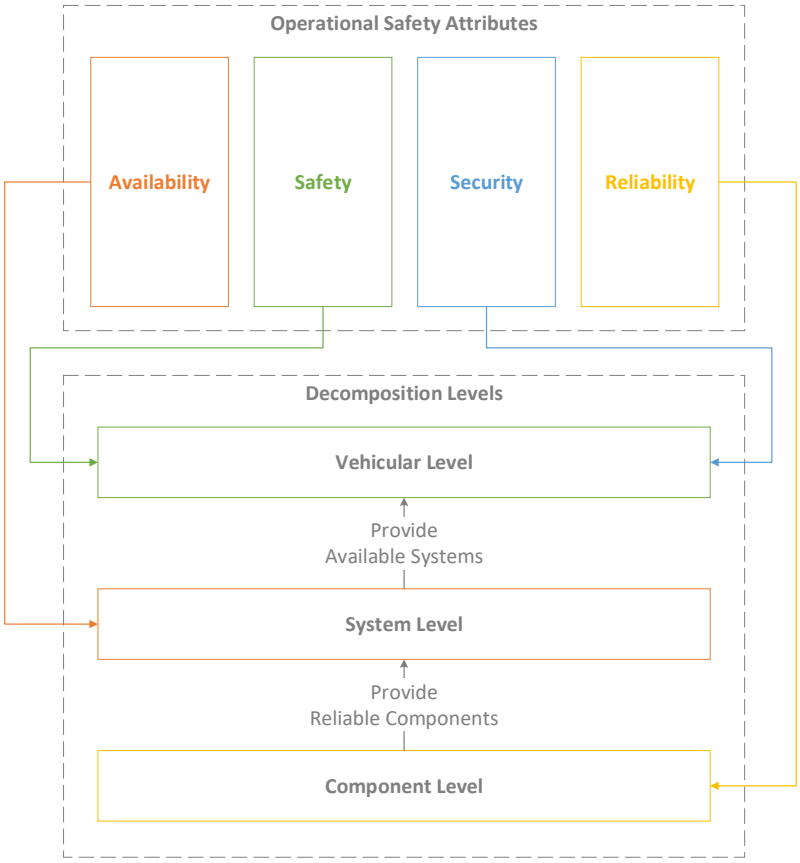

Figure 3.31: Operational Safety Attributes with the related Decomposition Levels (Adapted from [20]).

As already stated in the beginning of this Chapter, the awareness of the disruptive change in the current safety processes is already very high in the automotive industry as well as in the academic domain. Abdulkhaleq et al. have introduced the Operational Safety Attributes as seen in Figure 3.31. In this Figure, the Operational Safety Attributes were combined with the Decomposition Levels and mapped together in a logical view. The ISO 26262 safety standard is partitioning an Item into Systems and these are a combination of several individual Components. In this Figure the decomposition is declared as Vehicular Level, System Level and Component Level. For handling the complexity of safety we have to divide the Operational Safety Attributes to the specific Abstraction Layer such as Reliability to the Component Level, Availability on System Level and Safety and Security as a whole on the Vehicular Level.

In the last Subchapters, this thesis described several promising results on how to handle the complexity of safety in the context of Automated Driving and now it is necessary to

analyze the current approaches with the Operational Safety Attributes and the related Decomposition Levels. The introduced novel approaches have been [20, 21, 22, 23, 24]:

- **STPA Based Approach**
  The STPA approach is handling the operational safety from a holistic view. The main focus is on identifying usage scenarios in which an operator could be harmed. Based on the introduced Operational Safety Attributes overview this approach is assigned to Safety aspect on Vehicular Level.

- **Statistical Reference Model**
  The Statistical Reference Model is creating a statistical model of specific systems and sensors based on real operational data. Their approach is to continuously improve the internal statistical reference model and to detect total failures in prior. Based on the Operational Safety Attributes this approach is assigned to the Reliability aspect on Component Level.

- **Dynamical Tactical Safety**
  The Dynamical Tactical Safety approach is monitoring the current driving situation and is evaluating if the current system is fulfilling the desired ASIL Level in real-time. In the Operational Safety Attributes chart this approach is assigned to the Availability on System Level, because their main focus is on adapting the Functional modes to enable a fail-operational behavior.

- **Classification Failure Mode Effects Analysis**
  The Classification Failure Mode Effects Analysis is a novel safety analysis approach to support safety engineers in mitigating Machine Learning based safety risks. This approach is assigned to the Safety attribute on Vehicular Level.

- **Operational Design Domain**
  The Operational Design Domain is a similar approach as the STPA based approach and is focusing on detecting hazardous situations on a holistic view. Therefore, this approach is assigned to Safety on Vehicular Level.

Based on this analysis it becomes visible that the current scientific work has already addressed all Operational Safety attributes and that the most popular approach is the holistic view on the fully-automated vehicle to gain control over the high risks and uncontrollable states of automated driving. The Operational Design Domain (ODD) approach that is recommended by the SAE clearly shows that fully-automated driving vehicles must be continuously monitored in real-time with a specific internal model with functional border limitations. In case of a limit violation the system needs to be defensive and transit the current system into a safe situation such as stopping on the service lane. One of

the biggest challenges are left out situations as seen in the CFMEA analysis. Especially Machine Learning based control structures are introducing a wide variation of unintended controls caused by the incomprehensible mathematical models that are configured by millions of datasets. Particularly, the automotive industry is well sophisticated about the impracticality of considering all possible driving situations that are possible on all different continents, in each country, within all cultures in the whole world. Therefore, most of the research focuses on this specific challenge, because without a robust system design that is at least working harmless fully-automated driving will not be possible in the next few years or decades. But the Vehicular Level is trusting the lower abstraction Levels such as the System and the Component Level. Considering the best Safety Monitors on Vehicular Level can not work flawlessly if the lower abstraction Levels are unfit to provide flawless data and results. If we are considering the Divide and Conquer approach than we have to start at the Component Level because only if we are mastering this specific Level we can further progress to the other Levels. But the Component Level is the least considered Level in the Automotive Industry considering Fully-Automated Driving. That raises the question:

Why is the Component Level the most neglected domain in the context of Automated Driving?

Electrical systems are mostly highly integrated as semiconductor devices and therefore related to the semiconductor domain. Therefore, the Component Level is strongly connected to the semiconductor domain. In this domain, reliability is well investigated from a physical point of view and the industry has started to develop specific methodologies to measure and gain control of reliability issues that are published in specific industrial standards such as the IEC 62308. The IEC 62308 is a fundamental standard that is highly sophisticated and the Automotive Industry did not consider necessary to specify semiconductor safety in their standards such as the ISO 26262 initially. But with the revision of this standard specific fundamentals and methodologies have been integrated into Part 11 - Semiconductor Guideline. Most of their methodologies are referencing the IEC 62308 standard that represents the defacto standard for all possible electrical devices but mostly consumer based electronic devices. The semiconductor industry is mostly focused on developing novel automotive systems for vehicles that will be released in the next couple of months. Based on the fact that nowadays, beside some prototypes, there are no mass-produced vehicles that offers a wide range of fully-automated system functions. Therefore, this industry had no reason to think about the transition from a semi-automated to a fully-automated vehicle.

Another aspect why the Component Level is not that much considered is described in the Paper of Noy. The trend of fully-automated vehicles and their functionalities are

mostly driven by digital companies such as Google, Uber or Tesla. These new companies are entering the automotive market, but were mostly focused on huge enterprise software systems. Therefore, they are considering hardware as a must have but nothing more. These companies want to impress the overall public and this can not be done with high reliable components. They are working on higher abstraction levels such as detection of obstacles and controlling the vehicle.

The Component Level is already well fail-safe caused by the long tradition of reliability engineering in semiconductor devices and can be seen with the highly sophisticated industrial standards such as the IEC 62308. But most of the automotive industry is focusing on traditional manual driven vehicles and are beginning with introducing semi-automated vehicles on SAE Automation Level 3. But in the next few years or decades the Automotive Industry will go further to SAE Automation Level 4 and 5 and then the semiconductor industry has to provide more reliable components. If the semiconductor industry is missing this trend, it could be the case that the provided fully-automated vehicles are not safe or the launch of these vehicles will be postponed. This would be tragic but not existence-threatening. But there could be the case that this is an opportunity for novel start-up companies to take over the automotive market if they can provide this industry with highly robust components. To prevent such situations this thesis is emphasizing on the robustness and reliability of semiconductor devices on Component Level. This domain is responsible for the continuity of correct services and represents the ground base for all upper abstraction levels such as on System and Vehicle Level. An error of a single component is able to propagate this failure to the Vehicle Level and could trigger an action that is harmful for the passenger or other road participants. Considering the Operational Design Domain in which an If-Else statement is monitoring a specific boundary of the function and a component error is levering out this specific function could trigger a deadly accident. To prevent such a circumstance this thesis will be a base work of how to handle the Component Level of Automated Driving on SAE Automation Level 4 and 5.

Chapter 4

System Design and Methodologies

In the last chapters this thesis introduced the main challenges of future vehicles that have the ability to drive fully-automated. Currently, the automotive domain is mainly focused on the ISO 26262 standard when considering safety and reliability for automotive vehicles, but as already stated there is a main problem between fully-automated vehicles and the current standard, because the standard is still relying on the driver as a last backup instance in case of unintended failures. Over the next decades, this possibility will disappear and will force the automotive industry and their engineers to rethink these safety measures.

This chapter is divided into two parts: System Design of safety enhancements for LiDAR systems and Methodologies that can be used to optimize safety-critical Embedded Systems on reliability.

4.1 Reliability Gap

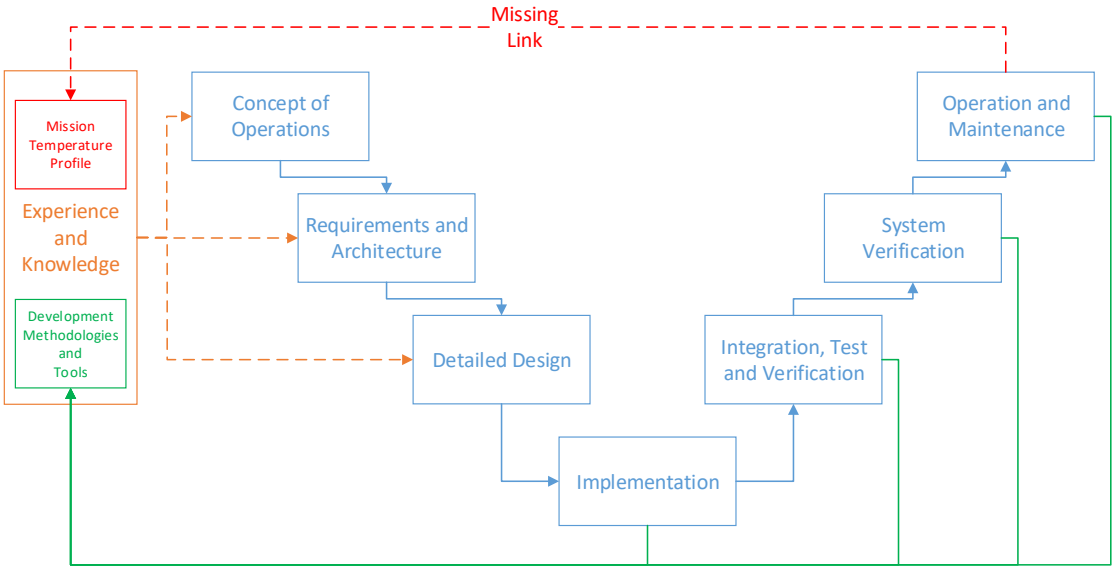

Figure 4.1: Reliability gap that is depicting the missing link between Operation and Maintenance and Experience and Knowledge.

Developing Embedded Systems in the Automotive domain is commonly done according to the V-Model. On the left side are the design phases at different abstraction and detail levels, at the bottom is the implementation phase and on the right side the verification and evaluation of the output. In Figure 4.1 is the V-Model with an Experience and Knowledge block that represents the basic know-how of the engineering teams as well as from the organization itself. Typically, any sort of best-practices or the usage of novel design tools and design methodologies are evaluated and are analyzed for future projects. But as already stated in the ISO 26262 there is an exception for field feedback of semiconductor devices caused by the fact of limited field data as already stated in Section 3.1.2.

This fact directly shows a missing link between Operation and Maintenance and the Mission Temperature Profile. The designer of the component is determining the mission temperature profile and any mismatch could lead to a lower reliability or in worst-case to an ASIL degradation. Considering this for fully-automated driving vehicles could lead to prior failures during critical operations such as driving with high speed on the highway. To prevent this it is necessary to rethink this situation and close this reliability gap because a design mismatch could have the most impact on hardware reliability based on the following facts:

- Mismatches between real and presumed temperature profiles directly affect component reliability (Exponential Effect) as seen in Section 3.1.

- Higher temperatures also directly influence hardware cost and this could lead to best-case assumptions to reduce cost.

This leads to the requirement of a novel HW/SW Co-Design approach that focuses on safety and optimizes safety-critical Embedded Systems on reliability.

4.2 Methodologies

4.2.1 Safety-Optimized Systems Development Lifecycle

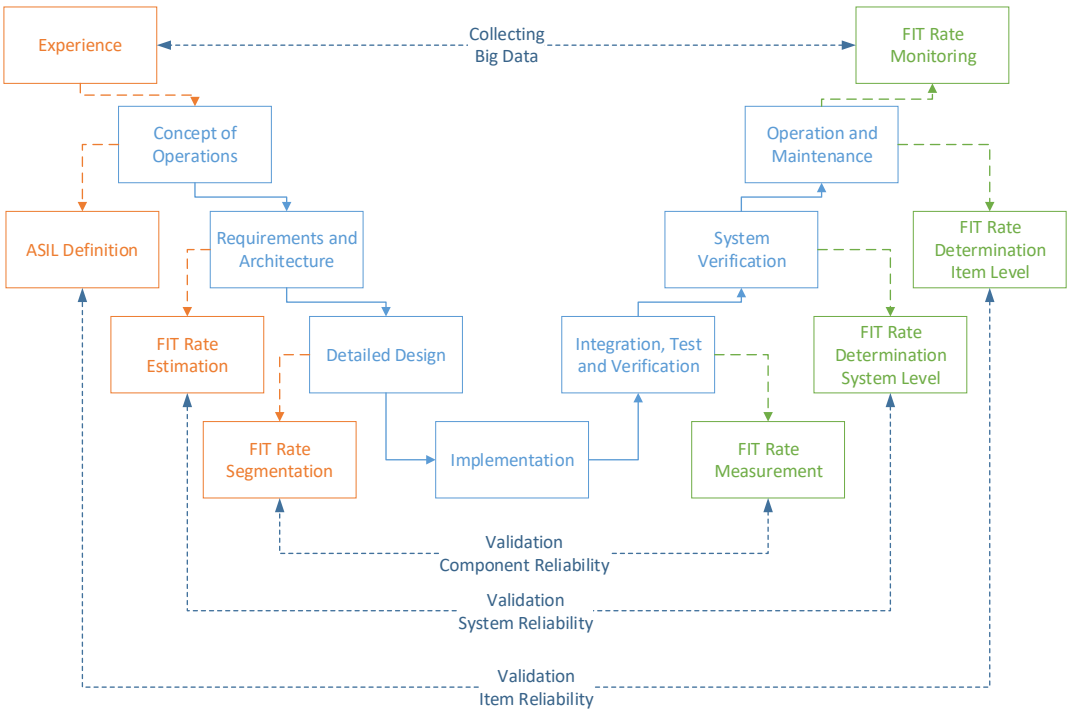

Figure 4.2: Systems Development Lifecycle that includes safety-optimized modules to harden safety-critical Embedded Systems for fully-automated driving.

The current System Development Lifecycle is based on the V-Model and must be extended with additional processes to enable an optimization of safety-critical Embedded Systems on reliability. The V-Model is hierarchically structured and represents different abstraction layers on the vertical axis. To enable safety optimization I have to add a process on each layer as seen in Figure 4.2.

In general, there are three main abstraction layers available in the automotive domain: Component, System and Item. The fact that late changes are related to higher costs,

as already stated in Section 2.2.2 inspires the need for validating the reliability of each abstraction layer as early as possible. Nowadays most of the reliability analysis is done afterwards when the product is already reaching the system or item level. To prevent this circumstance I have to implement three novel validation processes:

- **Validate Item Reliability**
  The Item abstraction layer represents an Embedded System that will be integrated inside the vehicle and is integrating several systems. This represents the highest abstraction layer and therefore is directly related to the functional specification document that is determined in the Concept of Operations. Inside this process step, the ASIL will be determined based on the HARA. Therefore, this process already offers a safety quantification based on the ASIL and the related reliability definition as described in Section 3.1. This quantification must be evaluated with the resulting FIT Rate on Item Level.

- **Validate System Reliability**
  This abstraction layer is based on System level and represents architectures and requirements of sub-parts of the Item. On this level, there is a need of separating the FIT Rate on Item level that was determined through the HARA. This separation already requires some sort of experience or simulation results to assess the presumable FIT Rate of individual systems.

- **Validate Component Reliability**
  Component Reliability must be validated on the lowest possible abstraction level such as modules. Modules can be integrated on hardware or software layer and represents the minimum unit. The quantification of the FIT Rate on this level is the most challenging part because there is the need of breaking the FIT Rate on system level down into smaller parts.

To enable validation of safety-critical Embedded Systems on these three abstraction layers I have to consider the following requirements:

- Introducing lifelong FIT Rate monitoring
- Integrating FIT Rate segmentation into the Development Lifecycle
- Measuring FIT Rates on individual modules before integrating them on System Level
- Analyze and measure software impacts on hardware reliability

4.2.2 Safety-Optimized HW/SW Co-Design Process

Reliability is one of the key parameters for novel fully-automated vehicles. As already described in Section 7.3, the main difference of stressed consequences between mechanical components and highly integrated semiconductor chips is the fact that mechanical components change their visual appearance such as fissures and their audio frequency by moving parts and any thermal stress inside semiconductor chips can not be detected at the outside. This could directly lead to a deadly accident considering the circumstance of a fully-automated vehicle that is driving with high speed on the highway. To prevent such accidents it is necessary to optimize these ADAS on reliability to extend the MTBF as long as possible. This can not guarantee a flawless operation in general but it will decrease the probability.

Figure 4.3 gives an overview of the typical driving factors about HW/SW Co-Design optimization. Most of the time performance and energy efficiency are the key factors that are optimized to extend battery usage [25].

The fully-automated driving area will disruptively change the design and implementation of novel ADAS systems and this will force engineers to optimize on other driving factors such as the reliability. This thesis introduces a novel approach that focuses on this requirement and allows for optimization of safety-critical Embedded Systems on component reliability. A process overview can be seen in Figure 4.4.

At the top is the Embedded System that is under development and which should be optimized on reliability. This HW/SW Co-Design flow has the precondition that the HARA has been performed and that the ASIL level with the related FIT Rate is available. The next step is about partitioning the Embedded System that is defined as Item according to the ISO 26262 part into systems, sub-systems and components. The whole Item has the FIT Rate about value X and represents the FIT Rate according to the ASIL definition such as 10 for ASIL D. As a next step, the process is dividing the whole Item into systems as a next, more detailed, abstraction layer. The example is reducing complexity by choosing exemplarily single systems such as the Control System. At this abstraction layer, the

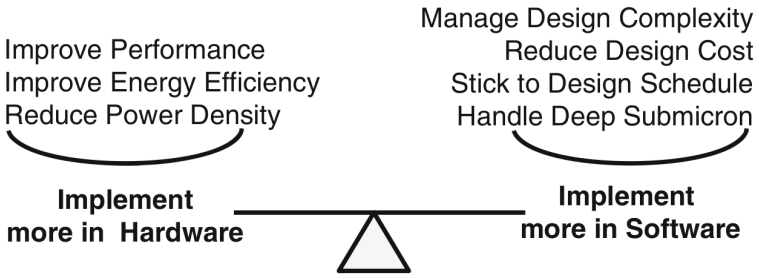

Figure 4.3: HW/SW Co-Design driving factors [25].

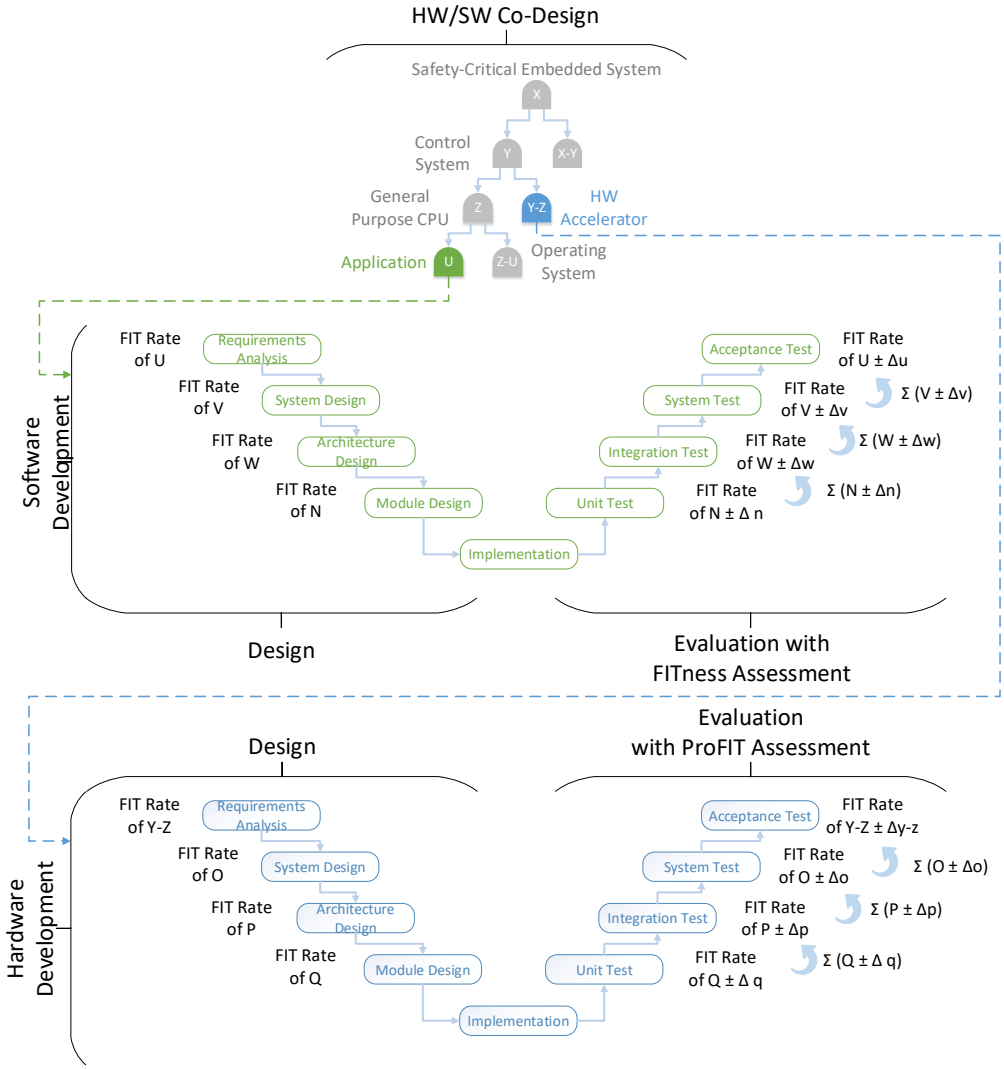

Figure 4.4: Safety-Optimized HW/SW Co-Design Process [26].

upper FIT Rate is divided and partitioned to all systems that are integrated in the Item. The Control System requires a FIT Rate of Y and all the other systems have the residual FIT Rate of X-Y. These steps will be further executed on all possible abstraction layer like the sub-system abstraction layer such as the General Purpose CPU as well as software modules that will be executed on the CPU [26].

The most complex task in this process is the exact separation of the FIT Rate for all different abstraction layers. A single mismatch at higher abstraction layers will propagate a failure through all lower abstraction layers. Therefore, to reduce the risk of wrong FIT Rate estimations it is advisable to use experts in this field or the usage of simulation models that are capable to provide detailed hardware information related the used transistors and

power dissipation [26, 96].

Towards Simulation based Component Reliability Estimation

The usual design process of developing optimized hardware-software systems is to start at a high abstraction layer and work through all abstraction layers till you reach the floor plan of the microchip. This approach enables the separation of layer specific problems and allows for faster development by using high abstraction tools and languages [97]. Developing and manufacturing Application-specific integrated circuits (ASIC) hardware components requires high efforts in time and money. Consequently, any mistake that was made during the development phase, such as wrong design decisions or functional mistakes, has a high impact on the success of a specific hardware component. For this reason, the hardware development industry started early to evaluate their hardware design in a virtual prototype that is implemented on a high-level abstraction layer such as SystemC [97].

SystemC is a library for C++ and represents a modeling and simulation language for hardware/software co-design. It is widely used in the industry to simulate high-level system designs to evaluate design decisions and functional verification of novel hardware/software system architectures [98]. The high acceptance of SystemC for virtual prototype verification can be seen in several projects such as the embedded image processing system from Chong et al. [99], the verification of the packet processing engine for a XDNP network processor by Pei-Jun et al. [100] or the AVS video decoder system modeling with SystemC by Mei Fen et al. [101]. Beside the use of SystemC for model-based hardware-software co-design, SystemC is also used for safety-critical domain analysis e.g. in the automotive industry.

The automotive industry is putting a huge effort in the design of fail-safe automotive components and they already started in early design phases such as hardware simulation at high abstraction layers to verify their system architecture. Shatat et al. [102] introduced a tool that is able to verify the timing behavior of virtual prototyped AUTOSAR software components at an early design stage. But there are also approaches to use SystemC for functional safety analysis such as the Fault tree analysis of embedded systems by Zarandi et al. [103]. Another safety-related example of the automotive industry is the White-Box error effect simulation for assisted safety analysis from Reiter et al. [104]. These examples clearly show that SystemC can be used to verify and evaluate functional safety related functions and requirements at an early design stage of the hardware components. Nevertheless, functional safety starts with reliable hardware components because any fail-safe system needs to rely on resilient components. For this reason the ISO 26262 functional safety standard for electrical and electronic systems claims specific component reliability

quality levels that depends on the specific ASIL of the system [10].

ASIL represents a risk classification that supports the developers of safety-critical automotive systems to specify safety requirements and is divided in four classes ASIL A to ASIL D. Where ASIL D represents the most critical system and requires among others the lowest failure of a value of 10 [10]. The FIT represents the quality of the component in terms of component reliability. If the final hardware component does not match the safety requirements of the specific ASIL level, it is necessary to redesign or add additional safety structures to the basic system architecture until the claimed specifications can be met. This circumstance causes high development efforts and can also have an impact on the profitability of specific systems. For this reason, the desired component reliability should be evaluated at an early design phase of the hardware development, preferably at an early stage of development such as virtual prototype verification.

The Arrhenius equation, as seen in (3.1), clearly shows that the FIT Rate is among others related to the power dissipation (P_{dis}) of the hardware component. Power dissipation of hardware components can be calculated with the following equation [105]:

$$P = f \cdot (U_{dd}^2 \cdot (1+\sigma) \cdot \sum_{k=1}^{K} \frac{\alpha}{2} \cdot C_k + T_{cp} \cdot (U_{dd}^2 \cdot \sum_{k=1}^{K} + U_{dd} \cdot \frac{\Delta I_{dsoff}}{\Delta W} \cdot \sum_{g=1}^{G} \cdot W_g) \tag{4.1}$$

The total power dissipation, as seen in (4.1), shows that the power dissipation is among others dependent on the number of transistor (K), the node activity (α), time-period (T_{cp}) and the power supply voltage of the component (U_{dd}). For hardware manufactures, the specific Base FIT Rate (λ) needs to be determined with the following equation that is from the IEC TR 62380 component reliability standard [51]:

$$\lambda = (\lambda_{die} + \lambda_{package} + \lambda_{overstress}) \cdot 10^{-9}/h \tag{4.2}$$

$$\lambda_{die} = (\lambda_1 \cdot N \cdot e^{-0.35 \cdot a} \cdot \lambda_2) \cdot \frac{\sum_{i=1}^{y} (\pi_i \cdot \tau_i)}{\tau_{on} + \tau_{off}} \tag{4.3}$$

$$\lambda_{package} = 2.75 \cdot 10^{-3} \cdot \pi_\alpha \cdot (\sum_{i=1}^{z} \pi_{ni}) \cdot \Delta T_i^{0.68}) \cdot \lambda_3 \tag{4.4}$$

$$\lambda_{overstress} = \pi_I \cdot \lambda_{EOS} \tag{4.5}$$

The Base FIT Rate of the hardware component can be determined with equations (4.2) (4.3) (4.4) (4.5), which clearly show that the rate is among others dependent on the base failure rates of the integrated circuit family, technology mastering and package

$(\lambda_1, \lambda_2, \lambda_3)$, but also from the number of transistors in the integrated circuit (N).

In the previous paragraphs several mathematical models have been introduced that describe the physical background necessary to determine the FIT Rate of a hardware component. Furthermore illustrating examples that already solved specific problems such as power dissipation or area estimation from high-level SystemC models. As a next step, these approaches should be advanced into a methodology that is able to calculate the specific FIT Rate at an early stage of development, considering the static FIT Rate based on the hardware components as well as the dynamic FIT Rate that depends on the operational power dissipation.

The process to determine the FIT Rate of a high-level virtual prototype in SystemC that can be seen in Figure 4.5 and splits into four phases:

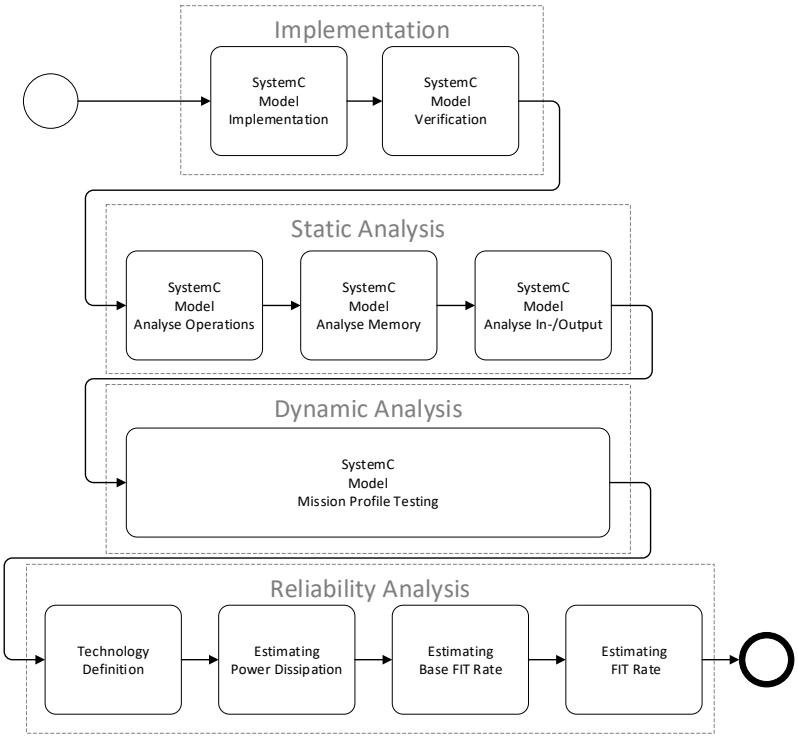

Figure 4.5: Overview of the simulation based FIT Rate determination process in BPMN notation.

1. **Implementation**
   The Implementation phase does not differ from the normal proceeding of implementing hardware components into a SystemC model.

   - **SystemC Model Implementation**
     In this step, the hardware-software co-design implementation of the desired

hardware component are implemented as a SystemC model.

- **SystemC Model Verification**
  This step is performed to verify the functional correctness of the implemented SystemC model.

2. **Static Analysis**
   The Static Analysis phase is necessary to determine the amount of transistors that are necessary to cover all operational tasks such as additions, all required storage such as registers and the Input-Output interfaces of the desired hardware component.

   - **SystemC Model Analyze Operations**
     In this step, all operators that are needed to provide all functions from the desired hardware component are counted such as additions, XOR, multiplication. These operators are then transformed into NAND gates and finally into transistors. As a result, all necessary transistors for the final hardware design are derived from the high-level SystemC implementation.

   - **SystemC Model Analyze Memory**
     In this step, the registers are summed up to get information about the required memory of the final hardware chip. This data is also transformed into transistors of the final hardware layer.

   - **SystemC Model Analyze In-/Output**
     As a last step, it is necessary to determine the Input and Outputs of the chip. This information is needed to determine the total power dissipation of the chip because of the necessary total amount of off-chip loads.

3. **Dynamic Analysis**

   - **SystemC Model Mission Profile Testing**
     The Dynamic Analysis can be performed optionally because this step is available to determine the average node charges and discharges (α) that are necessary for a more precise power dissipation calculation. For this purpose, test data that is similar to the data that will be executed on the real hardware in

the specific operational field should be executed on the SystemC model. Each bit flip will be recognized, recorded and statistically evaluated. Afterwards, the average node charges and discharges can be estimated. Nevertheless, this step can be skipped by performing a worst case analysis with α equals 1. This means that all nodes are permanently charged and discharged.

4. **Reliability Analysis**
   In this phase, the FIT Rate will be finally estimated for the low-level hardware component on transistor layer. For this purpose, it is necessary to specify the technological limits and values because the FIT Rate is dependent on the used technology.

   - **Technology Definition**
     In this step, the definition of the desired material technology is set such as CMOS, operation voltage, frequency, internal node capacitance, off-chip resistance and capacitance, junction temperature, n-channel width and others [105].

   - **Estimating Power Dissipation**
     The total power dissipation is calculated with equation (4.1).

   - **Estimating Base FIT Rate**
     It is necessary to calculate the base FIT Rate with equation (4.2).

   - **Estimating FIT Rate**
     In this step, the FIT Rate for the final hardware component, also considering the temperature variations caused by operational charges and discharges, is calculated by multiplying the Base FIT Rate with the Derating Factor.

After performing all phases of this novel *Simulation Based FIT Rate Determination Methodology*, the specific FIT Rate for the final hardware component on transistor layer is estimated.

Hardware Related Reliability Estimation

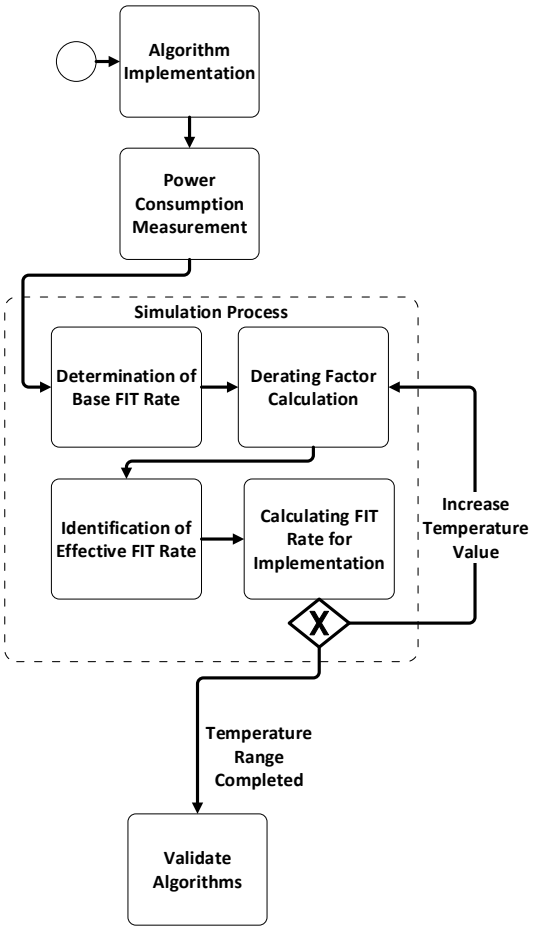

Figure 4.6: Process overview of the FITness Assessment that is able to determine the Hardware Reliability of specific IPs. [26, 27].

Enabling optimizations of safety-critical Embedded Systems on reliability requires quantification and measurement of different hardware designs such as Very High Speed Integrated Circuit Hardware Description Language (VHDL) implementations. Figure 4.6 depicts a hardware related reliability estimation algorithm that enables comparing two different hardware related algorithms [26, 27].

The FITness Assessment that can be seen in Figure 4.6 allows for this quantification of hardware implementations. The idea of this methodology is to use common standard procedures of component reliability estimations that are accepted and proven in use in the automotive domain. Therefore this methodology is using and combining different methodologies from the ISO 26262 standard. The methodology can be used for two different use cases [26, 27]:

- **Quantity based determination of the exact FIT Rate**
  The quantity based determination enables measuring the exact FIT Rate of a specific implementation in coherence with a specific hardware component. This is only possible when using an FPGA and related IPs or self written HDL modules.

- **Quality based determination of relative FIT Rate**
  The quality based determination is not related to a specific hardware component instead it focuses on comparing different algorithms by normalizing the measurement results. In this scenario it is just possible to make a statement that one algorithm will have a lower FIT Rate than the other. It is not possible to evaluate the exact FIT Rate. If there is a need to determine the exact FIT Rate it is necessary to use additional methodologies such as in Section 4.2.2 [26, 27].
  The FITness Assessment is divided in four steps to measure and evaluate different hardware algorithms and implementations [26, 27]:

  - **Power Consumption Measurement**
    This step focuses on measuring the power consumption of all implemented algorithms. It is advisable to use a generic framework in which all algorithms will be implemented because this will avoid a power consumption deviations based on different test environments. Furthermore, it needs to have a defined temperature for the whole testing such as 55°C.
  - **Base FIT Rate Calculation**
    The Base FIT Rate can not be measured, instead it must be determined with specific industrial standards such as the IEC TR 62380 [51] or provided by the hardware manufacturer in specific data-sheets.
  - **Effective FIT Rate Identification**
    The effective FIT Rate represents the reliability at a specific temperature value. For this purpose it is necessary to use the Arrhenius Equation to calculate the Derating Factor for other temperatures.
  - **Comparing different algorithms**
    In the last step all algorithms will be compared and this enables us to choose the most reliable one.

Further details about the hardware related reliability estimation can be found in the "FITness Assessment-Hardware Algorithm Safety Validation" [27] publication in Section 7.2 on page 129.

Software Related Reliability Estimation

Software and FIT Rates are not logically connected because FIT Rates are always describing the reliability of hardware components. But if software is considered as executable control instructions for the specific hardware module and related to the fact that it can control and actuate specific hardware parts than it can be seen that software has a direct influence on the power dissipation and also directly influences the thermal stress of the hardware component [26].

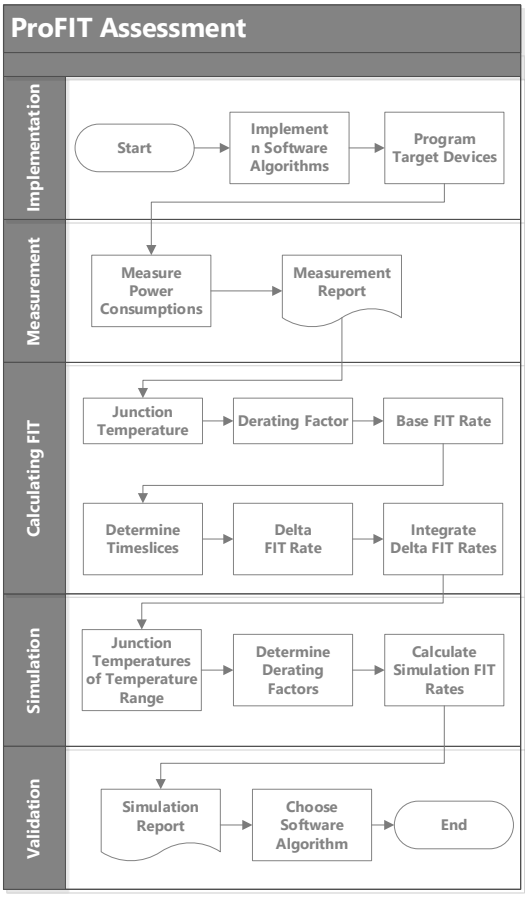

Figure 4.7: Process overview of the ProFIT Assessment that is able to determine the component reliability of specific software modules. [26].

Comparing functions that are implemented in software or hardware reveals one big difference between both variants. Logical functions that are implemented in hardware are rolled out as area and offer high performance and low latencies. If these functions are implemented in software than the area is reduced and transformed into time. This means that the function is divided into sub-routines and these sub-routines are executed on the same hardware several times. This general difference between hardware and software parts must be considered as well as it must be still in compliance with common proven-in-use

methodologies provided by the ISO 26262 standard [26].

Figure 4.7 shows the general process overview of the software related reliability estimation called ProFIT Assessment. This methodology also provides the possibility to perform a quality based and a quantity based evaluation of algorithms. But because all software modules have to be compiled and executed on a specific platform this fact can be neglected. The overall process can be divided into five different parts [26]:

- **Implementation**
  This step requires an implementation of specific functions in software. To guarantee a distortion-free measurement it is also advisable to write a general framework in which the different algorithms will be integrated.

- **Measurement**
  During the Measurement process the software modules are executed on a specific platform. It is important to consider the power consumption but also the current temperature.

- **Calculating FIT Rate**
  Software execution is primarily based on executing instructions inside the CPU and the organization of data. Therefore, time is an important factor and the amount of time a specific algorithm requires to perform a task also directly influences the power dissipation, thermal stress and the related component reliability. In this step, the FIT Rate is determined for each time-slice and summing up these values represents the FIT Rate for a specific temperature.

- **Simulation**
  The simulation step is necessary to determine the FIT Rate for other temperature ranges. These values can be used as input parameters for the Mission Temperature Profile and the related effective FIT Rate for a specific use-case.

- **Validation**
  The last step enables comparing different software algorithms with each other and choose an algorithm that is stressing the related hardware the least.

Further details about the software related reliability estimation can be found in the "HW/SW Co-Design Approach to Optimize Embedded Systems on Reliability" [26] publication in Section 7.6 on page 153.

4.2.3 Live State-of-Health Monitoring

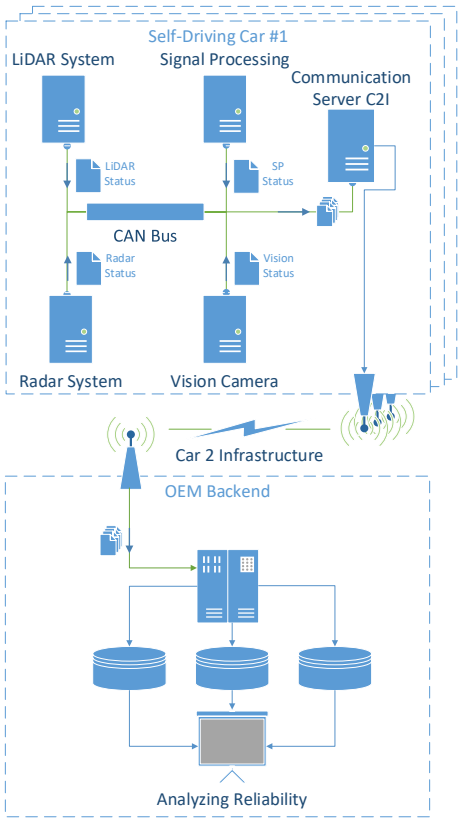

Figure 4.8: Illustration of future use-cases of the novel live state-of-health FIT monitor [28].

Component reliability is logically linked to the FIT Rate as described in Section 3.2. One of the most critical aspects of reliability at semiconductor components are wrong Mission Temperature Profiles as described in Section 3.2.3. Based on the fact that higher Mission Temperature Profiles are directly related to higher manufacturing cost caused by the need of more reliable components as well as the need of more material. This could seduce the automotive industry in specifying best-case temperature profiles with the goal to optimize the costs of the product. Nowadays, this would not directly affect the safety of an vehicle caused by the fact that the driver represents the last safety instance that is able to control the vehicle in unintended failures. Over the next decades, vehicles will advance their capabilities and provides fully-automated driving that transforms the driver into a passenger. In this scenario, best-case Mission Temperature Profiles could be misaligned with the real operation and lead to prior total failure of the system caused by higher stress with related ASIL degradation. But there can also be the case that the automotive industry is using too conservative Mission Temperature Profiles and that there is a potential to reduce cost. Both cases can't be evaluated considering the ISO 26262 and the

statement that the amount of field data is limited as described in Section 3.1.2. To enable an evaluation of the Mission Temperature Profiles as well as to provide more field data it is necessary to collect real data in the field and continuously send these data to the OEM and their Tier-1 and Tier-2 suppliers [28].

Figure 4.8 depicts a use-case of a fully-automated vehicle that provides state-of-health information to the OEM. All systems inside the car contain a specific live state-of-health monitor that is periodically sending this information over the Car-To-Infrastructure. This pool of data enables Big Data for safety and reliability in the automotive domain and also an analysis of the reliability of vehicle Items, specific systems or single semiconductor components. Furthermore, this information also contains temperature information about the whole operation time and could be used to optimize the current Mission Temperature Profiles of the OEMs [28].

One of the most critical aspect of electronic equipment is that such sensors and chips fail without any prior indication. This could have disastrous consequences for fully-automated driving systems and could lead to deadly accidents. But there is also an economical problem considering several maintenance services in short time intervals caused by sequential component failures.

To prevent certain circumstances as described before the novel live State-of-Health Monitor must fulfill the following requirements:

- **Live logging of current utilization of the safety-critical semiconductor device**
  - Correct Mission Temperature Profile data
  - Enabling Predictive Maintenance
  - Enabling Dynamic Safety
  - Life State-of-Health Monitoring
  - Detect reliability anomalies of software and firmware updates
- **ISO 26262 compliance**
- **Chip Area efficiency**
- **Flexible (Analog, Digital, FPGA, ASIC, Processes, Technologies, Functions**
- **Scalable Analysis (Single Devices up to complete Vehicle Fleet)**

Further details about the live State-of-Health Monitor can be found in the "Live State-of-Health Safety Monitoring for Safety-Critical Automotive Systems" [28] publication in Section 7.3 on page 135.

4.3 Safety Enhancements LiDAR

The last subsections described novel methodologies with a focus on optimizing fully-automated driving ADAS on reliability. The following subsection describes the current research prototype of a novel LiDAR system that is based on a 1D MEMS Micro-Scanning platform as described in Section 3.5. The current platform represents a robust design with several internal safety measurements. Nevertheless, this design represents a platform for SAE Automated Driving Level 3 and has therefore another focus on the internal safety measures. To enable a safe driving and a robust design for SAE Automated Level 4 and 5 there are still improvements possible that will be described in the next few sections.

4.3.1 Enabling Redundancy By Introducing Master-Slave Principle

Redundancy is one of the most essential approaches when considering safe and robust operation. Redundancy describes the procedure to duplicate specific parts of a system or the whole system and in case of failure switching to a backup system [10].

The novel 1D MEMS Micro-Scanning LiDAR approach is moving a laser beam in a horizontal line. If there would be just a single MEMS mirror then the whole safety and reliability would rely on this single construction. Based on the redundancy approach of the safety industry it would be beneficial to have a second LiDAR system that can support the overall environmental perception system. In case of two working LiDAR systems the range of sight in front of the car can be extended to a wider angle and in case of a failure the second LiDAR can still be used to provide data from the environment to establish a safe driving for the passenger as well as other road participants [29].

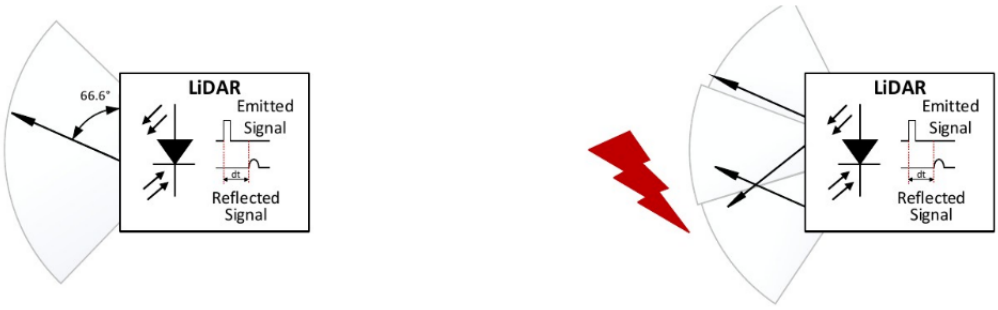

Figure 4.9: Interference between several LiDAR systems caused by the circumstance that the lasers are crossing each others.

Operating several LiDAR systems simultaneously leads to the side-effect of possible ghost images caused by the lasers that are crossing each others as seen in Figure 4.9. This side-effect is a crucial part of operating several LiDAR scanners simultaneously. To prevent this circumstance the lasers have to operate at the same frequency and simultaneously scan

the environment at the exact same angle position [29].

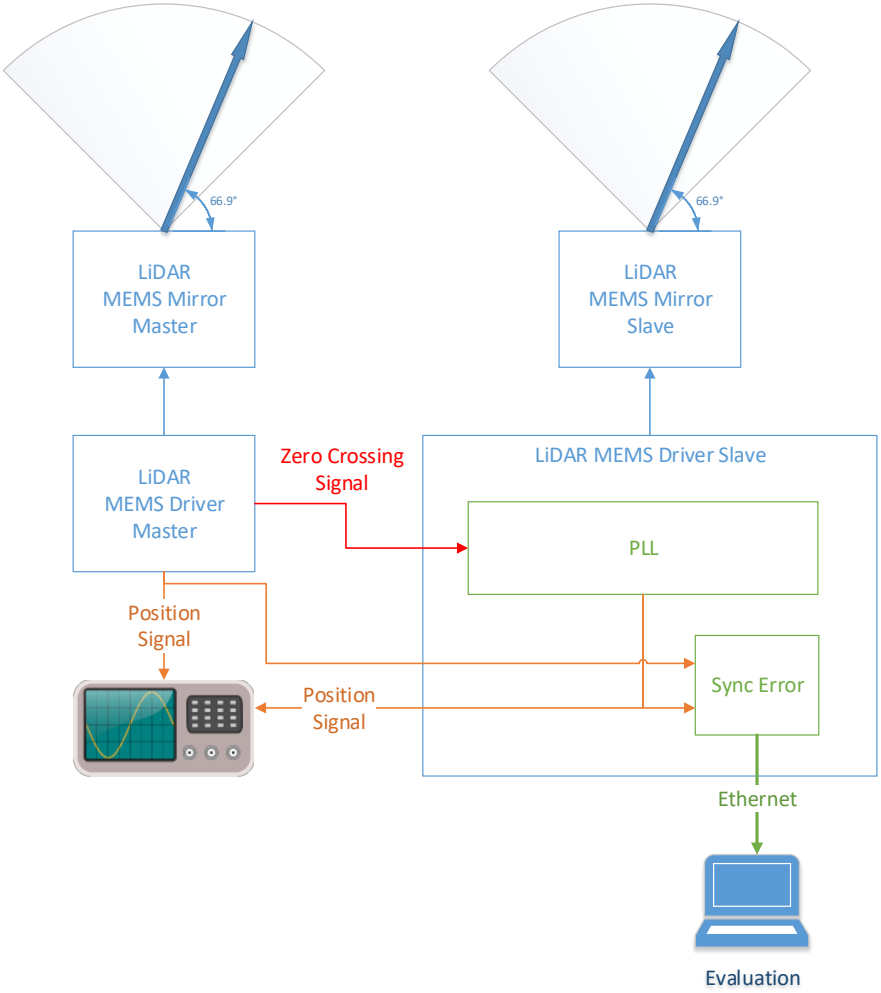

Figure 4.10: Synchronous mode concept overview of a Master-Slave principle that prevents crossing two or more LiDAR lasers [29].

To achieve an exact and aligned scan using several lasers a novel Master-Slave principle is required. The Master should control all other Slaves and prevent a crossing of the lasers. Figure 4.10 gives an overview of the concept of a synchronous mode of two independently controlled 1D MEMS Micro-Scanning mirrors. The main idea is that the Master is providing his Zero Crossing signal that represents an internal control signal for the position of the MEMS Mirror to all other Slave mirrors and that these mirrors are aligning their mirror to the same position. For evaluation purpose there is also a Sync Error module that is providing information of the desired position that is provided by the Master mirror and the position of the Slave mirror [29].

4.3.2 Enabling Fail-Operational Behavior

Transforming modern vehicles from traditionally controlled cars to SAE Automation Level 4 and 5 requires novel approaches concrning the safety aspect. As already mentioned in Section 7.3 is the fact that the driver can not be the last safety instance in case of uncontrollable failures. Therefore, the vehicle has to control every possible situation and has to manage any sort of unintended failures. This requires novel system architectures that enables fail-operational behavior. The main goal of these systems are to sustain operation until the vehicle is in a safe state that no human being or object could be harmed [30, 33].

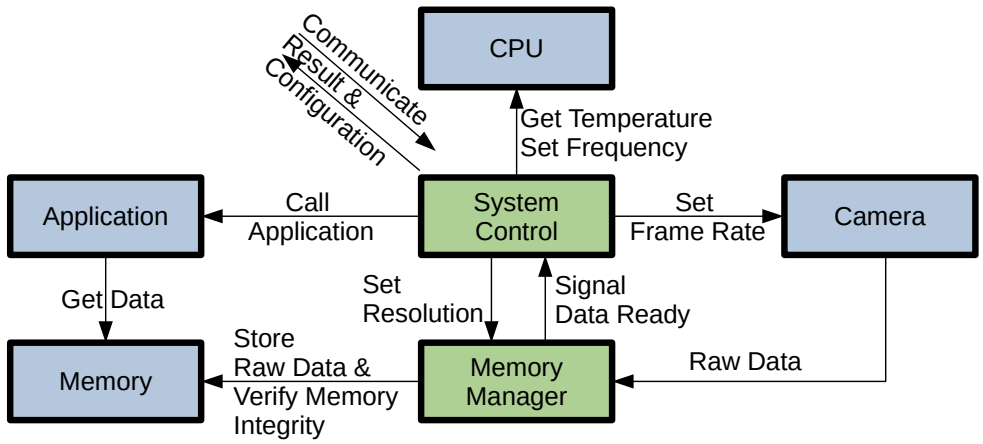

Figure 4.11: Overview of the novel Fail-Operational 3D Flash LiDAR system system architecture [30, 33].

Figure 4.11 describes the overall structure of the novel Fail-Operational 3D Flash LiDAR system. The system can be partitioned in two parts [30, 33]:

- **System Control**
  Module that is controlling the whole system and dynamically changes overall settings to enable fail-operational behavior.
- **Memory Manager**
  Storing memory data and continuously checking the correct state of the stored data blocks.

With these two modules the 3D Flash LiDAR system is able to fulfill the following requirements [30, 33]:

- Preserving Memory Faults
- Efficient and Effective Resolution Adaption

- Integrated Testing Functions
  - Realistic Scenario Simulations
  - Memory Fault Injection

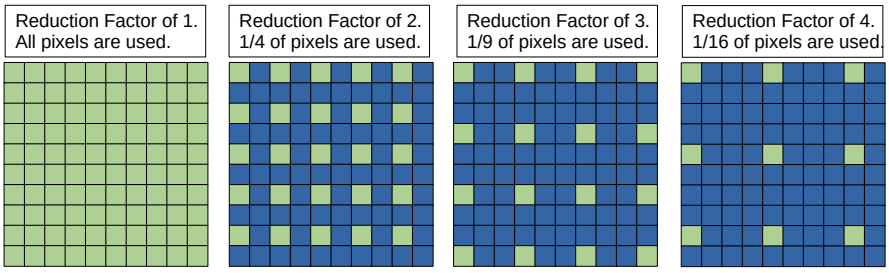

Figure 4.12: Efficient Dynamic Resolution adaptation of the novel Fail-Operational 1D MEMS Micro-Scanning LiDAR system [30, 33].

With continuous operation time of a LiDAR system, memory will continuously fail, especially in its last operation years. The Fail-Operational LiDAR system consists of an efficient dynamic resolution adaption algorithm depicted in Figure 4.12. The algorithm offers a Reduction Factor that can select sub-pixels such as one out of four and actively supports the system in case of corrupt memory or to prevent the corruption of memory blocks. The lower resolution automatically results to the fact that computer vision algorithms will not be able anymore to detect details inside the scenery, but it is still possible to detect objects on the street. For that reason, it is advisable to use lower resolutions on special roads such as highways. On highways, the possibility of sudden road participants on the roads is very low and therefore safer to use. If memory corruption happens during run-time than it is better to still provide an image to other ADAS than stopping the data flow abruptly. Figure 4.13 depicts the memory check module that is able to detect corrupt memory blocks and automatically disables them [30, 33].

4.3.3 Hardening LiDAR Against Residual Failures

Most of the time there are latent faults present in systems that will actively affect the system after long operational time. One of the most effective methods to mitigate this problem is to reboot a system [106].

After the reboot, some of these failures just disappear and the system can continue in its operation. But there are also cases in which an external event can trigger the need of rebooting a system. In case of LiDAR, strong shocks can trigger a total failure of the LiDAR system caused by the misalignment between the internal states of the Phase-Locked Loop (PLL) system and the real behavior and state of the analog MEMS mirror

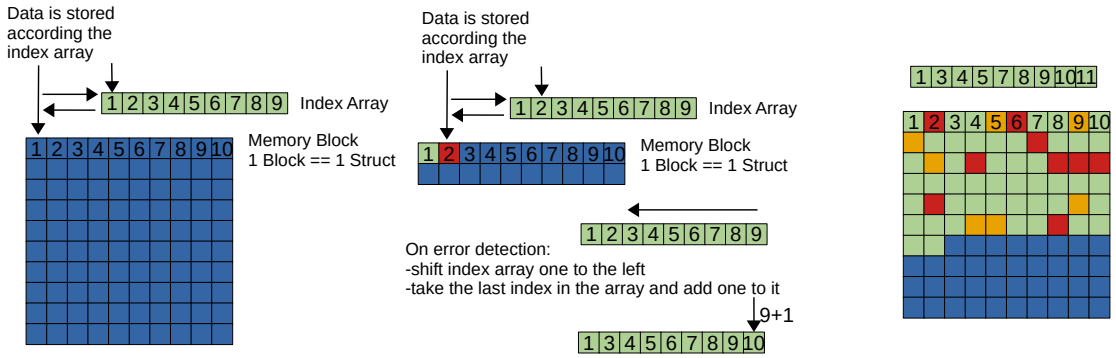

Figure 4.13: Memory check module of the novel Fail-Operational 1D MEMS Micro-Scanning LiDAR system [30, 33].

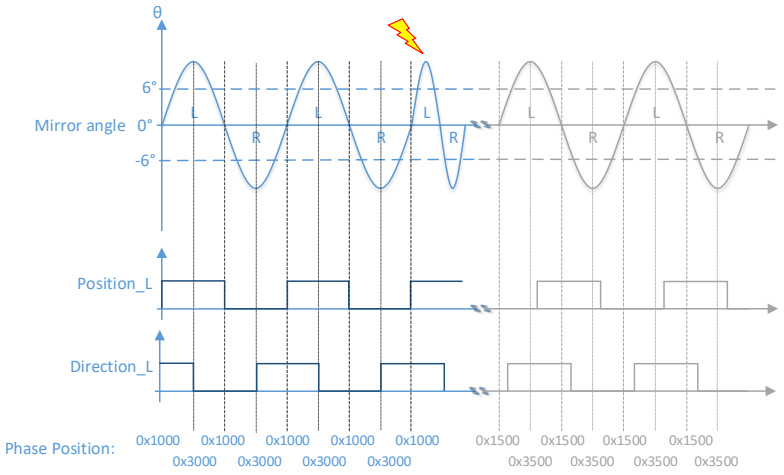

Figure 4.14: Fatal shock is triggering a total failure of the LiDAR system [31].

as seen in Figure 4.14.

When the PLL is losing the control of the MEMS mirror then the frequency of the mirror is dropping and as worst-case stopping the operation as seen in Figure 4.15. The state-of-the-art startup procedure of the MEMS mirror takes about 427 ms until full operation. This would result in the fact that at 100 km per hour the overall system would be blind for about 15m without any sight until the system can continue to provide environmental perception data. This is not possible considering a curvy country road [31].

To enable a fast resurrection in case of unintended latent faults it is necessary to speed up the current state-of-the-art startup procedure. Figure 4.16 depicts the novel approach that is based on preserving all internal states of the digital MEMS driver system that allows a faster start-up of the mirror because the start-up is slow caused by the non-linear oscillator behavior as described in Section 3.5.3.

The basic idea of the novel startup is based on the following two steps [31]:

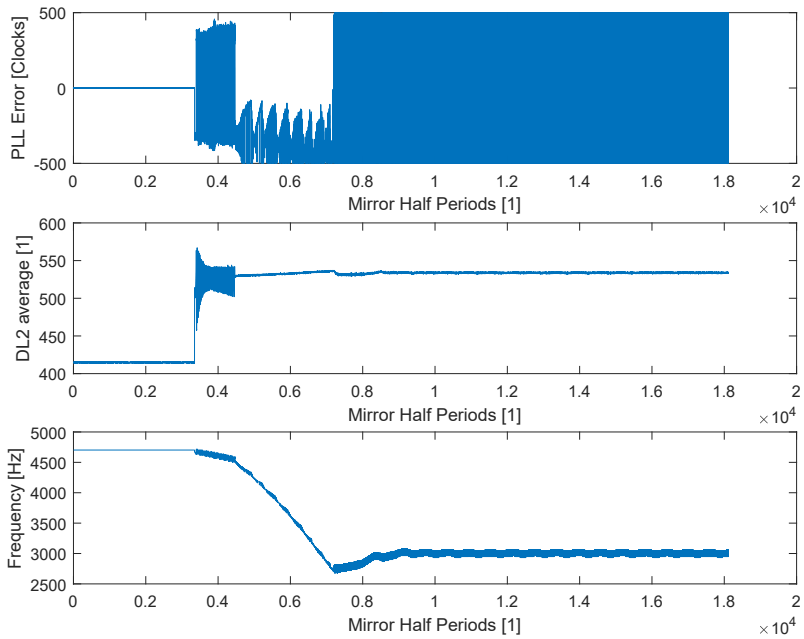

Figure 4.15: PLL loosing control of the MEMS mirror caused by a fatal shock of the LiDAR system [31].

- **Identifying Best Internal States**
  If there are no pre-saved internal states as well if the start-up procedure with the old pre-saved internal states are failing than the state-of-the-art procedure is starting the MEMS mirror and saves the internal LiDAR state signals into a non-volatile memory block.

- **Boost the Startup with Internal States**
  Starting the MEMS mirror with pre-saved values "kicks" the MEMS mirror directly into the right operational frequency [31].

Figure 4.16 depicts the startup process of the novel approach that will enable a faster and more safe startup routine. In the first section, the system is checking if the internal signals (jump frequency) and related signals are already available in the internal non-volatile memory. If they are not set then the system is proceeding with the state-of-the-art startup routine and detect the actual jump frequency and saves these parameters for future startup phases. If there are already startup values saved then the system is using the novel approach that is setting the LiDAR system into the Open-Loop mode with a intermediate frequency that is set before the real jump frequency. Based on the fact that the MEMS mirror is an analog component it is necessary to wait a specific amount of time that the mirror is able to settle. Afterwards, the controller is setting the jump frequency and it immediately will be able to operate as intended [31].

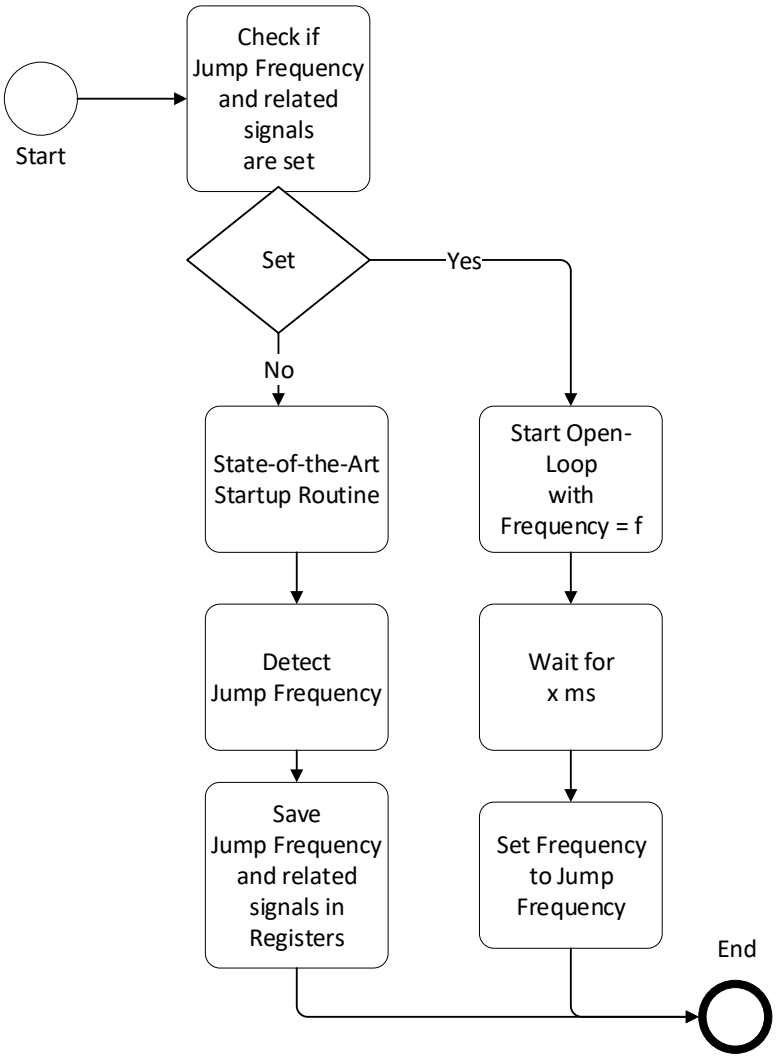

Figure 4.16: Flowchart of the novel start-up procedure that is integrated in the 1D MEMS Micro-Scanning LiDAR system [31].

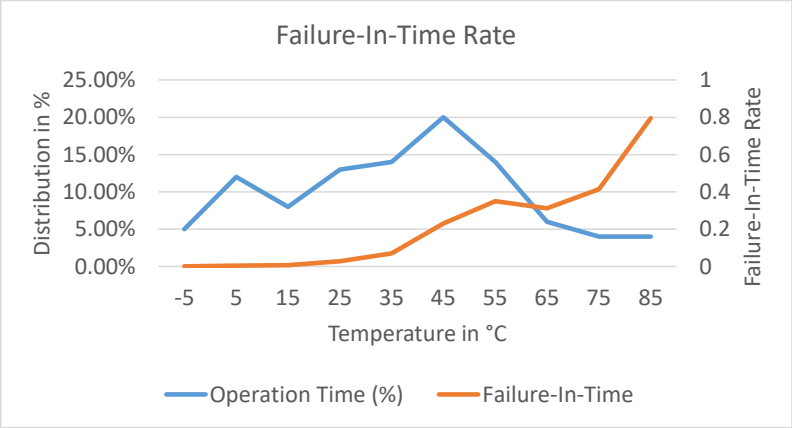

Figure 4.17: Temperature Distribution and the related FIT Rate [32].

4.3.4 Enabling Long-term State-of-Health Monitoring to detect Reliability Anomalies

Reliability is strongly connected to the exposed temperature of the electronic components that are mostly self heated through high power dissipation. The background information has already been introduced in Section 7.3 before. LiDAR will become one of the major enabler for automated driving, especially in case of SAE Automated Level 4 and 5. For this purpose, LiDAR needs to be highly robust and caused by the fact that at this high automation level there will be no driver available anymore to step in and take control of the vehicle. For that reason, novel systems needs to be as robust as possible and any failures caused by fatigue components must be detected in prior. In case of electronic components, this is the most challenging part because they fail without any prior signal and abruptly [32].

Figure 4.17 clearly shows the trend of the FIT Rate with higher temperatures and can be seen that with higher temperatures the Rate is increasing exponentially. This mathematical relation between the temperature and reliability enforces engineers and designers to use accurate Mission Temperature Profiles and any deviation could arise an ASIL degradation with the side effect that the component is not fulfilling requirements [32].

To prevent such cases, novel ADAS such as the LiDAR system should be monitored from a safety point of view to enable predicting reliability deviations. For LiDAR systems, this thesis introduces a novel approach that uses a temperature histogram to estimate the current and future reliability values. The values of the histogram can be used to determine the specific FIT Rate [32].

The main idea of the novel system approach is to use the FIT Rate as a credit system that can be consumed by the system. For that purpose, the system has to sample and record current temperature and save these values efficiently inside a histogram. This has

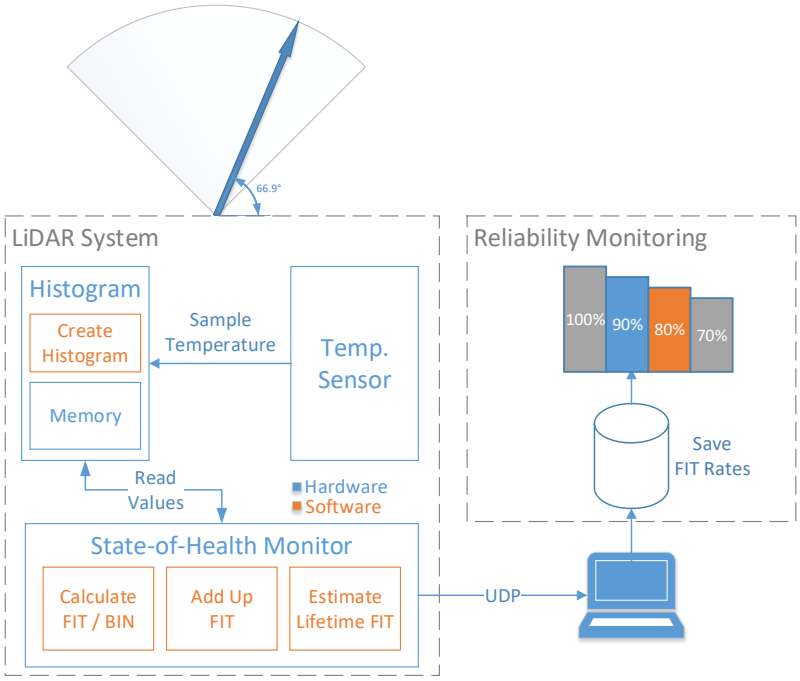

Figure 4.18: Conceptual System Architecture that will enable Live State-of-Health Monitoring for LiDAR system [32].

the big advantage that it requires less non-volatile memory caused by the fact that it will be summarized inside temperature classes. There is just the disadvantage that the chronological information is lost but in this use case it does not has any effect. The saved values can be used to calculate the current "used" FIT Rate and the expected FIT Rate of the whole lifetime. This also provides the possibility of introducing a ratio between the approximated and determined FIT Rate that instantly can express if the system reliability has dropped or not [32].

The Live State-of-Health Monitor is integrated inside the LiDAR system and the related Reliability Monitoring will be processed externally. Figure 4.19 shows the conceptual system architecture of the live state-of-health monitor integrated inside the LiDAR system and the related external reliability monitoring tool. The LiDAR system is integrating a temperature sensor, the Histogram module that is creating and saving the values inside a non-volatile memory module and the State-of-Health Monitor block that is able to estimate the lifetime FIT Rate. The external Reliability Monitoring tool is connected via User Datagram Protocol (UDP) and the specific data can be viewed live inside a specific GUI. A more detailed process overview can be depicted in Figure 4.19 and consists of the following steps [32]:

- **Save Temperature Values**
  The LiDAR system is continuously sampling current temperature of the semiconduc-

tor chip and saves these temperature values inside a non-volatile memory module. The temperature will be classified into specific temperature ranges that are determined through the histogram ranges [32].

- **Fetch Histogram Data**
  Transmitting the current histogram data from the non-volatile memory module to the Reliability Monitoring tool over UDP protocol [32].

- **Determine FIT Rate**
  The FIT Rate is an reliability indicator and can be calculated with specific mathematical equations such as the Arrhenius Equation. The reliability monitor is using the FIT Rate as a credit system that can be consumed by the semiconductor chip. If the chip has higher temperatures as intended than the consumption of the credit will be increased and the end of life will be reached sooner. The exact calculation is divided in the calculation of the Time Span of the Histogram Bins this means to calculate the run-time of the device at specific temperatures. Afterwards the FIT Rate for each temperature range will be calculated with the assumption that the system was running at this specific temperature from the beginning until now. Afterwards, the specific run-time of each temperature bin will be considered and the related FIT Rates of each bin will be summed up to the final FIT Rate that is representing the current consumed credit. This value can be used to estimate the expected lifetime FIT Rate that will give a feeling about if the component was overstressed or not. This value can be used to compare it with the theoretical lifetime FIT Rate that was determined during the design phase [32].

This approach enables an early detection of mismatches between the desired temperature profile and the real temperature profile. In case of deviations, suppliers are able to provide software or firmware updates to get rid of temperature deviations and to ensure a safe operation until end of life [32].

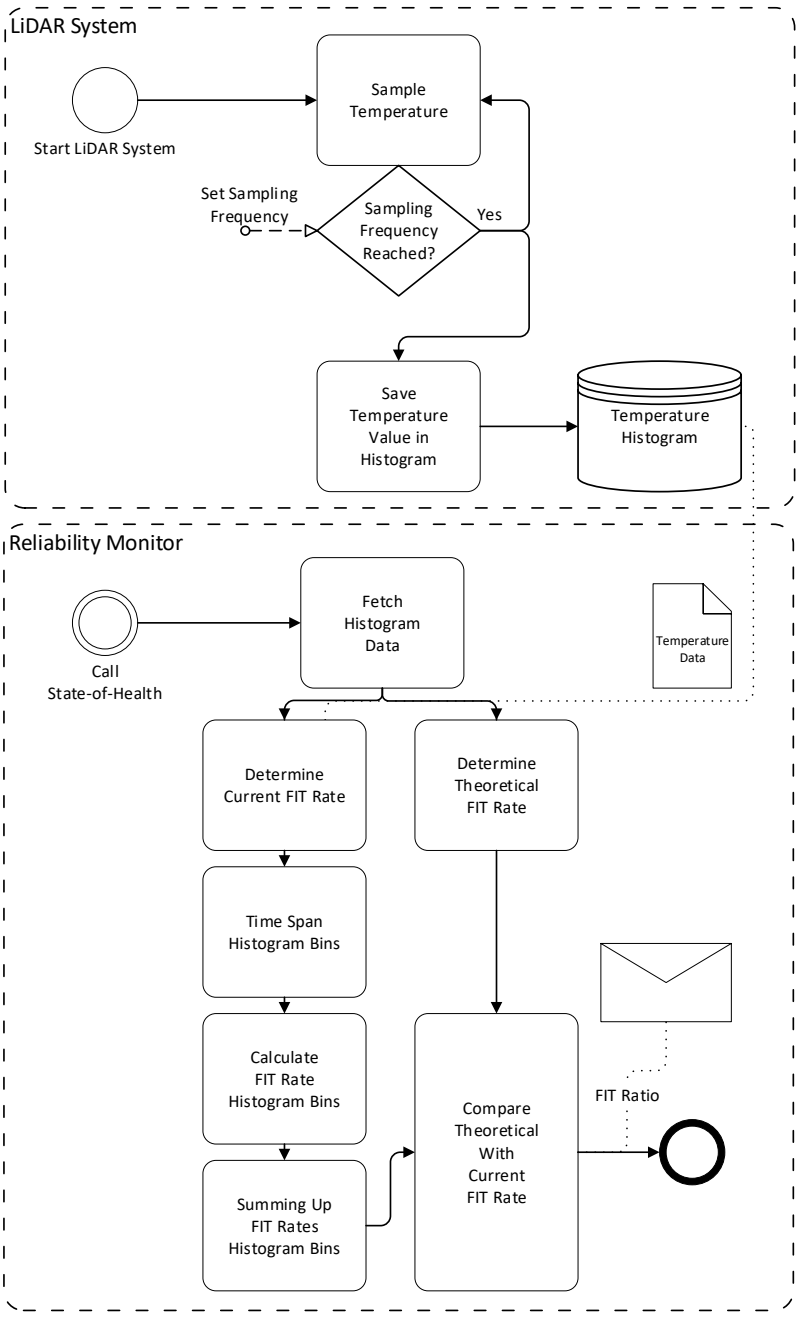

Figure 4.19: Flowchart that is describing the logical flow of the state-of-health safety monitor inside the LiDAR system [32].

Chapter 5

Evaluation and Results

5.1 Methodologies

This Chapter describes the Evaluation and Results of novel methodologies with the focus on supporting engineers and safety managers of developing fully-automated vehicles on SAE Automated Level 4 and 5. The methodologies are in compliance with the ISO 26262 standard. This Chapter also provides the practical results of the safety measures that have been introduced on a system level in Section 4.3.

5.1.1 Hardware Reliability Evaluation (FITness Assessment)

The hardware reliability evaluation is necessary for the novel HW/SW Co-Design methodology that was introduced in Section 4.2.2. The main idea of the whole design process is to optimize safety-critical systems on reliability. To enable a comparison between two independent implementations it is necessary to quantify the reliability on each implementation. The FITness Assessment [27] is one of the first methodologies that is able to quantify the reliability of hardware components and enables the comparison of different implementations as well as to choose the most reliable one [27].

For evaluating the effectiveness of this new methodology, I have used two Error Correcting Code (ECC) algorithms: Hamming-Code and Bose-Chaudhuri-Hocquenghem-Codes (BCH). Both algorithms are widely used for correcting and detecting bit-flips in memory segments [27].

Implementation

Figure 5.1 gives an overview of the general framework that was used for validating two ECC algorithms. The framework is separated into two parts. The ECC algorithm that is under test and the overall testbench that is triggering the ECC module and the validation of the

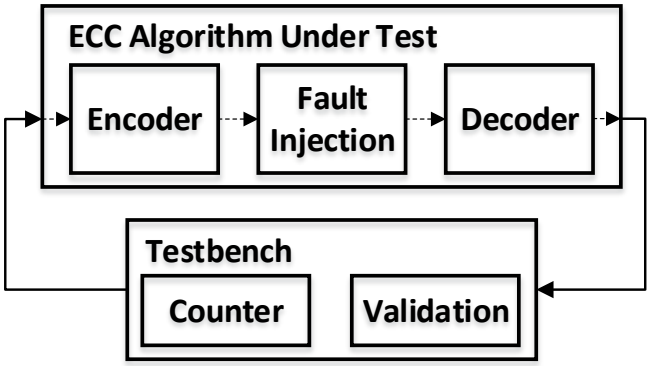

Figure 5.1: Overview of the general framework that was used for validating two ECC algorithms [27].

output results. The main focus of this framework was to provide a general module that is able to replace the ECC algorithm without any major changes because this decreases measurement deviations caused by implementation details. The ECC Algorithm Under Test module consists of three sub-modules. The Encoder and Decoder part represent the mathematical definition and procedure of the individual algorithm and the Fault Injection module is simulating bit flips that can be triggered by Single Event Upset (SEU) [27].

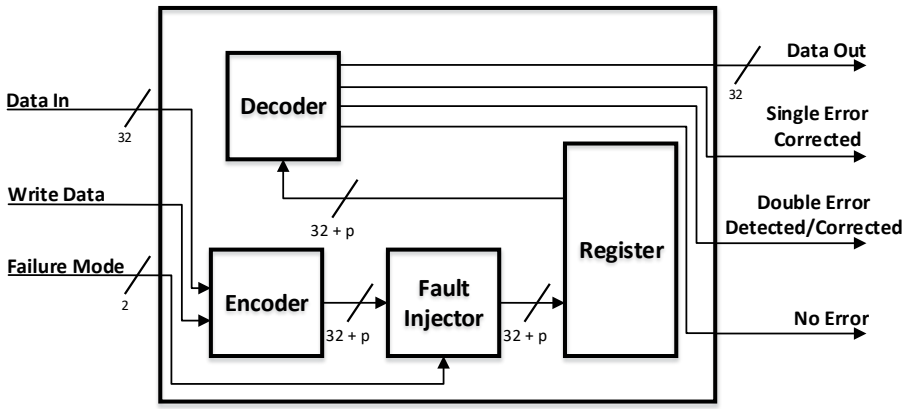

Figure 5.2: Pin configuration of both ECC algorithms including an overview of functional blocks inside [27].

The system architecture of the ECC Algorithm Under Test module can be seen in Figure 5.2. Both algorithms are using 32 bit data size. The Failure Mode pin allows the configuration of the amount of failures that will be triggered: Nothing, Single, Double, Triple Error Injection. The processed data will be saved in a register that will be read from the Decoder block. The Decoder is connected to several output pins that can signalize single error correction, double error detected/corrected and no error occurred as well as the data block [27].

Test Setup

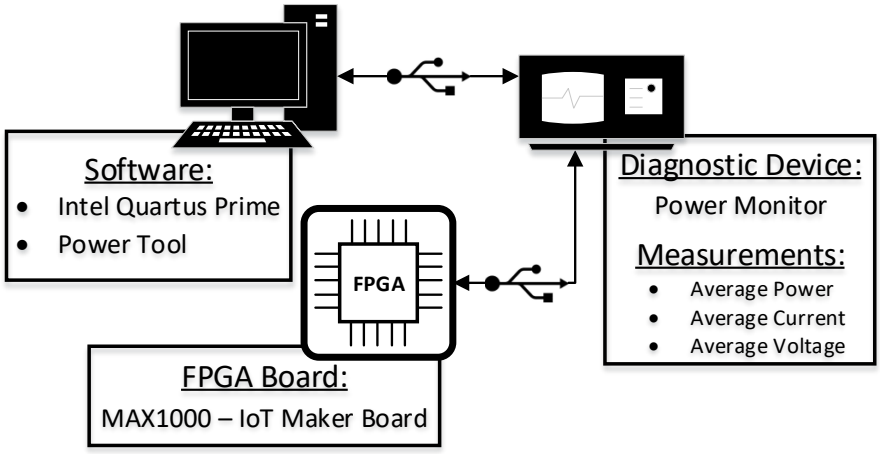

Figure 5.3: Overview of the measurement setup for evaluating the FITness Assessment algorithm [27].

Figure 5.3 shows the overall setup of the measurement process. The main controller was the FPGA board MAX1000 that had the big advantage that it had a small amount of additional hardware components and therefore lower additional power dissipation caused by additional chips. Another big advantage was the availability of reliability data inside the datasheet. On the software side the Intel Quartus Prime software was used to program the FPGA board as well as to extract data such as the amount of logical blocks that were used, and the Power Tool that is necessary to use the Mobile Device Power Monitor equipment. The Mobile Device Power Monitor equipment is able to measure the current, voltage and power dissipation [27].

Results

The test run was performed with the Hamming-Code as a Single Error Correction and Double Error Detection algorithm and the BCH code that represents a Single Error Correction and Double Error Correction algorithm. The first algorithm, the Hamming-Code, used 45 logical elements and had an average power dissipation of 571.78 mW. The second algorithm had about 65 logical elements and a power dissipation of 599.05 mW. Both algorithms were tested on the same platform at the same temperature. As a next step, with the help of the Arrhenius Equation and the Derating Factor a simulation at a specific temperature range was performed [27].

The results of the test run between the Hamming-Code and the BCH algorithm can be depicted in Figure 5.4. The simulation was performed on temperatures between $-40°C$ and $120°C$. It can be shown, that with higher temperatures has the Hamming-Code a

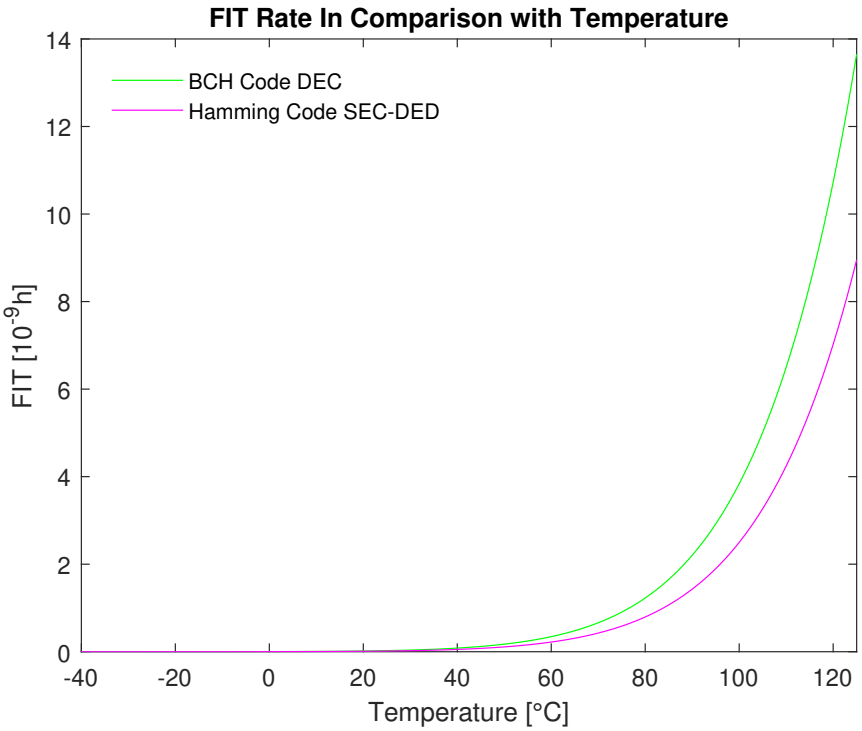

Figure 5.4: Results of the FITness Assessment algorithm using the Hamming-Code and BCH at different temperature [27].

higher reliability than the BCH code. This is resulted through the fact that the BCH has higher power dissipation and requires more logical blocks [27].

The experiment clearly shows that the FITness Assessment is an effective way to quantify the reliability of specific algorithm implementations. The methodology can be used to compare different implementations and enables engineers to choose the most reliable one to extend the MTBF and also harden safety-critical automotive systems. Especially for future fully-automated vehicles this methodology can be used to optimize these systems on reliability.

5.1.2 Software Reliability Evaluation (ProFIT Assessment)

Determining reliability of software components is not possible because software never gets old. Therefore, software will work every time the same as long as the hardware is working flawlessly. In this thesis, when I am talking about software reliability I am talking about how software is affecting the hardware. Different software implementations will use a different amount of hardware components considering memory, CPU processing time as well as some co-processors. This directly leads to the point in which an engineer can positively influence the power dissipation and this is directly related to the FIT Rate [26].

This Section describes the experimental results of the methodology that was described in Section 4.2.2.

Implementation

For Evaluating the ProFIT Assessment, I have used the MSP430 FR5969 microcontroller. This board contains additional analog circuits on the board to measure the power dissipation of the controller.

For comparing different algorithms, I have used six different sorting algorithms that are widely used in the field of Computer Science [26]:

- Binary Insertion Sort
- Heapsort
- Insertion Sort
- Megasort
- Quicksort
- Shell Sort

For the implementation the same approach as in the FITness Assessment was used. I employed a general framework in which all sorting algorithms can be exchanged without further major changes. This guarantees that the measurement results are not framework related [26].

Results

Based on the fact that software is dividing complexity into sequentially executed tasks also means that the power dissipation will vary over time as well as take different time to complete. Figure 5.5 clearly shows that effect with different timings between implementations as well as different spikes on power dissipation. It can clearly be seen that

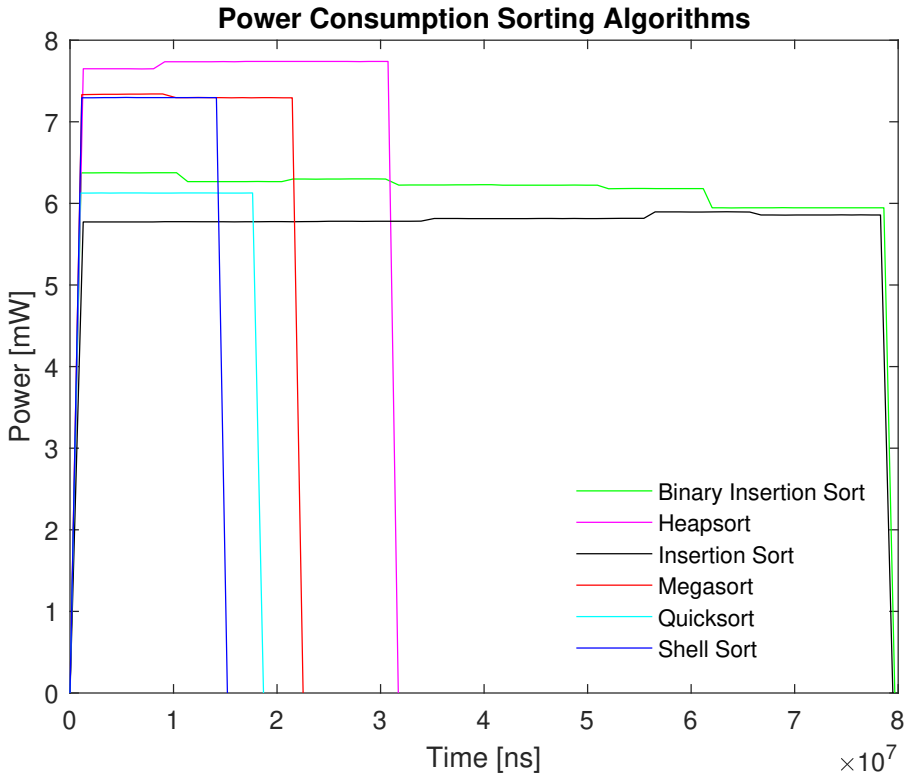

Figure 5.5: Results of the power dissipation of six different sorting algorithms implemented in C [26].

Table 5.1: Overview of the Power Consumption measurements of all C implemented sorting algorithms at 25°C ambient temperature [26].

	Average Power in mA	Energy in uJ	Time in ms
Binary Insertion Sort	6.18	438.2	77.53
Heapsort	7.72	178.4	31.71
Insertion Sort	5.82	440.0	79.48
Mergesort	7.31	124.8	22.52
Quicksort	6.12	60.7	18.69
Shell Sort	7.30	58.5	15.20

each algorithm needs different time and also has a specific power dissipation related to the amount of memory that it requires to solve the specific order task. The fastes algorithm was the Shell Sort algorithm that took about 15.2 ms and the slowest was the Insertion Sort with 79.48 ms. The average power of the Shell Sort was 7.3 mA and a overall energy consumption of 58.5 uJ. The Insertion Sort just used about 5.82 mA with a full Energy consumption of 440.0 uJ [26].

Applying the ProFIT Assessment on these two algorithms results in a FIT Rate of

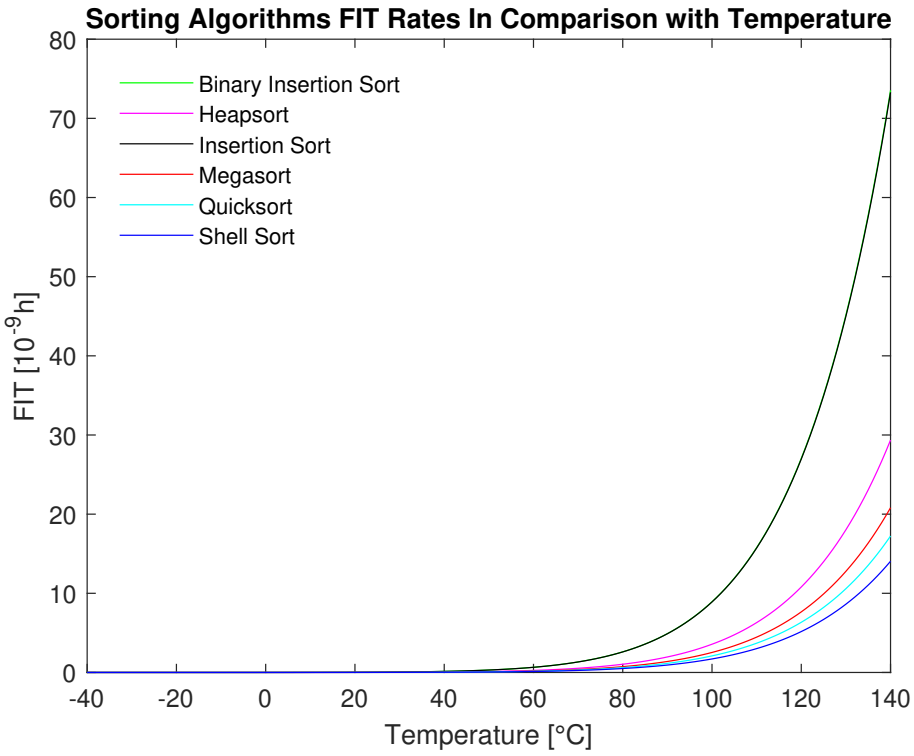

Figure 5.6: Results of the ProFIT Assessment algorithm using six different sorting algorithms implemented in C [27].

Table 5.2: Results of the algorithm FIT Rates calculation of the implemented sorting algorithms on the MSP430 FR5969 micro-controller board [26].

	FIT Rate in 10^{-9}
Binary Insertion Sort	1.87204922
Heapsort	0.747313371
Insertion Sort	1.865387949
Mergesort	0.529712728
Quicksort	0.438742916
Shell Sort	0.357627573

0.35 for the Shell Sort and 1.86 for the Insertion Sort as seen in Figure 5.6. This directly leads to the fact that the Insert Sort will affect the hardware components more and this also means that the reliability will decrease when using this algorithm [26].

These results clearly show that the ProFIT Assessment is working as intended and that engineers are able to compare the reliability of different software algorithms on hardware components. Based on the fact that most of the functionalities and control systems are already implemented as software modules raises the need of investigating the affect of different software algorithms but also future software updates on hardware reliability [26].

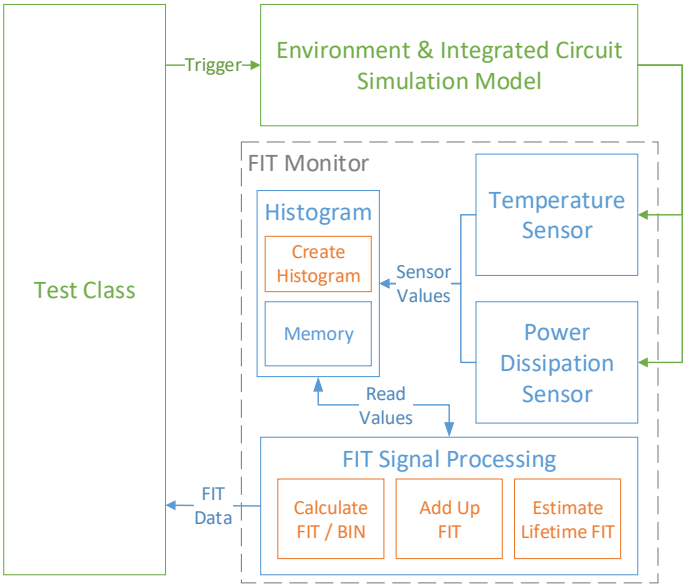

Figure 5.7: System architecture of the "RetroFIT" methodology that is used to monitor the current live safety of a LiDAR system [28].

5.1.3 Live State-of-Health Monitor (RetroFIT)

Live state-of-health monitoring is one of the key enabler for predictive maintenance as well as dynamic safety. The monitor is able to detect mismatches between the desired mission temperature profiles and the real profiles. But also the detection of reliability anomalies caused by software and firmware updates [28].

The idea and concept of a live state-of-health monitor was introduced in Section 4.2.3. The main idea is to continuously record the actual temperature on the semiconductor chip because temperature is one of the most crucial physical force that is decreasing the reliability of the chip [28].

To evaluate the feasibility as well as the effectiveness of a state-of-health monitor I have implemented the theoretical concept in a SystemC model as seen in Figure 5.7. The SystemC model is divided into three parts [28]:

- **Test Class**
  The Test class is instantiating all other modules and is triggering the Environmental Simulation module. Additionally, the module also is receiving the FIT Rates from the FIT Monitor module. The received values will be saved as a CSV file and can be further processed in Matlab.

- **Environmental and Integrated Circuit Simulation Model**
  This module represents the environmental conditions expressed as temperature in ∘C as well as the junction temperature and power dissipation of the chip.

- **FIT Monitor**
  The FIT Monitor module represents the main processing module that is actively measuring the temperature, as seen in Figure 5.8, and power dissipation with internal sensor classes and processes these values to the histogram class as seen in Figure 5.9. The histogram class is saving the data inside a memory by categorizing the actual temperature sensor values into temperature ranges. For enabling efficient memory usage, the temperature value will be saved inside a specific temperature bin of the histogram. The FIT Signal Processing module reads all the data of the histogram memory block and is calculating the estimated lifetime FIT.

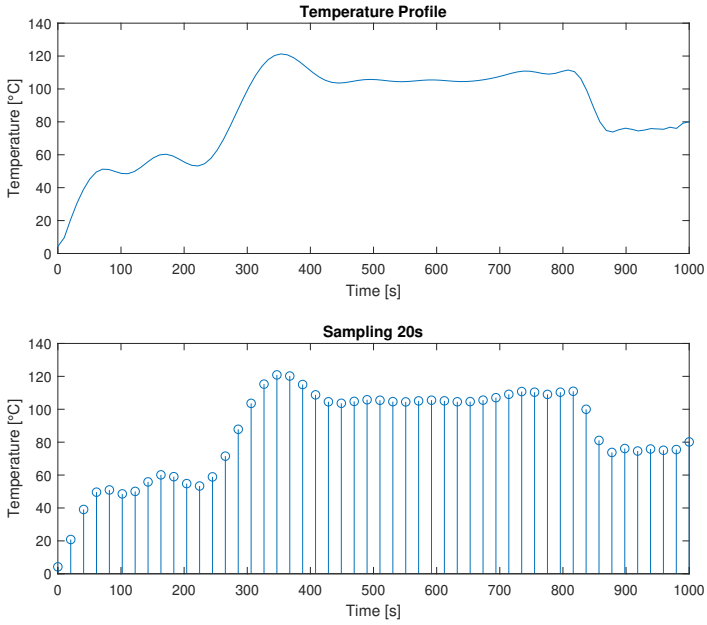

Figure 5.8: Temperature Mission Profile and Sampling results of the "RetroFIT" monitor [28].

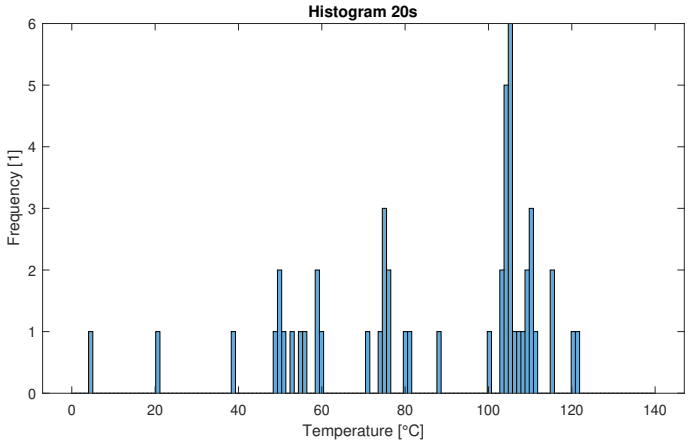

Figure 5.9: Histogram results of the "RetroFIT" monitor [28].

Table 5.3: Results of the SystemC simulation with the temperature mission profile that can be depicted in Figure5.9 [28].

	$\mathbf{FIT_{TS}}$	$\mathbf{FIT_{TTS}}$	$\mathbf{FIT_{LT}}$	$\mathbf{FIT_{RB}}$	$\mathbf{FIT_{Ratio}}$
FIT in [1]	2.36E-9	2.111E-9	8.5	7.6	1.118

Table 5.3 shows the processed data of the simulation model. The most important factor is the FIT Ratio that is directly showing if the current treatment of the chip was in compliance with the mission temperature profile or if the chip was overstressed. For this purpose, the monitor calculates the theoretical FIT Rate until this moment and the real FIT Rate according the temperature progression. The higher temperature progression can be seen through the ratio that is higher than 1. In case of a temperature regression that is lower than the mission temperature profile would result in a ratio that is below 1. If the actual temperature would be interpolated to the end of life of the system than we would have a FIT Rate of about 8.5 instead of 7.6. In this case, it would be no big problem at all but it could be the case that for some safety-critical systems that are ASIL D certified could result in an ASIL degradation when they reach a FIT Rate value higher than 10.

5.2 Safety Enhancements LiDAR

The second part of the Evaluation and Results chapter discusses and presents the results of enhancements and novel approaches of the 1D MEMS Micro-Scanning LiDAR platform that was implemented in a prototype platform that was introduced in Section 7.3.

5.2.1 LiDAR Synchronization of Master-Slave Compound

The synchronization of two or more independent MEMS mirrors is necessary to reduce the probability of interferences caused by crossing laser emitting signals at the receiver part of the 1D MEMS Micro-Scanning LiDAR system as described in Section 4.3.1.

Figure 5.10 depicts the internal signals of the slave mirror that is adapting his own frequency on the master mirror. The whole experiment is divided into three parts [29]:

- **Start-Up Phase**
  This phase is necessary that the master and slave mirror reach the top resonance curve and the MEMS mirror is working as intended.
- **Asynchronous Mode**
  In this phase both MEMS mirror are controlled independently on their own PLL.
- **Synchronous Mode**
  In this final step the slave MEMS mirror will receive the zero-crossing signal of the master mirror and matches his own frequency to the frequency of the master by using the interl slave PLL.

Figure 5.12 depicts a more detailed diagram of the synchronization step. It can be seen that at the moment of synchronization is rising the PLL error and the Sync Error. At the frequency diagram it can be seen that the slave mirror is increasing his frequency step-by-step. With each step, the total synchronization error is decreasing until the point is reached where the slave and the master mirror is running at the same frequency [29].

Table 5.4 gives the detailed measurement results of the starting frequency difference of about 229 Hz and the desired frequency of 4620 Hz. The amount of time of the synchronization process took about 125 ms [29].

Figure 5.12 shows the zero-crossing signal of the slave and of the master on an oscilloscope. In the left picture the asynchronous mode can be seen in which both signals are not properly aligned. In the right picture it can be seen, that with the synchronization both mirrors are working at the same frequency as well as at the same angle [29].

Table 5.4: Overview of the synchronization time results between two LiDAR systems working in a Master-Slave compound [29].

	t_{Start} **in [1]**	t_{Stop} **in [1]**	t **in [ms]**	f_{Start} **in [Hz]**	f_{Stop} **in [Hz]**
Master	-	-	-	4620	4620
Slave	20500	21700	125	4391	4620

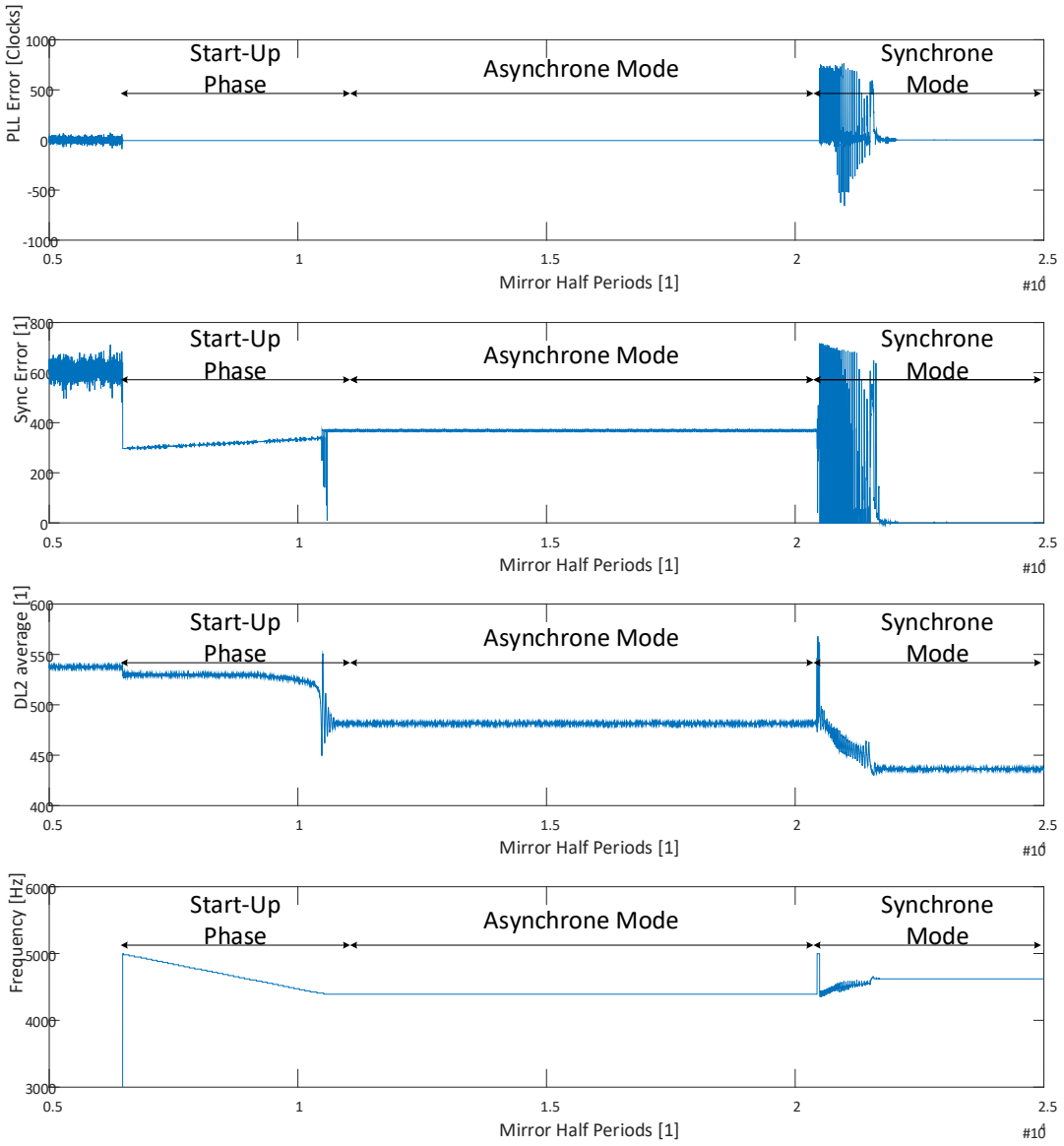

Figure 5.10: Results of the Master-Slave synchronization scenario from the Slaves point-of-view including the asynchronous part [29].

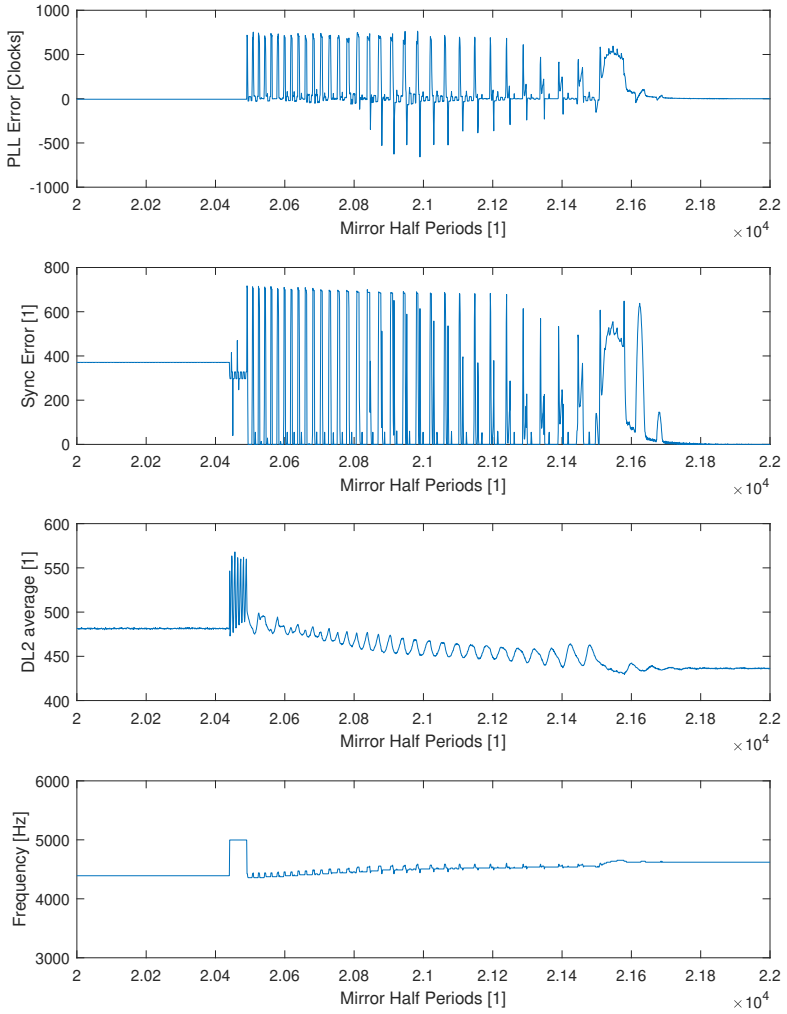

Figure 5.11: Synchronization details of the slave [29].

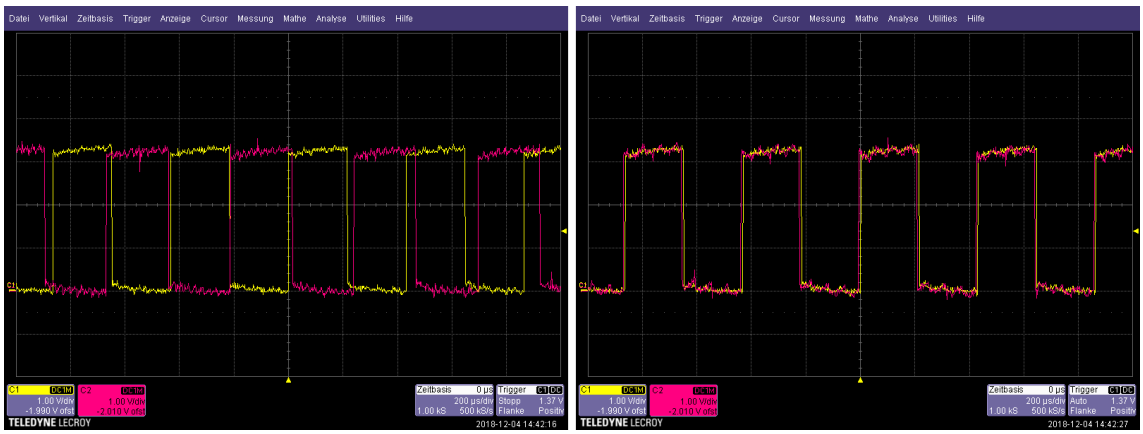

Figure 5.12: Oscilloscope Measurement Figure that clearly shows the synchronization (right) between the Slave and Master [29].

5.2.2 Fail-Operational LiDAR System

The following Sub-Section represents work that was done by Felix Warmer during his master thesis [33] at the Institute of Technical Informatics. My part was to support his work concerning safety aspects. Further information can be found in his Master Thesis.

Due to the fact that with SAE Automated Level 4 and 5 will be no driver available anymore to take over the control of the vehicle leads to the need of fail-operational behavior instead of the traditional fail-safe. As already described in Section 4.3.2, is the temperature and latent faults of volatile memory one of the most crucial aspects during operation time [30].

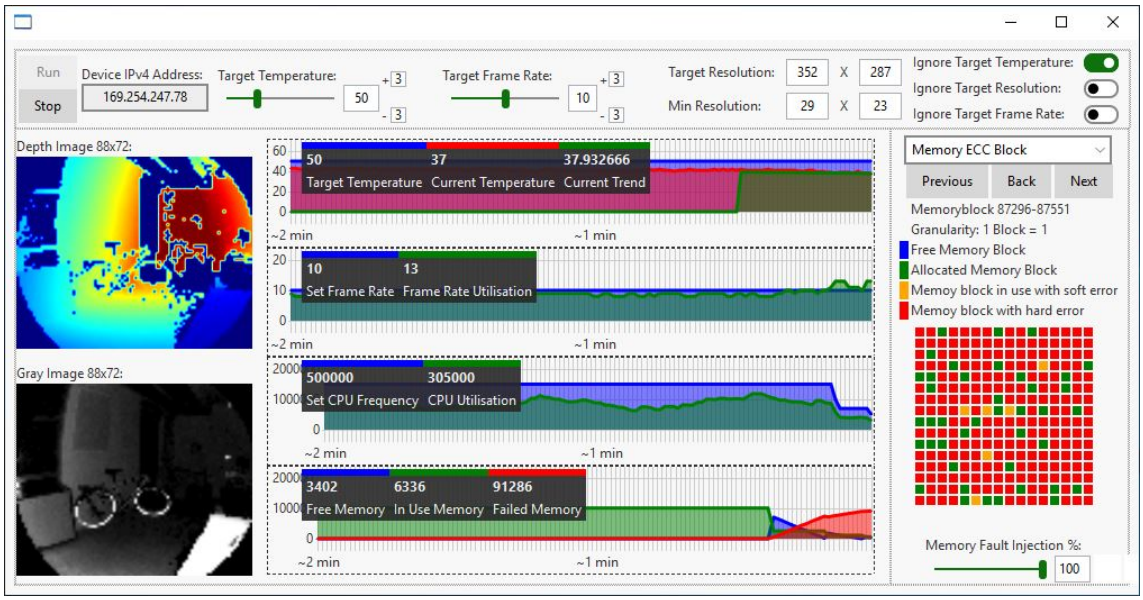

Figure 5.13: Overview of the control interface of the novel Fail-Operational 3D Flash LiDAR system showing live data, settings and related monitoring results [30, 33].

Figure 5.13 depicts the GUI of the novel fail-operational LiDAR system architecture. The main idea was to control the temperature of the whole system as well as the protection of the memory block in prior as well as the deactivation of corrupt memory blocks. Inside the GUI there can be a target temperature and a target frame rate set. With specific buttons the exact scenario can be set such as control the target temperature and dynamically change the CPU frequency and frame rate to comply with these settings. The graphs continuously show the current system state and allows an easy and fast review of the parameters. On the left side, the current output of the 3D Flash LiDAR can be seen with the depth image at the top and the gray image at the bottom. The memory fault module is depicted on the right side which supports fault injection inside the memory. The fail-operational LiDAR system architecture will automatically decrease the image

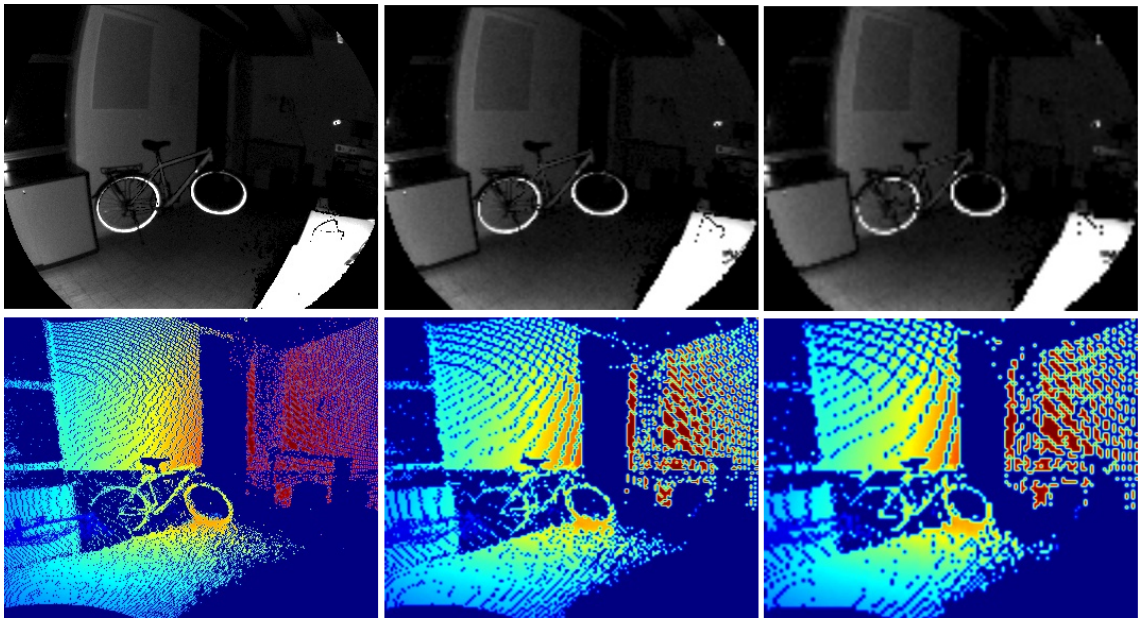

Figure 5.14: Live results of the 3D Flash LiDAR system showing the degradation of the image quality that is reduced from 352x287 to 118x96 [30, 33].

resolution of the point cloud as seen in Figure 5.14 [30, 33].

The current implementation also contains a simulation mode in which a specific test track can be set with country roads, urban city streets and highways. The system will be configured to meet a specific requirement such as keeping a specific temperature range and the system will dynamically change all other parameters to meet the specification. Figure 5.15 shows a test run between Graz and Hartberg with the goal to keep a specific target temperature. It can be seen that the system were able to meet this requirement. For this purpose, the system was dynamically changing the frame rate and the CPU frequency according the current road conditions [30, 33].

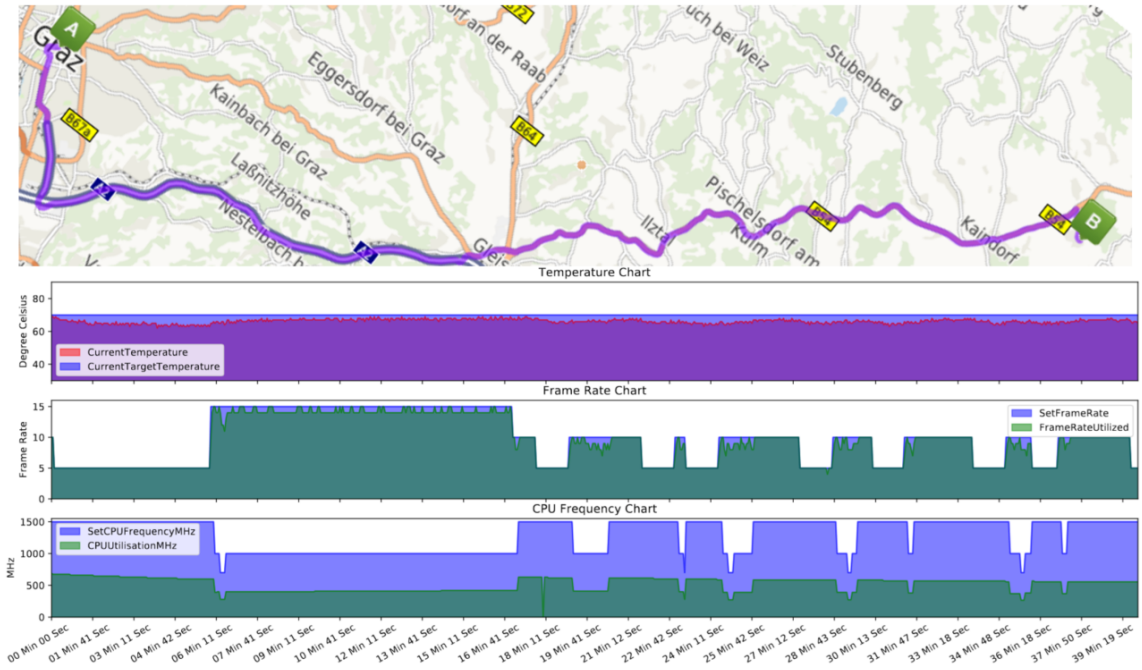

Figure 5.15: Overview of the testing scenario between Graz and Hartberg with the results of the monitoring tool [30, 33].

5.2.3 Speed-Up LiDAR's Transient Start-Up Procedure

Residual failures are the most threat regarding safety because they are not considered during the development cycle. They are occurring during run-time without any prior signalization. In case of automated driving of SAE Level 4 and 5 this could lead to deadly accidents. For that purpose, it is necessary to restart the whole system with the hope that the failure will disappear after a cold restart. The main problem considering a LiDAR system with MEMS mirrors is that it requires a certain amount of time until the mirror is at his specific operating point. For this purpose, the cold boot of the mirror needs to be as fast as possible to allow this procedure during operation time at high speed such on highways [31].

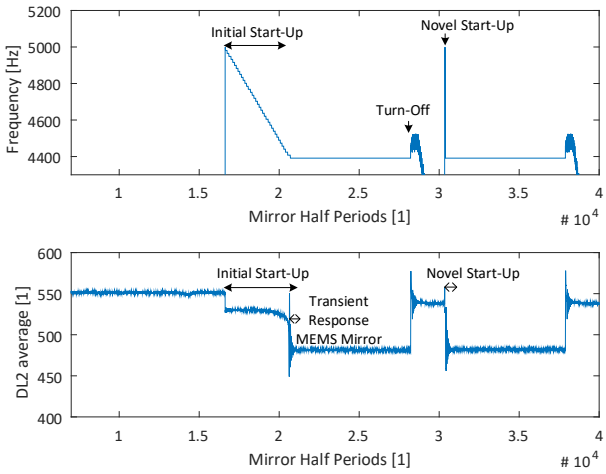

Figure 5.16: Initial Start-Up procedure of the 1D MEMS Micro-Scanning LiDAR system [31].

Figure 5.16 depicts the experimental result of the novel start up procedure of the 1D MEMS Micro-Scanning LiDAR platform. The state-of-the-art start up procedure took about 426.97 ms as seen in Table 5.5. After the initial start up phase the operating point values are saved in nonvolatile memory blocks and can be fetched at a cold restart. This can be seen in the right half of the diagram in Figure 5.16. This novel start up procedure just takes about 5.20 ms which results in the fact that at a speed of 100km per hours the blindness will be reduced from approximately 15m to 15cm [31].

5.2.4 Live State-of-Health Monitor

Reliability monitoring or Aging monitoring is already explored and as already mentioned in Section 7.3 there are many research publications available.

Section 5.1.3 describes the theoretical background and the methodology that will be used and implemented into the 1D MEMS Micro-Scanning LiDAR prototype platform.

Table 5.5: Comparison between the traditional start-up procedure and the novel procedure with measurement results [31].

	Begin	End	Time in ms
State-of-the-Art Start-Up	11590	7491	426.97
Novel Start-up	25610	25560	5.20

One of the most important requirements was the industrial compatibility regarding costs and compliance with the current safety standards especially the ISO 26262 standard. First I have analyzed 15 different research publications [16, 75, 76, 77, 78, 79, 80, 17, 81, 18, 82, 83, 84, 19] regarding blind spots as seen in Figure 5.17.

I have created 14 different categories to allow a comparison of the different publications:

- **Real Time**
  Capability of calculating and determining the current live state-of-health value or situation in real time.
- **ISO 26262**
  Describes if the current methodology or implementation is compliant with the automotive ISO 26262 safety standard.
- **Digital**
  The live state-of-health monitor can be integrated as analog circuit or fully integrated in digital logic.
- **Computation Efficient**
  Describes if the algorithm that are used computational efficient that is necessary if the algorithm is implemented in battery supported devices.
- **Memory Efficient**
  Memory efficiency is important because in the semiconductor industry equals area directly money and it is necessary to reduce the amount of space.
- **Configurable**
  Capability to configure the live state-of-health monitor regarding intended purpose.
- **Temperature History**
  Competence of saving the history of the temperature progression.
- **Chronological**
  Capability of the chronological order of the temperature history.

- **FIT Value**
  The automotive industry is using the FIT Rate as quantified value for reliability. This describes the possibility of estimating the FIT Rate regarding the usage profile of the system.

- **ASIL Evaluation**
  FIT Rates are directly connected to the ASIL level. The evaluation enables the possibility of detecting ASIL anomalies such as degradation caused by higher utilization.

- **Utilization Degree**
  Describes a value of the actual utilization regarding temperature history and if the component was already overstressed.

- **Portability**
  Capability of integrating the implementation or idea to other systems.

- **Temperature Sensors**
  Describes if the idea or methodology is using temperature sensors and therefore the Arrhenius equation.

- **Other Sensors**
  Describes if the methodology is using additional other sensors for reliability estimations.

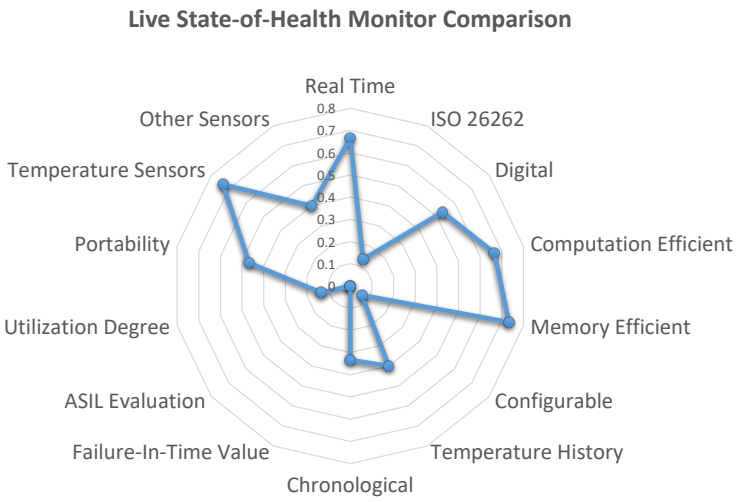

Figure 5.17: Comparing 15 different research publications from academic and industry regarding live state-of-health monitoring to detect blind spots.

Figure 5.17 describes the current situation of live state-of-health monitors in industrial and academic publications. It can be seen that most of the current implementations and methodologies are relying on temperature sensors and just a few are also using other sensors. Most of them are implemented computational and memory efficient and are also implemented as digital logic. The least implementations are compatible with the ISO 26262 standard. Therefore, there is no high interest in evaluating the FIT Rate and the ASIL level [32].

	Thesis	Saab	STMicroelectronics	Cisco	Renesas
Live	✓	✓	✓	✓	✓
ISO 26262	✓	✗	✓	✗	✓
Digital	✓	✓	✓	✓	✓
Computation	✓	✗	✗	✗	✓
Storage	✓	✗	✗	✗	✓
Configuration	✓	✗	✗	✓	✗
Temperature Values	✓	✓	✓	✓	✗
Chronological	✗	✓	✓	✓	✗
FIT	✓	✗	✗	✗	✗
ASIL	✓	✗	✗	✗	✗
Utilization	✓	✗	✓	✓	✗
Flexibility	✓	✓	✓	✓	✗
Temperature Sensor	✓	✓	✓	✓	✗
Additional Sensors	✗	✗	✓	✗	✓

Figure 5.18: Comparing the Live State-of-Health Monitor of this thesis with the four most important research papers.

The four most important papers regarding live state-of-health monitoring are already described in detail in Section 7.3. Figure 5.18 gives a comparison between the novel introduced key concepts. It can be seen that the novel live state-of-health monitor that has been introduced in this thesis fulfills most of the concepts except the chronological order of the temperature progression as well as it just uses the temperature senors as single source for the reliability estimation. The usage of the temperature sensor fulfills the reliability methodologies that are used in the ISO 26262 standard and is therefore fully compliant with this standard. The chronological order is not necessary regarding that it makes no difference at which point the temperature was assigned to the semiconductor device. Comparing this novel concept clearly shows that the RetroFIT methodology is the only public available concept that enables dynamic safety by providing FIT Rates and ASIL Evaluation [32].

Figure 5.19 gives an overview of the experimental prototype of the Live State-of-Health Monitor that was implemented in the LiDAR prototype platform. The figure shows the GUI of the program that is running on the external device that represents the external reliability monitor. It can be seen that the utilization of the device is just 0.17 and therefore the semiconductor device could be optimized on a lower Mission Temperature Profile to reduce the amount of material costs [32].

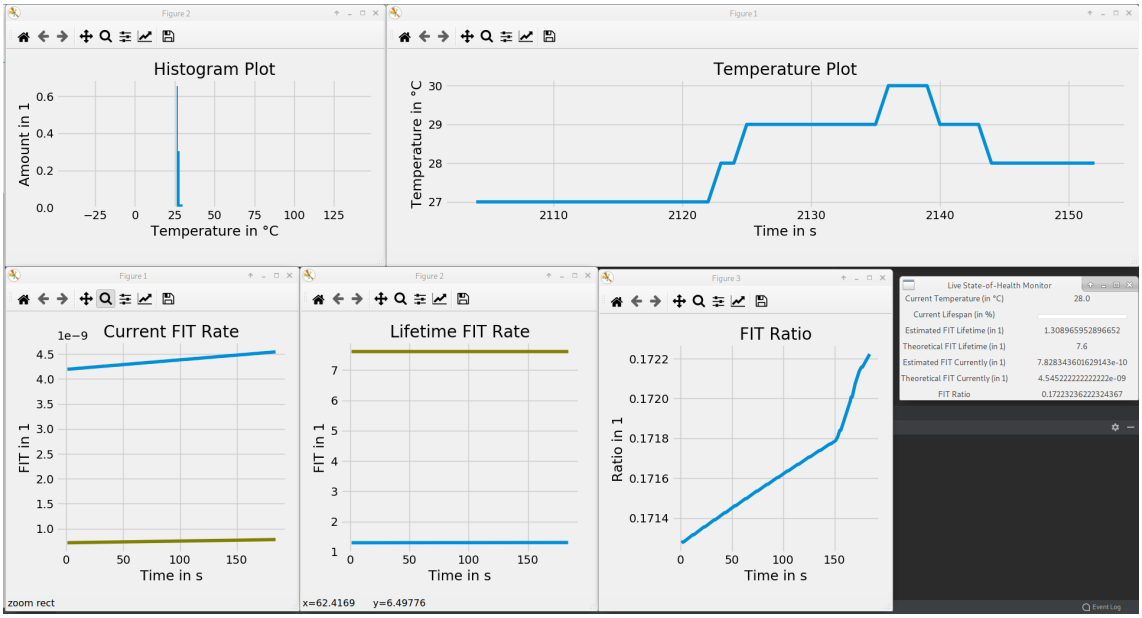

Figure 5.19: Overview of the GUI that is showing the current real time reliability data of the novel Live State-of-Health Monitor [32].

Chapter 6

Conclusion, Limitations and Future Work

6.1 Conclusion

This thesis describes novel approaches and methods to support engineers and safety managers in developing fully-automated vehicles that fulfill the requirements of SAE Automation Level 4 and 5. These automation levels are disruptively changing the automotive industry caused by the fact that traditionally the driver was the last backup instance in case of any unintended failure that is not recoverable. The circumstance that the driver will become a passenger and that the vehicle must be able to handle all situations on its own forces the industry to change its safety backup plans. The following challenges should be considered by the automotive industry in the next few years to master the technological change from SAE Automation Level 3 to 4 and upwards:

- **Introducing Fully-Automated Driving Systems into ISO 26262 Road Vehicle Safety Standard**
  The current ISO 26262 standard released in 2018 does not fulfill the requirements of SAE Automation Level 4 and 5 due to the fact that it still relies on the driver to control the effect of the failure as described in Section 1.3.1. Consequently, novel fully-automated vehicles must be optimized on safety and reliability, and robustness becomes one of the key factors for long-term safety of Embedded Systems.

- **Traditional HW/SW Co-Design Approaches does not emphasize on Component Reliability**
  HW/SW Co-Design is a design process of Systems Engineering and most of the time power consumption and costs are the most important factors during development. The change of reliability as the key factor for long-term safety leads to the need of

a novel HW/SW Co-Design approach that optimizes fully-automated driving systems on reliability. This thesis provides novel methodologies (FITness Assessment, ProFIT Assessment) that enables the quantification of reliability during development phases and provides the fundamental basis for the Safety-Optimized HW/SW Co-Design Process that is described in Section 4.2.2. These methodologies have been developed in the context of an academic fundamental research but can be seen as a base for a more sophisticated industrial compatible approach. My methodologies clearly show the feasibility of measuring component reliability at early development phases during the whole V-Model on different abstraction layers. This can be used to extend the Mean Time Between Failures value of safety-critical Embedded Systems. Especially in terms of developing novel systems such as LiDAR this methodologies can be used by the Industry to get a feel for the real FIT Rate and the desired FIT Rate and can proactively support the semiconductor industry in optimizing their processes or semiconductor material at an early stage, which could lead to lower overall development cost due to the fact that changes late in the development phase will affect the cost far worse.

- **Continuous Improvement of the Mission Temperature Profiles**
  Nowadays, reliability is considered as a given value after the development of a system. The highest impact on this given reliability value has the temperature change of a system. This is mathematically defined in the Arrhenius equation as described in Section 2.5. It can be seen that the relation between temperature and reliability has an exponential effect. Because of that the industry uses Mission Temperature Profiles, as described in Section 4.2.3, for dimensioning the intended systems on reliability. But these Mission Temperature Profiles could be designed as best-cases and this could lead to higher utilization of the system as initially intended. Until now, this was no problem, because the driver was the last safety instance and in case of prior failures the failure was controllable. But with fully-automated driving systems this will not be possible anymore. Therefore, the industry needs a feedback loop as described in the Blind Spot Analysis of Reliability Estimation in Section 3.3.5. This feedback loop monitors if the system is operating as intended or if changes to the behavior of the system or a replacement system is needed, in case of insufficient safety margins. Section 4.2.3 introduces and describes a novel safety monitor that is able to record the utilization of in each semiconductor chip and can predict the real FIT Rate based on the real usage. The monitor is also able to give the current reliability status of a single semiconductor chip, a system, a vehicle or a whole fleet. This is an enabler for Big Data in the context of safety, as described in Section 4.2.3, and can support OEMs and suppliers to optimize their systems to save cost or

to make their systems more robust in case of wrong Mission Temperature Profiles. The Live State-of-Health Monitor was implemented in a 1D MEMS Micro-Scanning LiDAR platform as described in Section 4.3.4.

- **Handle the Residual Risks with Robust Safety Hooks**
  The development of novel SAE Automated Level 4 and upwards vehicles will introduce novel automotive systems that have the ability to control several parts of the vehicle without any human control input. Considering all possible driving situations all across the globe, such as different road types, road conditions, weather, cultural behavior and traffic leads to the fact that there will be billions of possible situations and all of them can not be considered during the development phase. This will lead to the fact that there will be driving situations that have never been seen before by the system. In the worst case this could lead to unintended behavior of the system or to a total failure of the system and represents a residual risk for human damage. In case of residual risk that can still trigger a failure after a specific amount of operation time it is necessary to provide additional safety measures inside the LiDAR system to prevent deadly accidents. For the case of LiDAR this thesis introduces several safety enhancements as described in Section 4.3. In the automotive domain redundancy is one of the most powerful methods to enable fail-operational behavior. In case of failure of a single system, the second backup system will take over control and the normal user will not take any notice of this situation. To enable this option for the 1D MEMS Micro-Scanning LiDAR platform I implemented a synchronization of two independently controlled analog MEMS mirrors. This fundamental work represents the base for adding several MEMS mirrors inside a LiDAR system to increase redundancy. This thesis also introduced a novel system architecture that focuses on the compliance of a specific temperature range for the LiDAR system and a proactive protection of memory blocks with the possibility to disable specific memory blocks in case of failure that is enabling a fail-operational behavior for a LiDAR system. If there are still latent failures available that are not considered during the development phase which is always the case, the LiDAR system is equipped with a fast start up routine that is able to restart the whole analog MEMS mirror in about 5 ms, meaning that the system is able to restart fast enough to avoid problems due to long service outage of the LiDAR system.

In my Introduction I presented two research questions related to how reliability can be attested during development phase and what kind of systems must be integrated to detect and mitigate reliability deviations. With the research work that has been presented in Section 4 and the evaluation of Section 5 I could clearly show that with these novel methodologies and safety enhancements these two statements are possible. I have shown

with my work that the automotive industry is able to optimize their novel fully-automated systems on reliability and that any reliability deviations can be detected from the early development phase until decomposition.

Currently, the Semiconductor Industry is continuously improving the current safety processes and are homogenizing the whole industry with proven-in-use approaches such as the ISO 26262 - Part 11 Semiconductor Guideline. During my research work I have cooperated with Infineon Technologies Austria AG in Graz who have very sophisticated safety methodologies, processes and approaches. Some parts of this work such as the hardware and software quantification methodologies represent an academic approach that can not be directly integrated in the current industrial processes, because of the need of more experiments and studies regarding industrial experience. But there are also parts of this work that had a positive influence on their current work such as the fast transient start-up procedure of the LiDAR system that could be integrated in the commercial LiDAR MEMS Mirror Driver as well as the Live State-of-Health Monitor that triggered an internal discussion with the result that they are already working on this topic. This positive cooperation clearly shows that this work represents research topics relevant to the industry. The topics of this thesis will become more and more important over the next decades, due to the fact that current ADAS will evolve to the point in which SAE Automation Level 4 and 5 will be enabled for the whole vehicle driving functions. The methodologies introduced in this thesis can serve as a basis for discussion and should clearly show to the automotive industry that reliability becomes to the most important factor when developing fully-automated vehicles as well as reliability can be the key driving factor for these systems. This thesis represents one starting point with the goal of safe and robust automotive systems for automated driving. During my work I encountered that nowadays we are not able to develop safe fully-automated vehicles with the current methodologies. The methodologies presented in this thesis are hard to be implemented in the industrial automotive sector caused by the fact that it will increase the overhead of developing automotive systems, but they can show the right way to emphasize reliability of automotive systems.

6.2 Limitations

The methodologies and implementations introduced in this thesis are representing research work and therefore should not be applied directly in consumer products. The main purpose of these methodologies is to provide novel ideas to kick off discourse, especially on the need of optimizing safety-critical Embedded Systems on reliability, as well as experimental results to prove feasibility.

6.2.1 Methodology Limitations

HW/SW Co-Design Concept

The FITness Assessment and ProFIT Assessment methodologies that are used in the HW/SW Co-Design concept have been evaluated by applying use cases to each methodology. In this specific case, a single use case was enough to prove that different implementations result in different reliability values on the same hardware. Especially in case of software, these results were one of the first that depicted this circumstance and are meant to trigger a discussion about software and its effect on hardware regarding reliability. The methodology is working as intended and it is also compliant with the ISO 26262 standard. The biggest concern is, that semiconductor manufacturers must provide meaningful base FIT rates. A wrong base FIT Rate leads to a wrong output of both methodologies as well as the overall HW/SW Co-Design approach. This fundamental problem can not be solved by these methodologies. Instead it must be solved by specific standards such as the IEC 62308 as well as increasing the overall understanding of novel semiconductor processes regarding reliability of their products.

Live State-of-Health Monitor

The reliability monitor introduced in this thesis represents a novel idea that could be an enabler of dynamic safety evaluation during run time. The methodology uses the temperature as the key resource for reliability evaluation caused by the fact that the ISO 26262 and IEC 62308 are also using this physical quantity as key indicator for hardware reliability. But there are also other physical effects that have a high impact on the overall reliability such as mechanical forces, vibrations and fast cyclic temperature changes. Another case that has to be discussed is the case in which the reliability monitor should also record the temperature on the semiconductor chips when the vehicle is not running. Additional tests are required to evaluate the effects of environmental temperature changes on semiconductor chips when using this special reliability monitor.

6.2.2 Safety Implementations

The novel safety implementations that were integrated in the LiDAR prototype platform represent research work and should not be integrated directly into consumer products. One of the reasons is that not all safety cases have been considered and therefore there could be residual risk that has not been mitigated.

Synchronous MEMS Mirrors

The current implementation of controlling two independent MEMS mirrors synchronously represents a feasibility study and does not provide enough robustness for real products. During experiments I found that in special situations the PLL of the Slave mirror driver loses control of the MEMS mirror. This is caused by the Master mirror driver that is changing the frequency of the Master MEMS mirror. This triggers the Slave PLL to change the operational point of his own mirror and without the feedback of the Slave MEMS mirror the PLL of the Slave is not able to keep up with controlling the oscillation.

Fail-Operational LiDAR System

The current experimental prototype is using a 3D Flash LiDAR system that is limited in range, resolution and frames per second. The current system also represents a feasibility study that shows how temperature deviations and memory faults can be mitigated or prevented. Therefore the prototype can not be placed on a vehicle.

Start Up Procedure LiDAR

The start up procedure that has been developed for the 1D MEMS Micro-Scanning LiDAR system represents the most robust work of this thesis and can directly be integrated in a consumer product.

6.3 Directions for Future Work

As already mentioned, most of the work that has been done in this thesis was evaluated at an early research stage and often represents a proof of feasibility. Therefore, there are opportunities to evolve the current methodologies and safety enhancements of the LiDAR system:

- **Safety-Optimized HW/SW Co-Design Process**
  - Integrating a simulation based model that is estimating the base FIT Rate of the intended system functions.
  - Also consider from scratch ASIC implementations in the FITness Assessment methodology.
  - Integrate a novel methodology that is able to derive power consumption profiles from basic CPU control instructions and automatically analyze the resulting FIT Rate.
- **Live State-of-Health Monitor**
  - Continuous temperature recording of the semiconductor devices regarding non-operating hours of the vehicle.
  - Adding additional sensors such as vibration sensors to extend the trustworthiness of the derived reliability data.
  - Perform a case study with real semiconductor chips in the field and analyze the data over several years to build up a database for big data analysis. This data can be used to detect high utilization patterns that can be used to detect failures in prior and to enable predictive maintenance.
- **Safety Enhancement Implementations LiDAR**
  - Extend the current Master-Slave synchronization module with additional safety monitors as well as introducing a novel concept that is controlling the mirror on the slave side in a robust way.
  - The Fail-Operational LiDAR System should be equipped with the 1D MEMS Micro-Scanning LiDAR system that provides the range and enough frames per second to test the system on a real vehicle in a real driving situation.
  - Live State-of-Health monitor in the LiDAR system should be extended with vehicle-to-infrastructure systems to detect bottlenecks related sending reliability data over the infrastructure.

Chapter 7

Publications

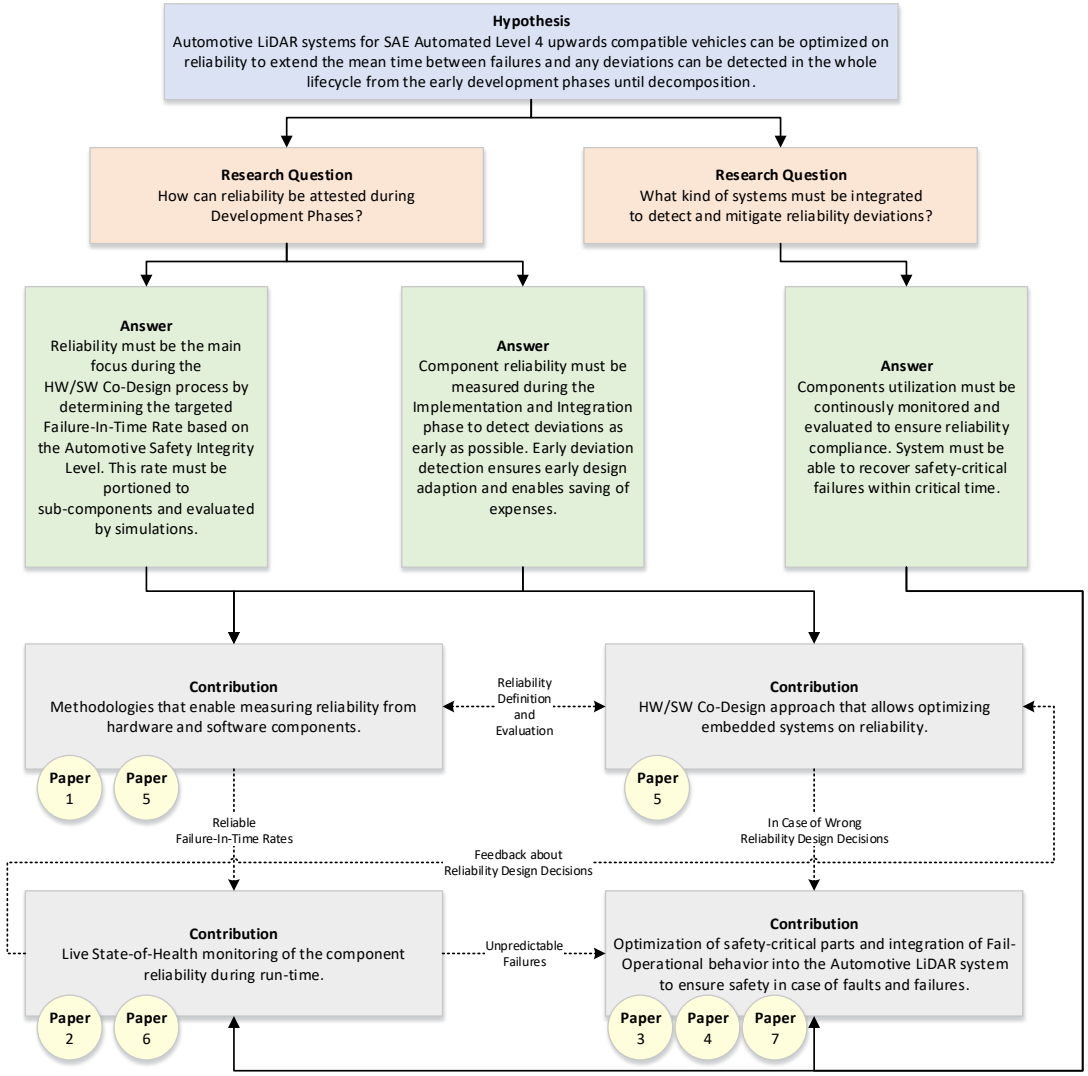

Figure 7.1: Overview of the Contributions of this Thesis and the related Scientific Publications.

7.1 Overview and Contribution

Figure 7.1 gives an overview of the main Hypothesis, the derived Research Questions and the Related Contributions. My main hypothesis is that the development of novel Advanced Driver Assistance Systems such as the LiDAR system can be developed with the main focus on reliability. The reliability is not longer a specific value called as the MTBF or FIT Rate, instead reliability becomes the key factor of the whole development lifecycle. This lifecycle contains from the early development phases until decomposition of the vehicle.

Based on this hypothesis I encountered that for changing the focus on reliability there are several gaps that need to be closed to enable this specific development focus. Based on these gaps I derived two main Research Questions:

- How can reliability be attested during Development Phases?
- What kind of systems must be integrated to detect and mitigate reliability deviations?

If reliability should become the main driven factor during development it requires solid methodologies that enable the measurement of reliability at different abstraction layers such as on component, system or item level. The quantification represents a value that will enable a comparison of different implementations as well as to control the compliance with a specific reliability requirement. Furthermore, there must be a superior methodology that supports engineers in separating the overall FIT Rate that is based on the HARA into smaller sub-modules. Only this circumstance will allow smaller iterations and early interventions.

Reliability is important for long-term safety but can not be used to mitigate failures. It can statistically extend the time of possible failures. For that reason, safety mitigations will not be as important as nowadays instead it will become more relevant caused by the fact that SAE Automated Level 4 and 5 vehicles will loose the human driver as a last safety instance. This directly affects the degree of confidence for failure mitigations. Novel vehicles must perform a transition from fail-safe to fail-operational behavior. During my thesis I designed novel safety concepts that increase the overall safety of environmental perception sensors. In my case I developed these concepts for a LiDAR system.

Based on these research questions I analyzed the common reliability processes of the automotive industry and in particular the reliability of semiconductor devices. The specification of the target FIT Rate is well explored and is the result of the Hazard and Risk Analysis. The HARA is deriving the desired ASIL Level and this is related to a specific FIT Rate. After this specification, reliability becomes a lower priority and the ISO 26262 and IEC 62308 is stepping in after the design and implementation process. Because the

calculation of the final Base FIT Rate is related to the final integrated circuit. In common vehicles that are mostly driven by a human driver this is sufficient from a safety point of view, because traditionally all safety-critical parts have a mechanical connection between the human driver and the related actors such as steering and braking. But for modern vehicles with the ability to introduce updates that enable SAE Automated Level 4 or 5 this will not be appropriate. For this purpose I encountered the following conditions that are also answering the Research Questions of this Thesis:

- Reliability must be the main focus during the HW/SW Co-Design process by determining the targeted FIT Rate based on the ASIL Level. This rate must be separated into sub-components and evaluated by simulations.
- Component reliability must be measured during the Implementation and Integration phase to detect deviations as early as possible. Early deviation detection ensures early design adaption and enables cost savings.
- Component utilization must be continuously monitored and evaluated to ensure reliability. A system must be able to recover safety-critical failures within critical time.

During my research I determined that the gap between the specification of the FIT Rate by the ASIL Level and the final Base FIT Rate from the produced Integrated Circuit is not providing methodologies that allow the integration of the reliability into all development phases considering the V-Model. Therefore, I had to investigate the current State-of-the-Art and based on these results develop a novel methodology that enables the measurement of reliability of hardware and software components. The main focus here was always the compliance with the common safety and reliability related standards such as the ISO 26262 and IEC 62308. Based on the previous Research Answers this Thesis provides the following Contributions:

1. Methodologies that enable measuring reliability from hardware and software components.
2. HW/SW Co-Design approach that allows optimizing Embedded Systems on reliability.
3. Live State-of-Health monitoring of the component reliability during run-time.
4. Optimization of safety-critical parts and integration of fail-operational behavior into the Automotive LiDAR system to ensure safety in case of faults and failures.

These Contributions are logically connected and are representing a closed safety system. Contribution 1 is directly connected to Contribution 2 and 3. The logical connection between Contribution 1 and 2 is the definition of the overall reliability and the evaluation of the specific requirement. For this purpose, this Thesis provides novel methodologies that enables the measurement of FIT Rates for sub-components on hardware and software level. These methodologies were bundled with a specific HW/SW Co-Design approach that emphasizes on developing Embedded Systems on reliability. Between Contribution 1 and 3 the focus is on analyzing the desired Base FIT Rates and represents a feedback loop of the Design Document and the unit that is in operation. The novel Live State-of-Health monitor enables the measurement of the real FIT Rate and the continuous optimization of the device caused by the fact that Firmware and Software updates can be rolled out over the air.

Contribution 2 is connected to Contribution 1 that was already described in the previous paragraph and to Contribution 4. The design of a specific product is always related to missing specifications. These missing specifications could lead to safety-critical situations. For this purpose, it is necessary to implement robust fail-safe and fail-operational functionalities or optimize safety-critical parts of the design. This Thesis implemented several safety monitors and safety functions that enable a safe operation of the LiDAR system even in safety-critical situations. This will catch unconsidered design situations or wrong reliability design decisions.

Contribution 3 directly gives Feedback to Contribution 2 about reliability design decisions. In case of wrong design decisions the Live State-of-Health monitor will detect these deviations. This enables the collection of real Mission Temperature Profile data as well as enables Big Data for Safety. If a specific system would be extensively used and it can be foreseen that this system could fail. This will allow predictive maintenance of safety-critical systems such as the Environmental Perception System. In case that the Live State-of-Health Monitor is failing because of wrong reliability estimation of the specific semiconductor device. The whole system will fall back to Contribution 4 which provides several safety-related implementations that are designed for fail-safe and fail-operational operation of the LiDAR system.

7.2 List

Publication 1: Strasser, Andreas and Stelzer, Philipp and Steger, Christian and Druml, Norbert, *FITness Assessment-Hardware Algorithm Safety Validation*, The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications, 24-28 Mar. 2019, Valencia, Spain.

Task	**Responsible**	**Realization**
Problem Finding	Fully	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	Fully	Fully
Hardware/Software Design	Fully	Fully
Implement Approach	Fully	Fully
Planning Experiment	Fully	Fully
Perform Experiment	Fully	Fully
Evaluate Experiment Results	Fully	Fully
Validating Results	Fully	Fully
Graphical Design	Fully	Fully
Text Writing	Fully	Fully

Publication 2: Strasser, Andreas and Stelzer, Philipp and Steger, Christian and Druml, Norbert, *Live State-of-Health Safety Monitoring for Safety-Critical Automotive Systems*, 2019 22nd Euromicro Conference on Digital System Design (DSD), 28-30 Aug. 2019, Kallithea, Greece.

Task	**Responsible**	**Realization**
Problem Finding	Fully	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	Fully	Fully
Hardware/Software Design	Fully	Fully
Implement Approach	Fully	Fully
Planning Experiment	Fully	Fully
Perform Experiment	Fully	Fully
Evaluate Experiment Results	Fully	Fully
Validating Results	Fully	Fully
Graphical Design	Fully	Fully
Text Writing	Fully	Fully

Publication 3: Strasser, Andreas and Stelzer, Philipp and Steger, Christian and Druml, Norbert, *Speed-Up of MEMS Mirror's Transient Start-Up Procedure*, 2019 IEEE Sensors Applications Symposium (SAS), 11-13 Mar. 2019, Sophia Antipolis, France.

Task	**Responsible**	**Realization**
Problem Finding	Partially	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	Fully	Fully
Hardware/Software Design	Fully	Fully
Implement Approach	Mostly	Mostly
Planning Experiment	Fully	Fully
Perform Experiment	Mostly	Mostly
Evaluate Experiment Results	Fully	Fully
Validating Results	Fully	Fully
Graphical Design	Mostly	Mostly
Text Writing	Fully	Fully

Contribution and Differentiation: For problem finding I was supported by Norbert Druml with whom I discussed that the current transient start-up process is too slow and needs to be accelerated. From that starting point on I decided to analyze the current design and start-up procedure. After this point I managed all Tasks independently in regard to the transient start-up procedure. My colleague Philipp Stelzer contributed the Shock Injection Design, Implementation and Evaluation part that is described in Section 3 - Part A of the paper.Figure 5 and 6 and the related measurement results of Figure 6 were also contributed by Philipp Stelzer. The Text of the Shock Injection paragraph was written by myself.

Publication 4: Strasser, Andreas and Stelzer, Philipp and Steger, Christian and Druml, Norbert, *Towards Synchronous Mode of Multiple Independently Controlled MEMS Mirrors*, 8th IFAC Symposium on Mechatronic Systems MECHATRONICS 2019, 4-6 Sept. 2019, Vienna, Austria.

Task	**Responsible**	**Realization**
Problem Finding	Partially	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	Fully	Fully
Hardware/Software Design	Fully	Fully
Implement Approach	Fully	Fully
Planning Experiment	Fully	Fully
Perform Experiment	Fully	Fully
Evaluate Experiment Results	Fully	Fully
Validating Results	Fully	Fully
Graphical Design	Fully	Fully
Text Writing	Fully	Fully

Contribution and Differentiation: To find the problem I was supported by Norbert Druml who discussed with me that there could be the case when more than one LiDAR system is operated than there will be high interferences. I further identified that this problem needs to be solved to enable a robust operation of multiple LiDAR systems.

Publication 5: Strasser, Andreas and Stelzer, Philipp and Steger, Christian and Druml, Norbert, *HW/SW Co-Design Approach to Optimize Embedded Systems on Reliability*, International Journal On Advances in Systems and Measurements, Volume 12 Nr. 3-4, 2019.

Task	**Responsible**	**Realization**
Problem Finding	Fully	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	Fully	Fully
Hardware/Software Design	Fully	Fully
Implement Approach	Fully	Mostly
Planning Experiment	Fully	Fully
Perform Experiment	Fully	Fully
Evaluate Experiment Results	Fully	Fully
Validating Results	Fully	Fully
Graphical Design	Fully	Fully
Text Writing	Fully	Fully

Contribution and Differentiation: I did not implement the sorting algorithms on my own. Instead I used implementations that were available from public sources such as Github, but these algorithms were just used as samples and therefore they have not contributed to my approach or methodology.

Publication 6: Strasser, Andreas and Stelzer, Philipp and Steger, Christian and Druml, Norbert, *Enabling Live State-of-Health Monitoring for a Safety-Critical Automotive LiDAR System*, 2020 IEEE Sensors Applications Symposium (SAS), 9-11 Mar. 2020, Kuala Lumpur, Malaysia.

Task	**Responsible**	**Realization**
Problem Finding	Fully	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	Fully	Fully
Hardware/Software Design	Fully	Fully
Implement Approach	Fully	Fully
Planning Experiment	Fully	Fully
Perform Experiment	Fully	Fully
Evaluate Experiment Results	Fully	Fully
Validating Results	Fully	Fully
Graphical Design	Fully	Fully
Text Writing	Fully	Fully

Publication 7: Strasser, Andreas and Stelzer, Philipp and Warmer, Felix and Steger, Christian and Druml, Norbert, *Enabling Fail-Operational Behavior and Degradation for Safety-Critical Automotive 3D Flash LiDAR Systems*, 2020 23nd Euromicro Conference on Digital System Design (DSD), 26-28 Aug. 2020, Portoroz, Slovenia.

Task	**Responsible**	**Realization**
Problem Finding	Fully	Fully
Theoretical Analysis	Fully	Fully
Find Suitable Approach	No	No
Hardware/Software Design	No	No
Implement Approach	No	No
Planning Experiment	No	No
Perform Experiment	No	No
Evaluate Experiment Results	No	No
Validating Results	No	No
Graphical Design	No	No
Text Writing	Fully	Fully

Contribution and Differentiation: I identified that there could be a problem with the LiDAR system regarding reliability in case of high temperature and high utilization of the memory module. The general project was transfered to my colleague Felix Warmer, who addressed the problem in his Master Thesis that can be found in the References. My task was to support of Felix Warmer and the academic preparation and the writing of the publication.

PESARO 2019 : The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

FITness Assessment
Hardware Algorithm Safety Validation

Andreas Strasser, Philipp Stelzer, Christian Steger
Graz University of Technology
Graz, Austria
Email: {strasser, stelzer, steger}@tugraz.at

Norbert Druml
Infineon Technologies Austria AG
Graz, Austria
Email: norbert.druml@infineon.com

***Abstract*—Error Correction Codes (ECC) are important safety methods for digital data to gain control of Single Event Upsets (SEU) in integrated digital circuits. SEU are responsible for single bit flips inside a digital circuit caused by ionizing radiation. This effect does not affect the physical structure of the components but the correctness of data inside flip flops. Consequently, data gets corrupted and the correct program flow gets disturbed. This effect needs to be considered especially for safety-critical systems. In the new ISO 26262 2nd Edition, the automotive domain suggests controlling SEU effects by algorithms that correct Single Bit Errors and Detect Double Bit Errors (SEC-DED). This raises the question what kind of impact Double Bit Error Correction (DEC) will have on the overall safety level for LiDAR (Light Detection and Ranging) systems. In this publication, we determine the difference between two ECC algorithms from a safety point of view: Hamming's code (SEC-DED) and Bose–Chaudhuri–Hocquenghem-Code (DEC). For this purpose, we developed a novel method for algorithm safety validation and applied it to both algorithms.**

Keywords–Safety Validation FPGA, Failure-in-Time Analysis FPGA, Error Correction Codes, ISO 26262 2nd Edition, Algorithm Validation.

I. Introduction

Fully autonomous driving will change our society, as well as individuals's daily routines and will improve overall road safety. To achieve the goal of autonomous driving, novel Advanced Driver-Assistance Systems (ADAS) are necessary. The two best-known ADAS are the Electronic Stability Control and the Anti-Lock Braking System, especially for their positive effect on active safety. Moreover, in the last years, a new generation of ADAS such as the Adaptive Cruise Control (ACC) has been established in middle class cars to avoid collisions. The next big step is introducing a comprehensive system enabling the perception of urban environment, which is one of the main goals of the PRYSTINE project [1].

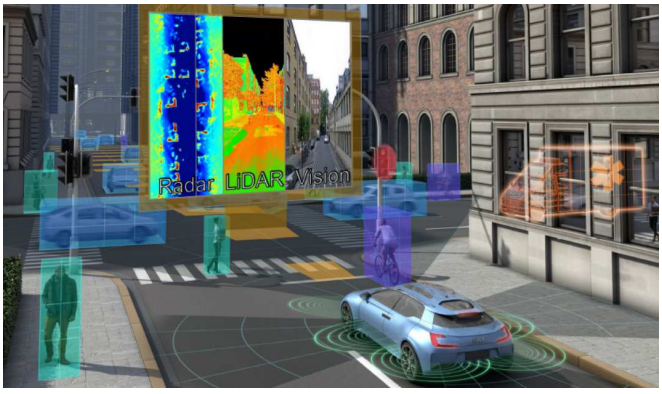

Figure 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

PRYSTINE stands for Programmable Systems for Intelligence in Automobiles and is based on robust Radar and LiDAR sensor fusion to enable safe automated driving in urban and rural environments, as seen in Figure 1. These devices must be reliable, safe and fail-operational to handle safety-critical situations independently [1]. In contrast to Radar, LiDAR has not been implemented in middle class cars yet but there are basic approaches in the automotive industry such as the 1D MEMS Micro-Scanning LiDAR system as seen in Figure 2 [2]. This modern LiDAR system consists of an emitter and receiver path. The emitter path contains the Microelectromechanical systems (MEMS) mirror and the MEMS Driver Application-specific integrated circuit (ASIC). Druml et al. [2] indicate that the MEMS Driver and its precision of sensing, actuation and control directly influence the complete LiDAR system's measurement accuracy. Consequently, the LiDAR system's control-related digital circuits need to be correct and fault-tolerant. Fault-tolerant digital circuits struggle mainly with random hardware faults like Single Event Upsets which are soft errors in semiconductor devices induced by ionizing radiation [3]. These events do not physically harm the semiconductor components but may alter the logical value of a flip flop [4]. These errors have been affecting digital integrated circuits for decades and therefore, Error Correction Codes (ECC) are used for safety-critical systems [5]. ECCs are self-repairing algorithms with the ability to correct certain bit errors and maintain data correction during runtime [6]. The effect of SEU exponentially increases with higher packaging density as less electrons are representing a logic value [4]. As the demand for semiconductor devices rises due to ADAS, packaging density needs to increase even faster to satisfy computation power for real-time video signal processing [7]. Nevertheless, this trend also introduces drawbacks, especially from a safety point of view, as the enhancement of packaging density also increases the sensitivity to SEU [4]. Consequently, the automotive industry needs regulations and standards for safety-related semiconductor devices. For safety-related electrical and electronic devices, the automotive industry considers the functional safety ISO 26262 standard. In nine normative parts, this standard

 ISBN: 978-1-61208-698-9

PESARO 2019 : The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

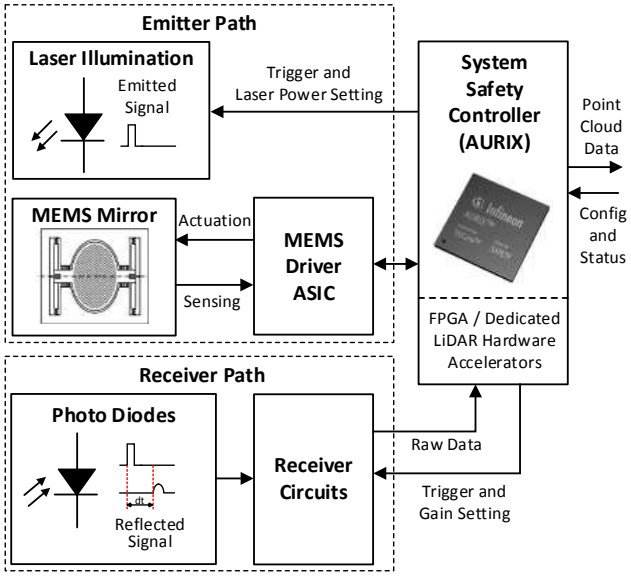

Figure 2. Overview of a LiDAR system for automonomous driving [2].

describes best practices to support engineers and managers in developing fail-safe automotive parts [8]. In the last years, this standard has been extended and the new version will be released end of 2018. The new version is called ISO 26262 2nd Edition and will include a part for semiconductors describing functional safety concepts for semiconductor devices [9]. For soft error mitigation, the standard suggests the use of Single Error Correction and Double Error Detection algorithms to protect digital circuits [9]. For semiconductor devices SEC-DED was already used in 1984 [5]. At that time, semiconductor devices were not that highly integrated and the packaging density was not as high as nowadays. Already in 1984, Chen et al. [5] described that in future semiconductor devices will use more complex ECC algorithms such as Double Error Correction and Triple Error Detection (DEC-TED). Contrary to the prediction of Chen et al. [5], the automotive industry still suggests using SEC-DED ECC algorithms 34 years later. This raises the question whether there are any disadvantages on DEC-TED algorithms or if the SEC-DED still fulfills the requirements for fail-safe automotive systems.

For this purpose, we will elaborate on the following two research questions:

- How can different ECC algorithms be validated from a safety point of view?
- Are Double Error Correction algorithms for LiDAR systems safer than SEC-DED algorithms?

II. Related Work

The need for error correction has always been vital for digital semiconductor devices due to possible alterations of flip flops caused by SEU. Already in 1984, Chen et al. described the application of these codes for semiconductor memory applications [5]. However, the history of ECC already began with punched card read errors in 1950. In this year, Hamming introduced his new approach for an automatic Error Correction Code during run-time to solve read errors [10]. Hamming's code is widely known and used for ECC. The algorithm corrects Single Bit Errors and is able to Detect Double Bit Errors (SEC-DED) by adding an additional parity bit [11]. For correcting more bits, other ECC algorithms are necessary. One of them is the concept of Bose-Chaudhuri-Hocquenghem-Codes (BCH-Codes). BCH-Codes can be used for multiple bit error corrections [12]. These two algorithms are the most important ECC concepts for digital integrated circuits and were already described by Chen et al. in 1984 [5]. Even modern and highly integrated complex systems still make use of Hamming's code and BCH-code [13] [14]. The novel ISO 26262 2nd Edition still refers to Hamming's ECC code to accomplish fail-safe digital circuits.

In the automotive industry, the ISO 26262 standard is used for functional safety. The new version ISO 26262 2nd Edition suggests ECC for diagnosing memory failures and rates the resulting diagnosis coverage as high. Therefore, this measure is often used for safety critical digital components [9] [13] [14]. For ECC, the standard still suggests the use of SEC-DED algorithms such as the Hamming code [9]. This raises the question whether SEC-DED has any advantages over DEC algorithms or vice versa. Still, novel safety critical automotive approaches, such as the fault-tolerant cache system for an automotive vision processor from Han et al. use SEC-DED [14].

The validation of algorithms is an important method for achieving certain requirements such as area, power dissipation or run time. Therefore, there are numerous articles about enhancing efficiency of fault-tolerant mechanisms through algorithm substitution [15] [16] [17]. Rossi et al. analyze the power consumption of fault-tolerant busses by comparing different Hamming code implementations with their novel Dual Rail coding scheme [15]. Also, Nayak et al. emphasize the low power dissipation of their novel Hamming code components [16]. Another example is the work of Shao et al. about power dissipation comparison between the novel adaptive pre-proccesing approach for convolutional codes of Viterbi decoders with conventional decoders [17]. Khezripour et al. provide another example for validating different fault-tolerant multi processor architectures by power dissipation [18]. Unfortunately, power dissipation is just one factor for reliability of safety-critical components and insufficient for safety validation. The most important indicator for safety at hardware level is the component reliability, which is measured in failure in time (FIT) rates [9]. Component reliability is the main indicator for safe hardware components and describes the quantity of failures in a specific time interval, mostly one billion hours [9]. These values can be calculated by specific standards for electronic component reliability such as the IEC TR 62380 [19] or statistically collected by field tests. Oftentimes, these field test have already been conducted by the manufacturers and are compiled in specific datasheets for component reliability [20]. For each component, the datasheets usually contain the specific FIT Rate for a certain temperature. To determine the FIT Rate for other temperatures, the Arrhenius equation as seen in (1) can be used.

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \quad (1)$$

where:

DF	is Derating Factor
E_a	is Activation Energy in eV
k	is Boltzmann Constant (8.167303 x 10^{-5} ev/K)
T_{use}	is Use Junction Temperature in K
T_{stress}	is Stress Junction Temperature in K

 ISBN: 978-1-61208-698-9

PESARO 2019 : The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

The Arrhenius Equation requires the Junction Temperature instead of Temperature values. The Junction Temperature represents the highest operation temperature of the semiconductor and considers the Ambient Temperature, Thermal Resistance of the package as well as the Power Dissipation as seen in (2).

$$T_j = T_{amb} + P_{dis} \cdot \theta_{ja} \tag{2}$$

where:

T_{amb}	is Ambiant Temperature
P_{dis}	is Power Dissipation
θ_{ja}	is Package Thermal Resistance Value

The validation of ECC algorithms is crucial for designers to pick the optimal ECC. Rossi et al. analyzed SEC-DED and DEC codes on area overhead and cache memory access time but their work did not consider the impact of different ECC algorithms from a safety point of view [21]. For designers of safety-critical digital circuits, it would be helpful to be able to pick the most safe ECC with the advantage of lower FIT Rates. Especially for automotive Tier-1 companies lower FIT Rates imply higher component reliability which is crucial for the economic success or failure of the whole system as profit margins are that small that every defect matters. Therefore, to support designers of safety-critical digital circuits, this paper's contributions to existing research are:

1) Developing a novel method for safety validation of algorithms on Field Programmable Gate Array that is based on the approved ISO 26262 2nd Edition methods.
2) Applying the novel method to quantify the differences between SEC-DED and DEC from a safety point of view.
3) Recommendation of ECC algorithm for safety-critical automotive LiDAR systems, based on the novel method of this paper.

III. FITness Assessment

To validate different ECC algorithms, it is necessary to quantify the essential values. Based on the functional safety standard ISO 26262 2nd Edition's approved methods, the FIT Rate is the most important factor for safety-critical hardware components. As stated in the Related Work section II, the Derating Factor influences the FIT Rate and is expressed in the Arrhenius equation (1). Combined with the Temperature Junction equation it is obvious that the power dissipation is the most significant quantity that can be influenced by designers of digital circuits (see (3)).

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{amb} + P_{dis} \cdot \theta_{ja}})} \tag{3}$$

Consequently, by decreasing Power Dissipation the designer increases component reliability. For Field Programmable Gate Array (FPGA), the power dissipation primarily depends on static and dynamic power consumption. Based on these physical principles, our novel method FITness Assessment for algorithm safety validation on FPGAs is segmented in the following parts, as seen in Figure 3:

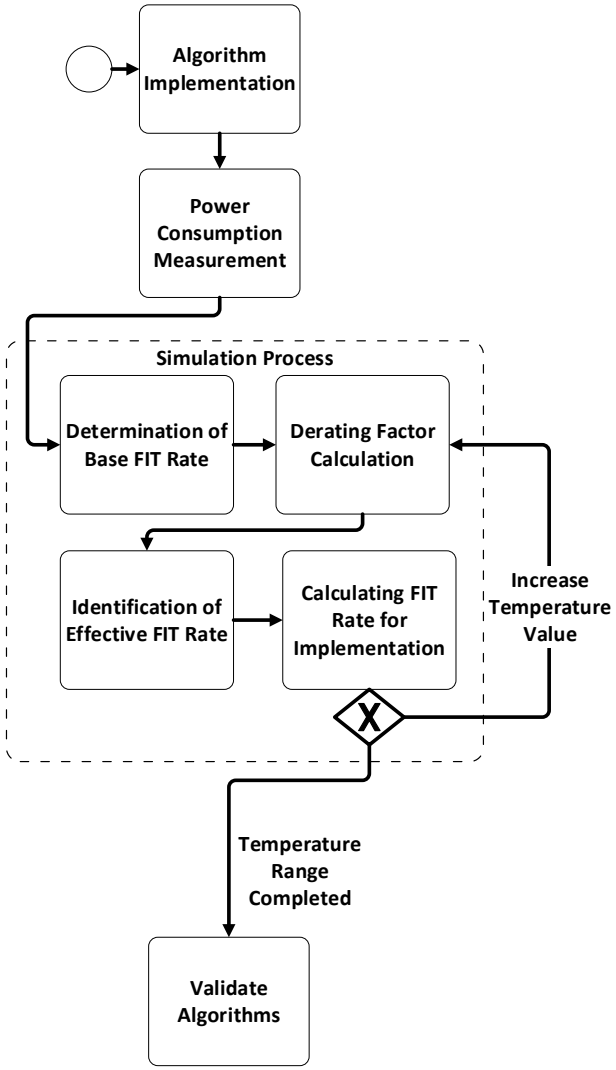

Figure 3. Workflow overview of our novel method FITness Assessment for algorithm validation from a safety point of view in Business Process Model and Notation.

1) **Algorithm Implementation**
To guarantee similar conditions for different algorithms, it is necessary to implement a generic framework that allows implementing algorithms without major changes.
2) **Power Consumption Measurement**
For each algorithm, a particular measurement is recorded. It is advisable to record the generic framework without any algorithm to be able to determine the algorithms' power consumption by subtraction.
3) **Determininationof Base FIT Rate**
The Base FIT Rate may be calculated by using the IEC TR 62380 [19] standard or analyzed statistically by field tests. Oftentimes, these field test have already been conducted by the manufacturers and are compiled in specific datasheets for component reliability.
4) **Derating Factor Calculation**
The Derating Factor can be calculated with the Arrhenius equation and the related Thermal Junction equation as seen in (1) and (2).

 ISBN: 978-1-61208-698-9

PESARO 2019 : The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

5) **Identification of Effective FIT Rate**
The Effective FIT Rate reflects the Base FIT Rate for a specific temperature and can be calculated with:

$$FIT_{ef} = FIT_{base} \cdot DF \quad (4)$$

where:

FIT_{base} is Base FIT Rate from FPGA Reliability Datasheet
DF is Derating Factor as seen in (1)

6) **Calculating FIT Rate of the Implementation**
The Effective FIT Rate as seen in (4) represents the component reliability for the whole FPGA. However, an FPGA is made up of many different logic elements. Consequently, the Effective FIT Rate can be broken down into the amount used by each logical element as seen in (5).

$$FIT_{imp} = \frac{FIT_{ef}}{N_{le}} \quad (5)$$

where:

FIT_{ef} is Effective FIT Rate as seen in (4)
N_{le} is Total Number of Logic Elements of the specific FPGA taken out from Datasheet

7) **Validate Algorithms**
The resulting FIT Rate of the implementation represents the FIT Rate of the specific algorithm and can be used for validation. It is adviseable to measure each algorithm once at room temperature conditions and simulate the rest of the temperature range by starting with the Derating Factor Calculation.

IV. Test Setup

In our research question, we analyze the differences between SEC-DED and DEC. For this purpose, we chose the Hamming code for SEC-DED as this code is recommended in the new ISO 26262 2nd Edition and the BCH-code for DEC, especially because other ECC algorithms are often based on this concept and both algorithms fulfil the following requirements:

- 32 Bit data size
- Combinatorical Logic
- Including Fault Injection Module
- SEC-DED or DEC Functionality

The generic algorithm framework contains a testbench with an automatic up-counter as well as a validator (see Figure 5). Both algorithms can be exchanged in the framework without any major changes. This enables a precise validation from a safety point of view.

In our test setup, we use the MAX1000 - IoT Maker Board by Trenz Electronic. This device is a small maker board for prototyping with sparse additional components. The main controller is the MAX10 10M08SAU169C8G, an FPGA device by Intel. For our research, the main advantages of using this board are:

- Small amount of additional hardware components
- Availability of Reliability Datasheet

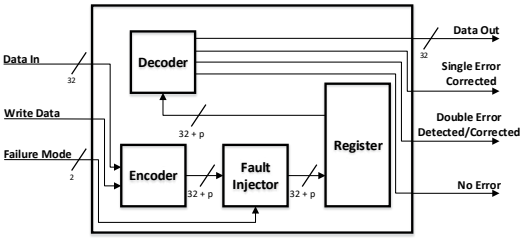

Figure 4. Pin configuration of both algorithms including an overview of functional blocks inside.

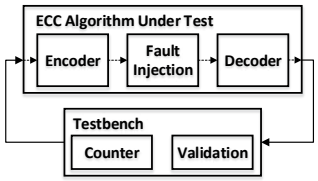

Figure 5. General framework for ECC algorithm validation including testbench and ECC algorithm.

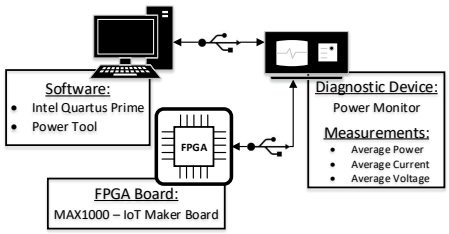

Figure 6. Overview of the entire measurement setup including software and hardware components.

This board also contains an FTDI chip that draws about 50 mA on average, which we will subtract out for our analysis. The power consumption measurement is performed by the Mobile Device Power Monitor of Monsoon Solutions. The big advantage of this power monitor is the direct measurement of USB devices. The entire measurement setup is shown in Figure 4 and 6 and contains the following software and hardware parts:

- Quartus Prime 18.0 (Intel)
- Power Tool 5.0.0.23 (Monsoon Solutions)
- Mobile Device Power Monitor (Monsoon Solutions)
- MAX1000 - IoT Maker Board (Trenz Electronic)

V. Results

This section summarizes our results of the comparison of SEC-DED and DEC ECC algorithm. The validation was performed with our novel FITness Assessment method for algorithm validation from a safety point of view as described in Section III.

The first algorithm we implemented was the Hamming code, which is a SEC-DED ECC algorithm. The implementation reserves 45 logic elements of the used FPGA and the whole board has an average power dissipation of 571.78 mW. With the second BCH-code DEC ECC algorithm, the board consumes an average of 599.05 mW and assignes 65 logic elements. The first result shows a difference between both algorithms in logic elements as well as in power dissipation resulting in a varying FIT Rate. The next step is the simulation

 ISBN: 978-1-61208-698-9

PESARO 2019 : The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

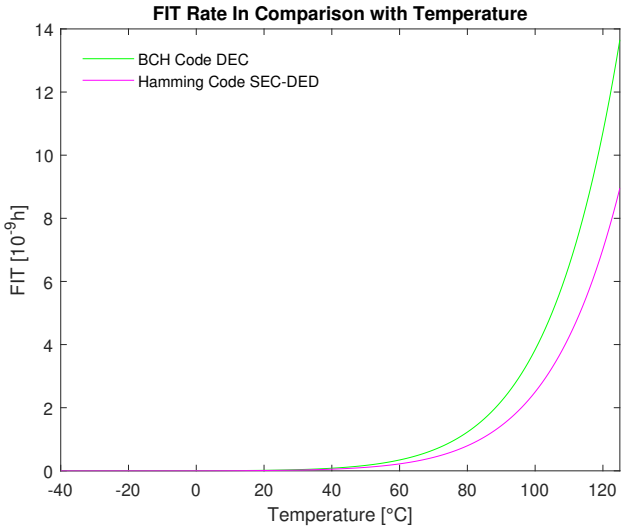

Figure 7. Simulation results of the resulted FIT Rates between -40°C and 125°C for both ECC implementations.

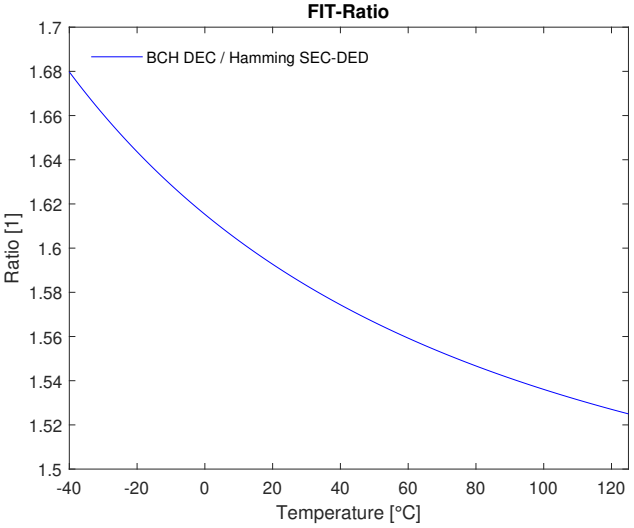

Figure 8. Overview of the FIT Rate overhead between SEC-DED and DEC ECC algorithm.

process over the whole temperature range. We selected a temperature range between -40°C and 125°C and the values of Table I were used for the simulation process. In our simulation we neglected the alteration of power dissipation through temperature because it would affect both ECC implementations evenly.

Figure 7 points out that both algorithms vary in their FIT Rate and rise exponentially with increasing temperature. The FIT Rate may be neglected for temperatures up to 40 °C. The Hamming code with SEC-DED shows a better FIT Rate indicating more reliability of the hardware components which results in a higher safety level. The reason for this difference is the greater number of logic elements used for the DEC ECC algorithm and the resulting increase of power dissipation. The higher power dissipation results in a higher Thermal Junction temperature as seen in (2) which leads to a higher FIT Rate.

Both algorithms were implemented without any safety measures. This means that any damage to the Logic Element of the FPGA leads to failure of the whole ECC algorithm and

TABLE I. RESULTS OF THE RESERVED LOGIC ELEMENTS AND AVERAGE TOTAL POWER DISSIPATION OF BOTH ECC IMPLEMENTATIONS.

	Hamming Code	BCH-Code
Used Logic Elements	45	65
Total Average Power Dissipation	571.78 mW	599.05 mW

the safe memory block. The ECC algorithm is the measure against SEU related altered flip flops inside the memory block which decreases the specific FIT Rate of the memory block. The results of Figure 7 do not represent the FIT Rates of the memory block but the FIT Rate of the pure ECC implementation. It is important to understand that the ability of more bit error correction is not considered for the algorithm validation because it only positively influences the FIT Rate of the memory block.

Moreover, it is important to understand that the absolute values of the FIT Rate always correlate to a specific FPGA. Consequently, it is advantageous to look at the ratio between the algorithms because this gives a better overview of the overhead. The SEC-DED/DEC ECC FIT Ratio is depicted in Figure 8. The FIT Ratio overhead of the DEC ECC algorithm is slighly decreasing with increasing temperature, which is negligible in practice.

We recommend using the Hamming code algorithm for SEC-DED error correction for 32 bit memory size registers in automotive LiDAR systems. The SEC-DED algorithm used in our experiment resulted in a FIT Rate that was at least 52% lower than the DEC ECC algorithm.

VI. Conclusion

In this paper we analyzed SEC-DED and DEC ECC algorithms from a safety perspective. In Section III, we introduced the FITness Assessment, a novel method for algorithm validation from a safety point of view. This method is based on approved methods of the novel automotive functional safety standard ISO 26262 2nd Edition. The result clearly shows that different algorithms lead to different FIT Rates. FITness Assessment allowed the measurement of each algorithm's specific FIT Rate, facilitating the selection of the most reliable ECC algorithm. Our case shows a DEC ECC algorithm that has a higher FIT Rate than the SEC-DED ECC algorithm. The FIT Rate reflects component reliability which is an important hardware indicator for safety.

The paper's findings demonstrate that algorithm validation from a safety point of view is possible and that different ECC algorithms also result in different FIT Rates. These differences should not be neglected from a safety as well as from a business point of view. The FIT Rate also statistically indicates the amount of defective components, which is an economically important indicator as lower FIT rates also result in less defect components. Our results also give an explanation why the automotive industry still suggests using SEC-DED ECC algorithms instead of DEC ECC algorithms as SEC-DED offers a lower FIT Rate than DEC. In our case, the difference in FIT Rate was at least 52% and consequently, we suggest using SEC-DED for LiDAR systems.

The automotive industry is disrupted by autonomous driving which is why fault-tolerance, safety and reliability will become increasingly important in the next years. Our novel method FITness Assessment enables the validation of different algorithms to be able to select the most reliable one, which

 ISBN: 978-1-61208-698-9

PESARO 2019 : The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

helps improve the overall safety level of the automotive vehicle by increasing component reliability.

VII. Acknowledgments

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

References

[1] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "Prystine - programmable systems for intelligence in automobiles," in 2018 21st Euromicro Conference on Digital System Design (DSD), Aug 2018, pp. 618–626.

[2] N. Druml, I. Maksymova, T. Thurner, D. Van Lierop, M. Hennecke, and A. Foroutan, "1D MEMS Micro-Scanning LiDAR," in Conference on Sensor Device Technologies and Applications (SENSORDEVICES), 09 2018.

[3] B. D. Sierawski, J. A. Pellish, R. A. Reed, R. D. Schrimpf, K. M. Warren, R. A. Weller, M. H. Mendenhall, J. D. Black, A. D. Tipton, M. A. Xapsos, R. C. Baumann, X. Deng, M. J. Campola, M. R. Friendlich, H. S. Kim, A. M. Phan, and C. M. Seidleck, "Impact of low-energy proton induced upsets on test methods and rate predictions," IEEE Transactions on Nuclear Science, vol. 56, no. 6, Dec 2009, pp. 3085–3092.

[4] R. Islam, "A highly reliable SEU hardened latch and high performance SEU hardened flip-flop," in Thirteenth International Symposium on Quality Electronic Design (ISQED), March 2012, pp. 347–352.

[5] C. L. Chen and M. Y. Hsiao, "Error-Correcting Codes for Semiconductor Memory Applications: A State-of-the-Art Review," IBM Journal of Research and Development, vol. 28, no. 2, March 1984, pp. 124–134.

[6] J. Singh and J. Singh, "A Comparative Study of Error Detection and Correction Coding Techniques," in 2012 Second International Conference on Advanced Computing Communication Technologies, Jan 2012, pp. 187–189.

[7] H. Shaheen, G. Boschi, G. Harutyunyan, and Y. Zorian, "Advanced ECC solution for automotive SoCs," in 2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS), July 2017, pp. 71–73.

[8] R. Mariani, "An overview of autonomous vehicles safety," in 2018 IEEE International Reliability Physics Symposium (IRPS), March 2018, pp. 6A.1–1–6A.1–6.

[9] I. n. E. ISO, "Draft 26262 2nd Edition: Road vehicles-Functional safety," International Standard ISO/FDIS, vol. 26262, 2018.

[10] R. W. Hamming, "Error detecting and error correcting codes," The Bell System Technical Journal, vol. 29, no. 2, April 1950, pp. 147–160.

[11] H. Liu, D. Kim, Y. Li, and A. Z. Jia, "On the separating redundancy of extended hamming codes," in 2015 IEEE International Symposium on Information Theory (ISIT), June 2015, pp. 2406–2410.

[12] Z. Xie, N. Li, and L. Li, "Design and Study on a New BCH Coding and Interleaving Techniques Based on ARM Chip," in 2008 4th IEEE International Conference on Circuits and Systems for Communications, May 2008, pp. 315–318.

[13] S. Sooraj, M. Manasy, and R. Bhakthavatchalu, "Fault tolerant FSM on FPGA using SEC-DED code algorithm," in 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Dec 2017, pp. 1–6.

[14] J. Han, Y. Kwon, K. Byun, and H. Yoo, "A fault tolerant cache system of automotive vision processor complying with ISO26262," in 2016 IEEE International Symposium on Circuits and Systems (ISCAS), May 2016, pp. 2912–2912.

[15] D. Rossi, A. K. Nieuwland, S. V. E. S. van Dijk, R. P. Kleihorst, and C. Metra, "Power Consumption of Fault Tolerant Busses," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 5, May 2008, pp. 542–553.

[16] V. S. P. Nayak, C. Madhulika, and U. Pravali, "Design of low power hamming code encoding, decoding and correcting circuits using reversible logic," in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), May 2017, pp. 778–781.

[17] W. Shao and L. Brackenbury, "Pre-processing of convolutional codes for reducing decoding power consumption," in 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, March 2008, pp. 2957–2960.

[18] H. Khezripour and S. Pourmozaffari, "Fault Tolerance and Power Consumption Analysis on Chip-Multi Processors Architectures," in 2012 Seventh International Conference on Availability, Reliability and Security, Aug 2012, pp. 301–306.

[19] T. IEC, "Iec 62380," Reliability data handbook–universal model for reliability prediction of electronics components, PCBs and equipment (emerged from UTEC 80-810 or RDF 2000), 2004.

[20] "Reliability Report," Jul 2018, [retrieved: 01, 2019]. [Online]. Available: https://www.intel.com/content/www/us/en/programmable/support/quality-and-reliability/reports-tools/reliability-report/rel-report.html

[21] D. Rossi, N. Timoncini, M. Spica, and C. Metra, "Error correcting code analysis for cache memory high reliability and performance," in 2011 Design, Automation Test in Europe, March 2011, pp. 1–6.

 ISBN: 978-1-61208-698-9

2019 22nd Euromicro Conference on Digital System Design (DSD)

Live State-of-Health Safety Monitoring for Safety-Critical Automotive Systems

Andreas Strasser†, Philipp Stelzer†, Christian Steger† and Norbert Druml*
†Graz University of Technology, Graz, Austria
{strasser, stelzer, steger}@tugraz.at
*Infineon Technologies Austria AG, Graz, Austria
{norbert.druml}@infineon.com

***Abstract*—Autonomously driving vehicles require higher safety and reliability standards than traditional human-driven vehicles as they need to be able to handle safety-critical situations on their own. Therefore, these systems needs to demonstrate fail-operational behavior to ensure safety of the passengers by basic car controls. Especially silent failures of semiconductor devices can be critical from a safety point of view. Semiconductor devices fail abruptly and cannot be detected in advance.**

This paper presents a novel sensor approach to detect those kind of silent failures ahead of time and to ensure safety for future advanced driver-assistance systems (ADAS) such as LiDAR (Light Detection and Ranging). We have evaluated the design of our novel sensor concept in SystemC which will be implemented in a LiDAR system to mitigate silent failures as well as enable dynamic safety contracts.

***Keywords*-Safety, Safety Monitoring, Aging Monitor, Component Reliability, Safety Integrated Circuits, Live FIT Estimation**

I. Introduction

Autonomous driving is one of the next big steps of our society and is the key enabler of Smart Mobility [1]. Smart Mobility reinvents the urban environment by connecting infrastructure, vehicles and people to allow better quality of life, efficient energy usage and reduced costs for everyone. As a result, this era will disruptively change the daily routines of individuals as well as urban life [2]. 50 years ago, the idea of Smart Mobility started in Germany when Continental, a leading German automotive manufacturing company, tested tires on their test track Contidrom. Continental wanted to ensure constant conditions for testing and developed a self-driving car for this purpose [3]. This marked the beginning of autonomous driving. Nowadays, self-driving cars have already made their way to public streets. Tesla was the first company to release a semi-autonomous driving function called "Autopilot" [4]. Past accidents showed that it is hard to ensure safe semi-autonomous driving in urban environments by traditional methods [5]–[7]. Consequently, new Advanced Driver-Assistance Systems (ADAS) such as LiDAR (Light Detection and Ranging) need to be developed and combined with established systems. This is also the PRYSTINE (Programmable Systems for Intelligence in Automobiles" project's focus which aims at developing a comprehensive environment perception system by using LiDAR, radar and vision cameras as shown in figure 1 [1]. One of the key challenges of autonomous driving is safety and reliability of before mentioned systems. Traditional human-driven vehicles are fully - or supported by ADAS almost fully - controlled by the driver. Therefore, the system can return control and responsibility to the driver in critical situations. In future, vehicles with fully autonomous driving functionality will not have this possibility and need to be able to deal with critical situations on their own. That's one of the reasons why the impact of safety and reliability in the automotive domain is steadily increasing [8].

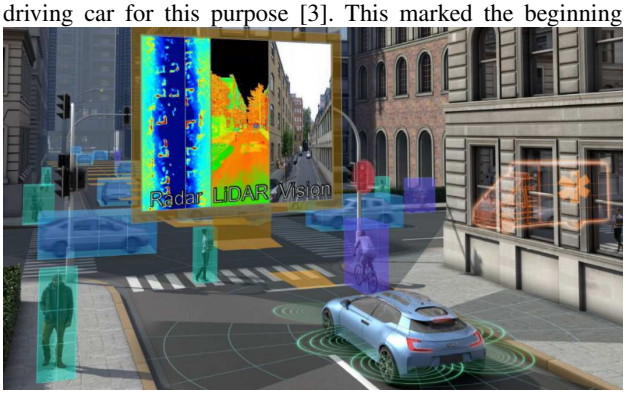

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

Nowadays, safety-critical automotive systems are developed in compliance with the ISO 26262 standard. This standard covers the development of electrical and electronic components for the automotive domain with a special focus on safe hardware and software components [9]. The standard added a guideline especially for semiconductor devices but does not support or cover dynamic safety functions such as "Conserts M" or "Ontology-Based-Run-time-Reconfiguration". Dynamic safety functions are necessary to establish resilience and flexibility to complex cyber-physical systems (CPS) [10]. Especially for future ADAS, such as the fail-operational urban surround perception system of the PRYSTINE project, this concept is vital to ensure fail-operational behavior during runtime.

Fail-operational systems require information about the common reliability and safe state of each system. Up to now, there is no possibility to retrieve live information about component reliability. Usually, components are designed for a specific utilization profile and safety is dimensioned for this profile. If there are substantial deviations to this profile, components could be undersized from a safety point of view [9]. It

978-1-7281-2862-7/19/$31.00 ©2019 IEEE
DOI 10.1109/DSD.2019.00025

would be beneficial to enable live monitoring of semiconductor devices' component reliability to communicate the state-of-health of individual components.

This paper will address the following research questions:

- Is it possible to detect component reliability of semiconductor systems during run-time?
- How can component reliability be measured for semiconductor devices?

II. Related Work

In general, detecting safety-related issues of mechanical components is rather trivial as it often involves vibration or noise during the operation [11]. For electrical or electronic components, detecting safety-related issues is much more complex. These systems fail silently and abruptly [9]. Especially for fully-autonomous vehicles, this fact poses a substantial risk as these systems need to handle every safety-critical situation on their own and any failure could trigger fatal road accidents. If we consider tucks carrying ecologically harmful substances, accidents may also lead to environmental disasters.

In general, designers of safety-critical semiconductor devices construct and dimension components for specific utilization profiles. These profiles cover the worst case utilization of the component to ensure component reliability during lifetime. Especially for semiconductor companies that design "Safety Elements out of Context", this design philosophy is difficult as they need to find the best compromise between cost and reliability. Overdimensioning hardware leads to higher costs, which may be the decisive factor for making business or not.

Nowadays, every semiconductor device contains additional safety-related monitoring circuits. For digital circuits, common monitors are error correction codes (ECC) or Built-In-Self-Test (BIST), analog circuits use monitors such as the Built-In-Current Sensor (BICS). These monitors mitigate specific problems: For instance, ECC control single event upsets (SEU), BIST checks correct functionality [9]. Shaheen et al. [12] describe common ECC practices in the automotive domain such as Parity Bit, Single Error Correction, Single Error Correction and Detection to detect and correct SEU during run-time [12]. Sargsyan [13] describes different BIST technologies that ensure correct functionality of digital semiconductor devices such as Production Mode Testing, Power-on Mode Testing and Mission Mode Testing. These tests are executed at startup or during idle time and compare the result with deposited patterns [13]. For analog circuits, Smith et al. describe the BICS that can detect current leakage [14]. Beckler et al. [15] introduce the On-Chip Diagnosis for early life and wear-out failures [15]. All these approaches only focus on testing the specific circuit's functionality in a specific moment and can not give any information on the current state-of-health. Therefore, it is necessary to have historical data about the device such as temperature, for instance. Szekely et al. [16] introduce a sensor for on-line temperature monitoring of safety-critical Integrated Circuits (IC). However, this sensor focuses on observing and communicating current temperature to external systems but does not cover temperature history [16]. Especially temperature history has a big impact on component reliability and needs to be considered from a safety point of view because higher temperature relates to higher component stress and this negatively influences the reliability.

Component reliability is one of the key requirements for safety-critical hardware devices. Nowadays, the automotive industry's approved safety methods are compiled in the ISO 26262 standard [9]. In general, these methods quantify hardware devices' component reliability in the failure in time (FIT) Rate. The FIT Rate represents the amount of failures that statistically arises within one billion operating hours. The FIT Rate is calculated or statistically determined by specific standards such as the IEC TR 62380 [17]. Usually, each semiconductor manufacturer publishes the specific FIT Rates for their devices in the component reliability data sheet [18]. These data sheets usually provide the FIT Rate for a specific test temperature which can be used to calculate equivalent FIT Rates for specific temperatures using the Arrhenius equation as seen in (1).

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \tag{1}$$

where:

DF	is Derating Factor
E_a	is Activation Energy in eV
k	is Boltzmann Constant (8.167303 x 10^{-5} ev/K)
T_{use}	is Use Junction Temperature in K
T_{stress}	is Stress Junction Temperature in K

The Derating Factor (DF) represents the positive or negative feedback of the specific temperature on the semiconductor device and depends on the Junction Temperatures that need to be determined with equation (2).

$$T_j = T_{amb} + P_{dis} \cdot \theta_{ja} \tag{2}$$

where:

T_{amb}	is Ambient Temperature
P_{dis}	is Power Dissipation
θ_{ja}	is Package Thermal Resistance Value

Equation (2) shows that the component reliability depends on the power dissipation as well as on the ambient temperature of the integrated circuit. The Derating Factor can be used for calculating the specific FIT Rate for a specific temperature as seen in (3).

$$FIT_{Base} = DF \cdot FIT_{DS} \tag{3}$$

where:

DF	is Derating Factor as seen in (1)
FIT_{DS}	is Base FIT Rate of Component Reliability Data sheet

The idea of Beckler et al. [15] and Szekely et al. [16] with these equations could be used for live component reliability monitoring.

Therefore, this paper's contribution to existing research is:

- Developing a novel method for enabling live safety monitoring of safety-critical automotive systems.

- Implementing the novel method in SystemC to prove feasibility.
- Describing the integration of the novel method in a safety-critical LiDAR sensor system for autonomous driving.

III. Use Case Overview

Self-driving vehicles handle safety-critical situations on their own without any control of a driver. Consequently, a high safety and reliability standard is necessary to ensure fail-operational behavior. In the next few years LiDAR will become common in middle-class cars and will be an important part of self-driving functionality [19]. LiDAR is an environment perception systems in combination with Radar and Vision [1].

The 1D MEMS LiDAR system of Druml et al. [19] is a novel approach to develop an inexpensive ADAS that is suitable for the mass. Novel technologies are always related to unknown failures [11]. Especially in the domain of self-driving cars, these failures are not tolerable because they result in severe road accidents.

To increase the learning curve and to evolve safer and more reliable LiDAR systems as fast as possible, component reliability should be monitored live to get real-time data of a single vehicle as well as of a complete fleet. This will enable functions that increase the overall safety level of an individual driver as well as the overall road safety. Both scenarios will be described in our use case that is divided into two sections:

- Live Reliability Data for Customers
- Live Reliability Data for Original Equipment Manufacturer (OEM)/Suppliers

A. Live Reliability Data for Customers

The reliability data of a single vehicle can be used to determine the overall usage level of a specific system as well as of the complete car. This could be used for enabling predictive maintenance like in the aircraft industry. If a specific FIT Rate is reached and the safety-critical device is dropping in the Automotive Safety Integrity Level (ASIL), this could trigger the replacement of the specific device. Especially for self-driving cars this approach could ensure a specific safety level of all self-driving road vehicles.

Another use case is the review of the complete car if individual maintenance repairs are worth to accomplish. If a certain amount of systems has reached a specific FIT Rate, this would suggest that these systems will also fail in the next few months. This will support the customer during his decision, if a repair is useful or not.

B. Live Reliability Data for OEM/Supplier

For OEMs and suppliers, the reliability data is valuable to understand whether the systems are designed for their use cases and whether there are any problems that could arise during warranty time. By using real-time data, suppliers can interfere to adapt the software parts of the devices to ensure a specific FIT Rate until the end of lifetime.

Especially software updates are changing the behavior of devices and may have a big impact on the overall safety level. By collecting reliability data of these live monitors, it will be possible to investigate and evaluate changes of these updates from a safety point of view.

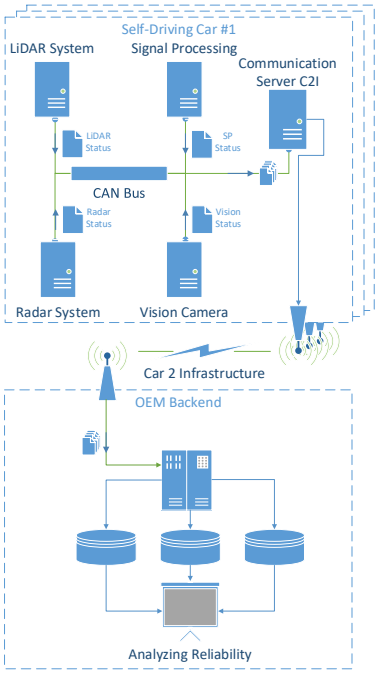

Fig. 2. Use case overview of the live FIT Monitor for safety-critical LiDAR sensor systems.

IV. RetroFIT - Live Safety Monitoring Sensor

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{amb} + P_{dis} \cdot \theta_{ja}})} \quad (4)$$

By combining both equations of the Related Work on component reliability, it becomes obvious that it is possible to calculate the theoretical FIT Rate for a specific temperature as seen in (3). However, component temperature is changing over time which results in different FIT Rates. Therefore, considering these temperature profiles as a time slice in a whole mission profile [9] will be used and integrated in our novel approach of live safety monitoring.

The idea behind our novel approach is to sample the power dissipation and the actual case temperature at a specific time interval. The power dissipation measurements are averaged and saved in a register which represents the average power dissipation of the whole lifetime. The temperature values are classified in a specific temperature range and integrated in a histogram. This histogram represents the whole temperature history of the integrated circuit during lifetime and can be used for further component reliability computations.

For calculating the FIT Rate at a specific time, the following steps are necessary:

1) Calculate FIT Rate for each Histogram Bin
2) Determine the time span percentage of each Histogram Bin
3) Calculate the FIT Rate for each Histogram Bin

4) Sum up each individual Bin FIT Rates to the overall FIT Rate
5) Determine and check with theoretical lifetime FIT Rate

A. Calculate FIT Rate for each Histogram Bin

Each Histogram Bin represents a specific temperature. In our case, we chose a temperature range between 0°C and 140°C. For each Bin, the specific FIT Rate can be calculated by using equation (3) and (4). These FIT Rates represent the statistical lifetime FIT Rate assuming this device would run on this specific temperature for the whole lifetime.

B. Determine the time span percentage of each Histogram Bin

As a first step, the run-time of the device until this moment is determined. For this purpose, all samples of the whole Histogram are summed up as seen in (5).

$$T_{OR} = \frac{\sum n \cdot T_{SR}}{3600} \tag{5}$$

where:

T_{SR} is sampling rate of the measurements.

The overall run-time can be used to determine the specific amount of run-time for each Histogram Bin as seen in (6).

$$T_{Run} = \frac{T_{SR}}{3600 \cdot T_{OR}} \cdot n \tag{6}$$

where:

T_{SR} is sampling rate of the measurements.
T_{OR} is the whole run-time of the device as calculated in (5).

The equation (6) is used to calculate the run-time for each Histogram Bin. In the next step, the specific FIT Rate considering the specific run-time is calculated.

C. Calculate the FIT Rate for each Histogram Bin

In the next step, the FIT Rate of the whole lifetime of each Histogram Bin is calculated.

$$FIT_{Bin} = \frac{FIT_{RB}}{T_{EL}} \cdot T_{Run} \tag{7}$$

where:

FIT_{RB} is FIT Rate of the specific temperature of the Bin as calculated in (4).
T_{Run} is the whole run-time of the device as calculated in (5).
T_{EL} is the expected lifetime of the semiconductor device that has been selected during design phase.

D. Sum up each individual Bin FIT Rates to the overall FIT Rate

In the last step, all individual FIT Rates of the Bins are summed up to an overall FIT Rate.

$$FIT_{TS} = \sum FIT_{Bin} \tag{8}$$

where:

FIT_{Bin} is FIT Rate of each Bin as calculated in (7).

This value represents the FIT Rate to this specific timestamp and can be compared to the theoretical FIT Rate up to this timestamp as well as the theoretical FIT Rate until the end of the expected lifetime.

E. Determine and check with theoretical lifetime FIT Rate

In the last step, we observe if the FIT Rate of the current timestamp exceeds the theoretical FIT Rate that was chosen during design phase.

$$FIT_{TTS} = FIT_{DS} \cdot \frac{T_{OR}}{T_{EL}} \tag{9}$$

where:

FIT_{DS} is theoretical FIT Rate for a specific temperature as seen in (4).
T_{OR} is run-time of the device until this timestamp as seen in (6).
T_{EL} is the expected lifetime of the semiconductor device that has been selected during design phase.

The ratio between the theoretical FIT Rate and the calculated FIT Rate gives a tendency about the usage of the device and whether there should be any concern due to predicted over-stress until the end of the lifetime.

$$FIT_{Ratio} = \frac{FIT_{TS}}{FIT_{TTS}} \tag{10}$$

Ratios that are greater than one indicate that the device was used too extensively and that there could be over-stress until the end of the expected lifetime. This also increased the theoretical amount of failures until the end of the lifetime. The amount of statistical failures can be determined with equation (11).

$$FIT_{LT} = FIT_{TS} \cdot \frac{T_{EL}}{T_{OR}} \tag{11}$$

where:

FIT_{TS} is the calculated FIT Rate for a specific timestamp as seen in (8).
T_{OR} is run-time of the device until this timestamp as seen in (6).
T_{EL} is the expected Lifetime of the semiconductor device that has been selected during design phase.

V. Results

We will implement the "RetroFIT" method in a LiDAR system as seen in Figure 3. To evaluate the functionality and behavior of this methodology we implemented this approach in SystemC.

In Figure 4 the architecture of the implemented FIT Monitor can be seen. The architecture consists of the "Environmental and Integrated Circuit Simulation Model" that contains the temperature profile (as seen in Figure 5) curve that will stimulate the FIT Monitor. The histogram will save each sampled value of the temperature as well as the average power dissipation. The last part is the signal processing where the FIT Rates are calculated as described in Section IV. In Figure 5 the upper diagram is showing temperature profile that have been

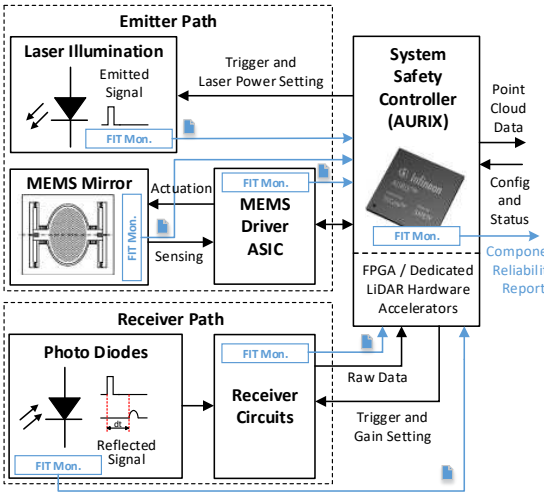

Fig. 3. Live FIT Monitor integration into the safety-critical LiDAR sensor system to enable live safety monitoring [19].

used for our simulation. The lower diagram shows the specific temperature values for each sampling point. In our simulation we have sampled with a frequency of 0.05 Hertz. The related Histogram of our simulation can be seen in Figure 6. Each Histogram Bin represents a 1°C and is distributed on the x-Axis. The amount of samples can be read out on the y-Axis. In our simulation the most samples could be found between 100°C and 110°C. Compared with the temperature profile of Figure 5 this looks plausible.

TABLE I
FIT RESULTS OF OUR SYSTEMC MODEL SIMULATION WITH TEMPERATURE PROFILE INPUT AS SEEN IN FIGURE6.

	FIT_{TS}	FIT_{TTS}	FIT_{LT}	FIT_{RB}	FIT_{Ratio}
FIT in [1]	2.36E-9	2.111E-9	8.5	7.6	1.118

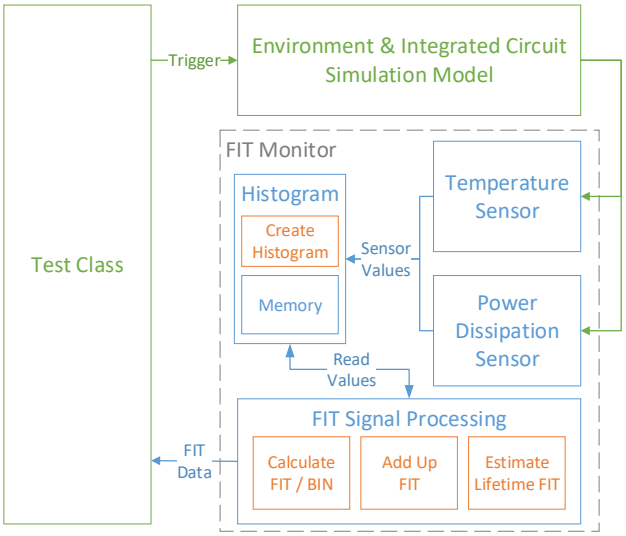

Fig. 4. SystemC model overview of the "RetroFIT" methodology to enable live safety monitoring for safety-critical LiDAR sensor systems.

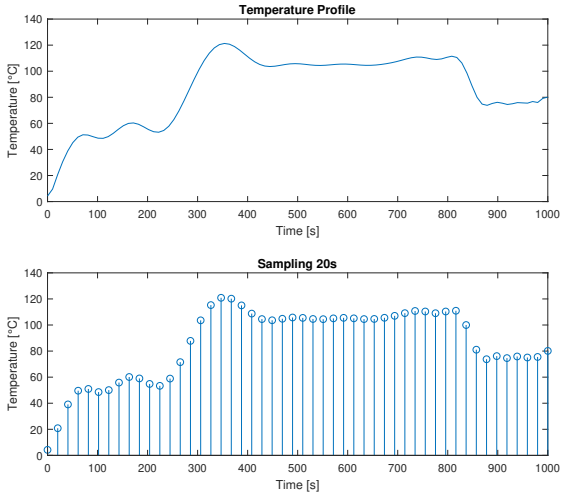

Fig. 5. Measurement results of the "RetroFIT" monitor.

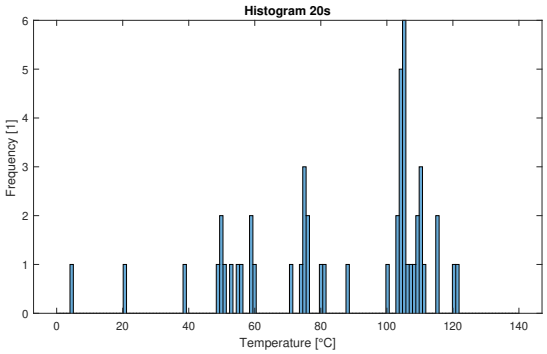

Fig. 6. Histogram results of the "RetroFIT" monitor.

In Table I the FIT results of our SystemC simulation can be seen. The device has an FIT_{RB} value of about 7.6 in 1 Billion operating hours at 100°C. The provided temperature profile, as seen in 5, over-stresses the component and this results in a higher FIT_{LT} of about 8.5. As a result the device has been over-stressed by 11.8%. Consequently, a continuously operated device with this temperature profile would result in a higher FIT Rate than from the designer of the device expected.

VI. SUMMARY

In Section IV, this paper introduces the novel "RetroFIT" sensor to support live safety monitoring of electrical and electronic devices. Nowadays, electronic components such as sensors and micro-controllers fail without any prior indication. Especially for fully automated driving, this circumstance may cause disastrous consequences such as deadly accidents. For future autonomous driving vehicles, our novel method can communicate the actual component reliability.

To give an overview about the application of our novel sensor, we have introduced two common use cases from the customer point of view as well as from the OEM/Supplier point of view. Both cases show that "RetroFIT" has a big impact on the overall road safety as the sensor may for instance trigger component replacement. The values could be obtained

by qualified car repair shops as well as displayed inside the driver's cabin including service deactivation.

In section V, we prove that the sensor concept is feasible and that it is possible to live monitor component reliability for electronic devices.

Fail-operational systems become increasingly essential. Our novel "RetroFIT" sensor enables dynamically changing contracts during run-time. This concept is one of the key enablers of advanced fail-operational systems. Our sensor enables the communication of the actual ASIL level of components and communicates these values to other systems. This will detect ASIL degradation during run-time and trigger safety related functions to increase the overall system safety.

Acknowledgments

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

References

[1] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "Prystine - programmable systems for intelligence in automobiles," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, Aug 2018, pp. 618–626.

[2] R. Faria, L. Brito, K. Baras, and J. Silva, "Smart mobility: A survey," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, July 2017, pp. 1–8.

[3] Mmpro. [Online]. Available: https://publicarea.admiralcloud.com/p/a49d3d8ba92f3cdbfa864f

[4] M. Dikmen and C. Burns, "Trust in autonomous vehicles: The case of tesla autopilot and summon," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct 2017, pp. 1093–1098.

[5] "Accident investigations." [Online]. Available: https://www.ntsb.gov/investigations/Pages/HWY18FH011.aspx

[6] F. Lambert, Fred, and Electrek, May 2018. [Online]. Available: https://electrek.co/2018/05/09/tesla-model-s-fatal-crash-fire-national/

[7] S. Levin, "Tesla fatal crash: 'autopilot' mode sped up car before driver killed, report finds," Jun 2018. [Online]. Available: https://www.theguardian.com/technology/2018/jun/07/tesla-fatal-crash-silicon-valley-autopilot-mode-report

[8] R. Mariani, "An overview of autonomous vehicles safety," in *2018 IEEE International Reliability Physics Symposium (IRPS)*, March 2018, pp. 6A.1–1–6A.1–6.

[9] I. n. E. ISO, "Draft 26262 2nd Edition: Road vehicles-Functional safety," *International Standard ISO/FDIS*, vol. 26262, 2018.

[10] T. Amorim, D. Ratasich, G. Macher, A. Ruiz, D. Schneider, M. Driussi, and R. Grosu, "Runtime safety assurance for adaptive cyber-physical systems: Conserts m and ontology-based runtime reconfiguration applied to an automotive case study," in *Solutions for Cyber-Physical Systems Ubiquity*. IGI Global, 2018, pp. 137–168.

[11] N. Leveson, *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011.

[12] H. Shaheen, G. Boschi, G. Harutyunyan, and Y. Zorian, "Advanced ECC solution for automotive SoCs," in *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS)*, July 2017, pp. 71–73.

[13] D. Sargsyan, "Iso 26262 compliant memory bist architecture," in *2017 Computer Science and Information Technologies (CSIT)*, Sept 2017, pp. 78–82.

[14] P. A. Smith and D. V. Campbell, "A practical implementation of bics for safety-critical applications," in *Proceedings 2000 IEEE International Workshop on Defect Based Testing (Cat. No.PR00637)*, April 2000, pp. 51–56.

[15] M. Beckler and R. D. Blanton, "On-chip diagnosis for early-life and wear-out failures," in *2012 IEEE International Test Conference*, Nov 2012, pp. 1–10.

[16] V. Szekely, M. Rencz, J. M. Karam, M. Lubaszewski, and B. Courtois, "Thermal monitoring of safety-critical integrated systems," in *Proceedings of the Fifth Asian Test Symposium (ATS'96)*, Nov 1996, pp. 282–288.

[17] T. IEC, "62380," *Reliability data handbook–universal model for reliability prediction of electronics components, PCBs and equipment (emerged from UTEC 80-810 or RDF 2000)*, 2004.

[18] "Reliability report," Jul 2018. [Online]. Available: https://www.intel.com/content/www/us/en/programmable/support/quality-and-reliability/reports-tools/reliability-report/rel-report.html

[19] N. Druml, I. Maksymova, T. Thurner, D. Van Lierop, M. Hennecke, and A. Foroutan, "1D MEMS Micro-Scanning LiDAR," in *Conference on Sensor Device Technologies and Applications (SENSORDEVICES)*, 09 2018.

This full text paper was peer-reviewed at the direction of IEEE Instrumentation and Measurement Society prior to the acceptance and publication.

Speed-Up of MEMS Mirror's Transient Start-Up Procedure

Andreas Strasser†, Philipp Stelzer†, Christian Steger† and Norbert Druml*
†Graz University of Technology, Graz, Austria
email:{strasser, stelzer, steger}@tugraz.at
*Infineon Technologies Austria AG, Graz, Austria
email:{norbert.druml}@infineon.com

***Abstract*—Light Detection and Ranging (LiDAR) sensors are the next generation of Advanced Driver-Assistance Systems (ADAS). This device will be a key enabler for automated driving. As a consequence these devices must be highly robust, fail-operational and safe. In this paper we introduce a novel concept to speed-up the start-up procedure of 1D MEMS Micro-Scanning LiDAR systems to enable quick recovery after unexpected fatal shocks to ensure safe driving for passengers and other road participants.**

***Index Terms*—MEMS Mirror, LiDAR, LiDAR Safety , Start-Up Phase, LiDAR Optimization**

I. Introduction

In the next few years, autonomous driving will disruptively change the automotive industry as well as our society [1]. Autonomous driving is one of the key enablers for smart mobility. Smart mobility will change the urban environment by connecting vehicles, infrastructures and citizens together and enables resource-efficient short-distance traffic [2]. In Europe several partners founded "PRYSTINE" (Programmable Systems for Intelligenze in Automobiles), a research project that focus on the development of next-generation Advanced Driver-Assistance Systems (ADAS). PRYSTINE's focus is on the development of a fail-operational urban surround pereception system, containing robust RADAR and LiDAR (Light Detection and Ranging) systems [1]. RADAR is already a proven technology in the automotive industry and can already been found in middle-class vehicles. The RADARs are used in ADAS such as the Adaptive Cruise Control (ACC) to avoid collissions. [3]. The LiDAR technology instead can not been found in middle-class vehicles yet, but there are feasbility studies such as Google's Waymo project [4]. The LiDAR system of Google's research car contains a mechanical rotating LiDAR system [5], this device has the big disadvantage that it is mounted on top of the car and influences the aerodynamic negative and is rather expensive [6], [7]. A smarter approach is the novel LiDAR concept of Druml et al. with their 1D MEMS Micro-Scanning LiDAR system as seen in Figure 2 [8]. Their approach integrates the rotating mirror into a Micro-Electro-Mechanical system (MEMS). This will decrease the overall costs and enables an integration inside the driver cabin without any negative influence on vehicle's aerodynamics [8].

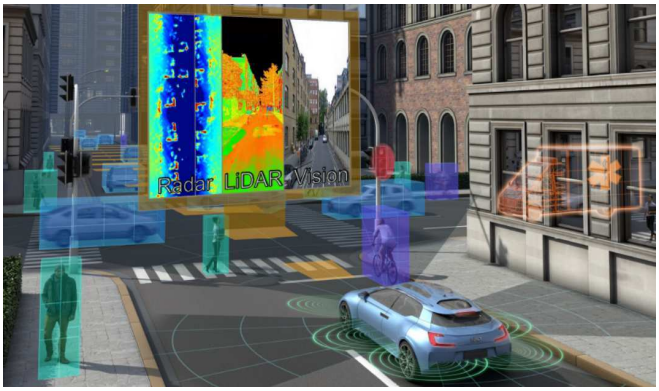

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

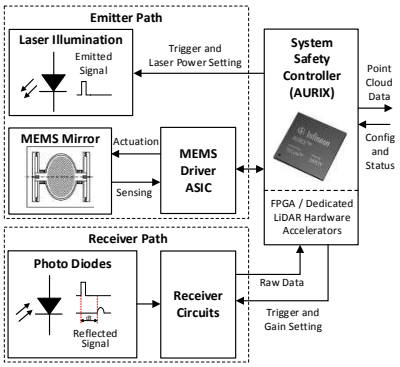

Fig. 2. Overview of a LiDAR system for automonomous driving [8].

LiDAR systems will be a major key enabler for autonomous driving for Level 3 driving automation of the SAE's automation levels [1]. On Level 3 the drivers can move their eyes off the street and enjoy a movie during their trip. For this driving automation level the provided systems needs to have a high level of safety, reliability and must be fail-operational [1]. One of the most critical situation of the 1D MEMS Micro-Scanning LiDAR system is the long duration of the transient start-up procedure of the MEMS mirror until it can operate. In general the long duration would be no problem, if the mirror is starting at engine start and turned off when the engine stops. Unfortunately, the MEMS mirror is sensitive to fatal shocks. In this situation, the shock influences the MEMS mirror and could disrupt the functionality of the whole LiDAR system. In such a situation, there is only the

978-1-5386-7713-1/19/$31.00 ©2019 IEEE

possibility to restart the transient start-up procedure of the MEMS mirror. The problem in that case is, that during the start-up phase the LiDAR system is not able to recognize any deviations on the street and could cause an accident. Consequently this start-up procedure needs to be as fast as possible to recover safely after a shock in a specific time to mitigate possible accidents.

II. Related Work

MEMS mirrors are already used as optical scanners in different fields to enable a two dimensional movement of a laser [7], [9], [10]. In most applications, the occurance of strong vibrations and their consequences on the MEMS mirrors are neglected because mostly these systems are deployed for non-moving applications such as terahertz wave generators or coherent light sources [10]. In the last years the MEMS mirror technology has been introduced in the automotive domain to enable cheap and robust LiDAR systems for supporting automated driving [8], [11], [12].

A. 1D MEMS Micro-Scanning LiDAR

Druml et al. have introduced a novel 1D MEMS LiDAR concept, as seen in Figure 3. This concept offers a high measurement range, represents a low-cost design is highly robust against shocks and vibrations and provides ASIL-C safety level [8].

The LiDAR system can be operated in open and closed control-loop. Both loops are used to guarantee a robust scan shape. In Figure 4 the direction of the mirror and the related signal states are displayed. The phased-locked loop (PLL) follows the oscillating MEMS mirror and adapts the values of the internal control registers to ensure a correct continous operation [8].

Druml et al. describes that, because of the high Q factor of the mirror, the design is highly robust against external perturbations such as shocks or vibrations [8]. Consequently shocks and vibrations needs to be considered for LiDAR systems in the automotive domain.

B. Vibration Effects on LiDAR systems

The effects of exposed vibrations on LiDAR systems have already been examined for airborne LIDAR systems. Hongchao et al. [13] presented in their results that vibrations could cause positioning errors.

Both paper clearly shows that the effects of vibrations on LiDAR systems should not be neglected in the automotive domain. Automotive vehicles and their components are strongly exposed to vibrations during lifetime through different road conditions. MEMS mirrors are minimized mechanical structures and could be affected by these vibrations.

The automotive domain already considers vibration exposures

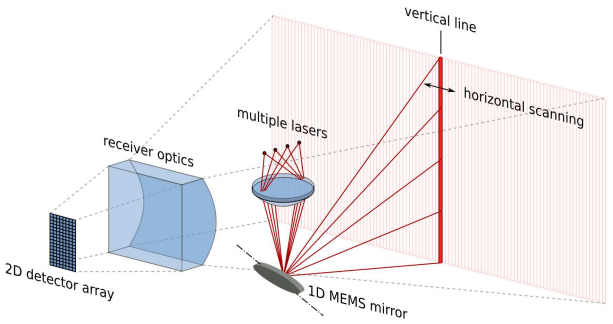

Fig. 3. Concept overview of the 1D MEMS Micro-Scanning LiDAR system of Druml [8].

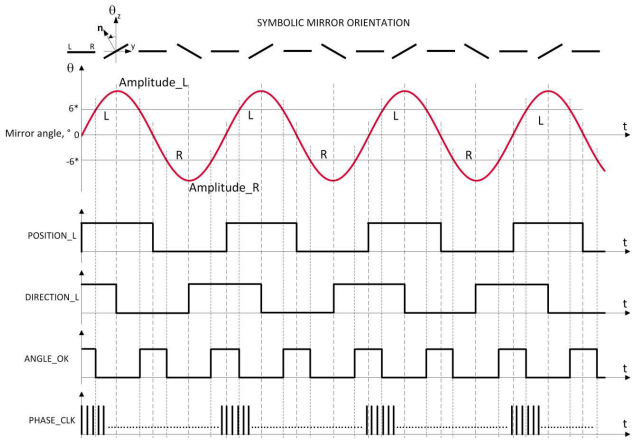

Fig. 4. Signal overview of the 1D MEMS Micro-Scanning LiDAR system of Druml [8].

on mechanical components such as mechanical connectors. For mechanical connectors the automotive domain has developed industrial standards such as “USCAR-2” [14] or “LV 214” [15] that specify certain requirements that must be fullfilled to guarantee safety along appalling road conditions. For MEMS based LiDAR systems, these vibrations could result in an fatal shock that could trigger an immediate stop of the whole LiDAR system. The usual recover-procedure in this case is to restart the whole MEMS mirror.

These circumstances arises several research questions that we are focussing in this paper:

- Is it possible to disrupt the LiDAR MEMS mirror through a fatal shock?
- How long does the state-of-the-art transiert start-up procedure take to recover the MEMS mirror to a certain frequency?
- Could the start-up procedure be accelerated to minimize the recovery time?

III. Speed-Up MEMS Mirror’s Start-Up Procedure

In this section we provide system architecture information about the state-of-the-art start-up procedure and our novel approach to speed-up the common start-up procedure. To

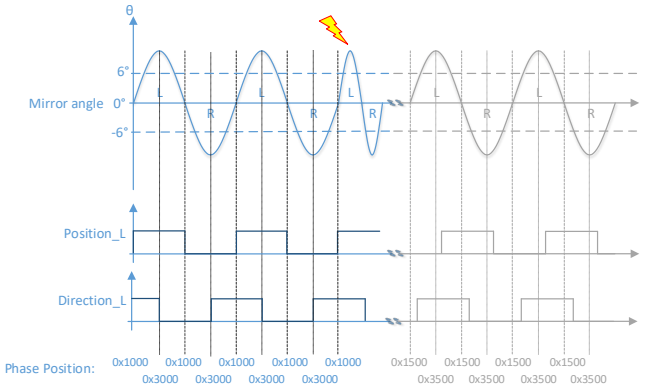

Fig. 5. Concept overview of the impacts of an unintended shock on the LiDAR signals.

clarify the needs of this improvement we firstly describe a case, where the novel 1D MEMS Micro-Scanning LiDAR system by Druml et al. could fail [8].

A. Shock Injection

In Figure 5 the mirror's angle and the related position and direction signal can be seen. The first two cycles are equivalent to the signals of Figure 4. At the beginning of the third cycle a fatal shock occurs and negatively affects the MEMS mirror. This could be seen in a rapidly frequence change of the mirror's angle. First of all, the mirror is possible to recover himself to the previous settled frequency, but the position and the direction signals do not match anymore. In Figure 6 the described worst-case is depicted: a fatal shock causes the PLL to loose its lock. The shock was triggered by a hardware module that simulates the impacts of a fatal shock. The consequences of the shock could be seen through the rapidly increase of the PLL error. The PLL fails and with the PLL the settlement of the control register values. The MEMS mirror is sliding down to a lower frequency due to the PLL that lost its lock. At this state the LiDAR system could not

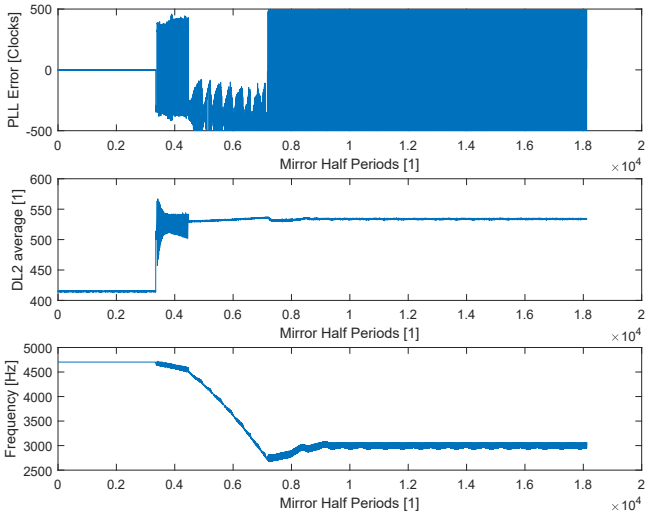

Fig. 6. Measurments and effects of a PLL lock loose, possible triggered by a fatal shock to the LiDAR system.

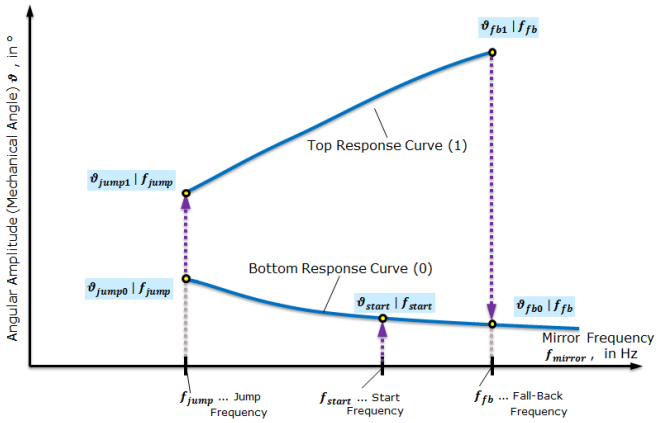

Fig. 7. Overview of both resonance curves of the MEMS mirror [8].

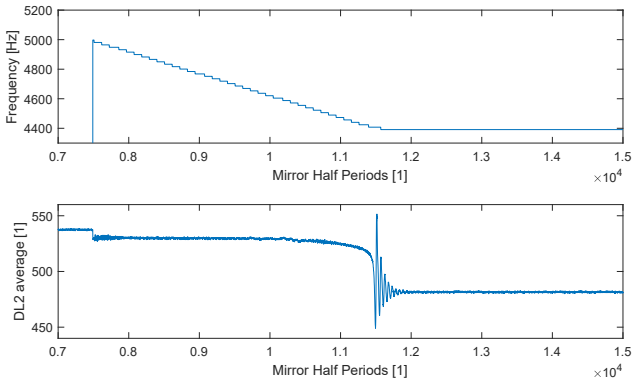

Fig. 8. State-of-the-Art start-up procedure of the 1D MEMS Micro-Scanning LiDAR system.

find back to the previous operating point and recovery is only possible through a MEMS mirror restart.

B. State-of-the-Art Start-Up Procedure

In Figure 8 the transient response of the state-of-the-art start-up procedure can be seen. The mirror provides a top and a bottom resonance curve. The mirror is starting on the lower curve and needs to be driven to the jump frequency. At this jump frequency, the MEMS mirror is jumping on the top response curve [8]. Consequently the start-up routine starts at 5000 Hz and decreases the frequency until the MEMS mirror is jumping onto the top response curve. The response of the top curve can bee seen in Figure 8 at the average mirror current DL2 signal. The conservative start-up procedure needs about 430 ms until the mirror can be used for signal processing. Consequently during this time the LiDAR system has no possibility to send any data to the automated driving signal processing units.

This amount of time would be no problem, if the MEMS mirror would start at engine start and stop at engine off. But there is always the possibility of a fatal shock during run-time, as we have shown in Figure 5 and Figure 6. As a consequence, to ensure safe behavior during run-time this start-up procedure needs to speed-up.

C. Novel Start-Up Procedure

To speed-up the start-up procedure it is necessary to set the specific jump frequency. But the jump frequency needs different additional settings such as counter settings of the PLL. These values are MEMS mirror related and vary for each device. In Figure 9 a functional overview of our novel start-up procedure can be seen. At first start-up of the mirror device the specific jump frequency and all related signals need to be found with the help of a calibration procedure. If these values are already saved in the specific registers the MEMS mirror can immediately be forced to this specific frequency. This frequency point will trigger the jump onto the top response curve. The novel start-up procedure can be divided into two logical branches:

1) **Initial Start-Up**
   Jump frequency and related signals are not known and the device is started for the first time.
2) **Continuous Start-Up**
   Jump frequency and related signals are known and saved in the specific registers.

Firstly the MEMS mirror driver is checking if the jump frequency and all related counter signals are set in the specific registers. If not, the "Initial Startup" path will be executed. In this path the state-of-the-art start-up procedure will be executed. When the jump occurs the MEMS mirror driver is saving all related counter parameters into registers. In the next start-ups these values could be used for speeding-up the start-up procedure.

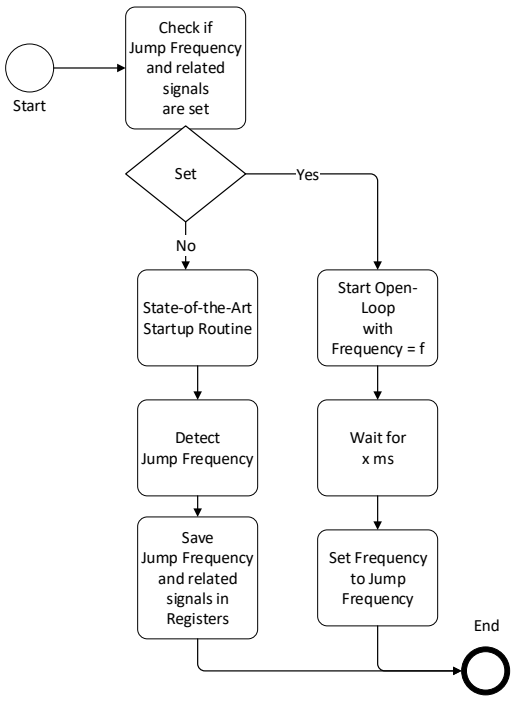

Fig. 9. Functional overview of our novel start-up procedure for speeding up the recovery time.

IV. Results

In this section we provide measurement results of our novel start-up procedure that was introduced in Section III-C.

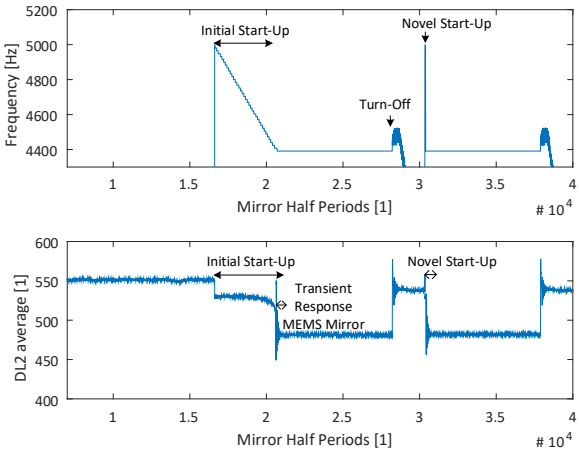

Fig. 10. Initial start-Up measurement of the novel start-up procedure.

In Figure 10 the whole start-up process of our novel start-up procedure can be seen. In the Initial start-up phase the jump frequency and the related signals are not saved in the specific registers. Therefore the MEMS mirror driver triggers the Initial start-up phase. The measurements clearly shows the state-of-the-art start-up procedure. In the next phase the MEMS mirror firstly gets stopped. At the next start-up the MEMS mirror jump frequency and related signals are known and set and the MEMS mirror can immediately jump onto the top resonance curve.

In Figure 11 the magnified Continous start-up phase can be seen. The Continous start-up phase needs about 5.2 ms until the MEMS mirror is ready to proceed.

Figure 12 clearly shows that our novel methodology also works with pre-saved values into the specific registers.

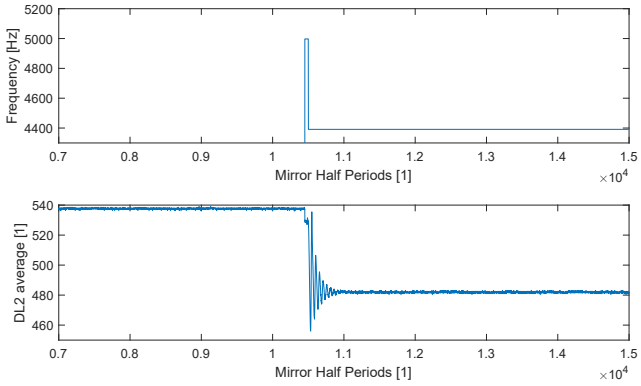

Fig. 11. Magnification of the Continous start-up phase of the novel start-up procedure.

TABLE I
MEASUREMENT RESULTS OF THE STATE-OF-THE-ART START-UP PROCEDURE AND THE NOVEL START-UP PROCEDURE.

	Begin	End	Time in ms
State-of-the-Art Start-Up	11590	7491	426.97
Novel Start-up	25610	25560	5.20

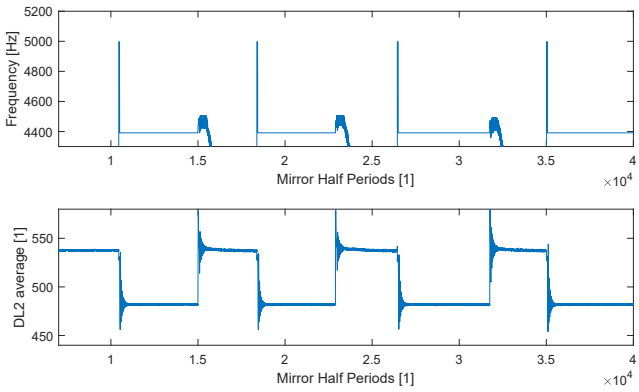

Fig. 12. Novel start-up procedure with pre-saved jump frequency and related signals, including frequent start-stop procedures.

Furthermore Figure 12 proves that it also works for frequent start-stops phases.

V. SUMMARY

In our paper we have introduced a novel start-up procedure for 1D MEMS Micro-Scanning LiDAR systems. The state-of-the-art procedure requires about 430ms until the MEMS mirror is ready to proceed and this is too long for automated driving.

In Section II we have discussed the need of a small recovery time after a fatal shock, probably triggered by appalling road conditions. In Section III-A we have introduced a concept and measurement results, how these shocks will affect the MEMS mirror until the LiDAR system stops working. This result clearly shows that fatal shocks have an impact on the LiDAR system and needs to be mitigated. For this purpose we have designed a novel Start-Up procedure.

In Section III-C we have introduced our novel start-up procedure that is able to shorten the start-up time of the MEMS mirror. In Section IV we have provided measurement results that proves the efficiency of the procedure as well as showing that the start-up phase can be reduced from 430ms to 5.2ms. Furthermore, we have shown that by pre-saving specific signal values into registers this start-up could be speeded up at every start and can also be used for frequent start-stop procedures.

Our novel start-up procedure can be used to quickly recover the MEMS mirror after a fatal shock. With this procedure, the LiDAR system can be recovered in a short time that still ensures safe driving for passangers and road participants.

VI. ACKNOWLEDGMENTS

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

REFERENCES

[1] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "Prystine - programmable systems for intelligence in automobiles," 08 2018.

[2] R. Faria, L. Brito, K. Baras, and J. Silva, "Smart mobility: A survey," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, July 2017, pp. 1–8.

[3] W. Pananurak, S. Thanok, and M. Parnichkun, "Adaptive cruise control for an intelligent vehicle," in *2008 IEEE International Conference on Robotics and Biomimetics*, Feb 2009, pp. 1794–1799.

[4] S. Verghese, "Self-driving cars and lidar," in *Conference on Lasers and Electro-Optics*. Optical Society of America, 2017, p. AM3A.1.

[5] G. Pennecot, P.-Y. Droz, D. E. Ulrich, D. Gruver, Z. Morriss, and A. Levandowski, "Devices and methods for a rotating lidar platform with a shared transmit/receive path," Sep. 16 2014, uS Patent 8,836,922.

[6] Muoiod, "Google just made a big move to bring down the cost of self-driving cars," Jan 2017. [Online]. Available: https://www.businessinsider.de/googles-waymo-reduces-lidar-cost-90-in-effort-to-scale-self-driving-\cars-2017-1?r=US&IR=T

[7] B. Yang, L. Zhou, X. Zhang, S. Koppal, and H. Xie, "A compact mems-based wide-angle optical scanner," in *2017 International Conference on Optical MEMS and Nanophotonics (OMN)*, Aug 2017, pp. 1–2.

[8] N. Druml, I. Maksymova, T. Thurner, D. Van Lierop, M. Hennecke, and A. Foroutan, "1D MEMS Micro-Scanning LiDAR," in *Conference on Sensor Device Technologies and Applications (SENSORDEVICES)*, 09 2018.

[9] X. Zhang, L. Zhou, C. Duan, D. Zheng, S. Koppal, Q. Tanguy, and H. Xie, "A wide-angle immersed mems mirror and its application in optical coherence tomography," in *2016 International Conference on Optical MEMS and Nanophotonics (OMN)*, July 2016, pp. 1–2.

[10] W. M. Zhu, W. Zhang, H. Cai, J. Tamil, B. Liu, T. Bourouina, and A. Q. Liu, "A mems digital mirror for tunable laser wavelength selection," in *TRANSDUCERS 2009 - 2009 International Solid-State Sensors, Actuators and Microsystems Conference*, June 2009, pp. 2206–2209.

[11] L. Ye, G. Zhang, Z. You, and C. Zhang, "A 2d resonant mems scanner with an ultra-compact wedge-like multiplied angle amplification for miniature lidar application," in *2016 IEEE SENSORS*, Oct 2016, pp. 1–3.

[12] U. Hofmann, F. Senger, F. Soerensen, V. Stenchly, B. Jensen, and J. Janes, "Biaxial resonant 7mm-mems mirror for automotive lidar application," in *2012 International Conference on Optical MEMS and Nanophotonics*, Aug 2012, pp. 150–151.

[13] H. Ma and J. Wu, "Analysis of positioning errors caused by platform vibration of airborne lidar system," in *2012 8th IEEE International Symposium on Instrumentation and Control Technology (ISICT) Proceedings*, July 2012, pp. 257–261.

[14] "Performance specification for automotive electrical connector systems uscar2-4." [Online]. Available: https://www.sae.org/standards/content/uscar2-4/

[15] "The impact of lv 214-4, the german automotive oem connector test specification." [Online]. Available: https://www.automationmag.com/education/features/6499-the-impact-of-lv-214-4-the-german-automotive-oem-connector-\test-specification

Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 52-15 (2019) 31–36

Towards Synchronous Mode of Multiple Independently Controlled MEMS Mirrors

Andreas Strasser * **Philipp Stelzer** * **Christian Steger** *
Norbert Druml **

* *Graz University of Technology, Graz, Austria*
{strasser, stelzer, steger}@tugraz.at
** *Infineon Technologies Austria AG, Graz, Austria*
{norbert.druml}@infineon.com

Abstract: Light Detection and Ranging (LiDAR) will be one of the key enablers of smart mobility. Smart mobility creates a fully connected urban environment with graceful benefits for the city such as quality of life, reduced costs and more efficient energy usage. Modern LiDAR systems that are constructed for the automotive industry are using Micro-Electro-Mechanical Systems (MEMS) mirrors. In general, these mirrors are operated independently as a single device from a control system called MEMS Driver. In future, a synchronous mode for independent controlled MEMS mirrors will be crucial for novel applications such as synchronously operating a scanning receiver and emitter.
In this paper we present a feasibility study about controlling multiple independent MEMS mirrors synchronously. For this purpose we created a novel Master-Slave system architecture model that enables synchronization. This proof-of-concept design of the Master-Slave system architecture were implemented in two FPGAs to evaluate the feasibility of synchronizing multiple independent MEMS mirrors.

Keywords: LiDAR MEMS, Mirror Synchronization, MEMS Mirror, Automotive, Synchronization, Automated Driving

1. INTRODUCTION

In the next few years, the everyday life in cities will change through the urban trend of smart mobility. Smart mobility is the generic term for connecting citizens, vehicles, infrastructure and transportation system together to an integral system (Desima et al. (2017)). This system will improve the quality of life, reduce costs, enables efficient energy usage and improves the mobility quality of citizens (Faria et al. (2017)). One of the key enablers for smart mobility, from the automotive domain, are self-driving cars. Self-driving cars have the ability to drive the car on their own decisions and control the vehicle without any interventions from any passenger (Lugano (2017)). This vision has already become reality through Tesla's self-driving functionality called "Autopilot". Tesla's "Autopilot" was the first Advanced driver-assistance system (ADAS) that was able to maneuver the car in urban environments autonomously (Dikmen and Burns (2017)). Tesla's self-driving functionality is based on RADAR, ultrasonic sensors and vision cameras that are able to perceive the environment up to 250m of the car's front (Tesla (2018)). In the last years the system was not flawless and there have been accidents such as the deadly accident in California (Board (2018)). The crash of Wei Huang with his Tesla model is another example that clearly shows the technical limitations of Tesla's current Autopilot design (Stewart (2018)). In this case the Autopilot did not recognize a white truck because it was detected as the sky. Consequently, the use of vision cameras is not sufficient for fail-safe autonomous driving. To enable fail-safe autonomous driving, additional ADAS technologies such as Radar and Light detection and ranging (LiDAR) are necessary. The fusion of Radar, LiDAR and cameras is considered as the best possible solution to enable fail-safe automated driving and is covered through the European research project Programmable Systems for Intelligence in Automobiles (PRYSTINE) (Druml et al. (2018a)). PRYSTINE's focus is on developing a comprehensive environment perception system by using LiDAR, Radar and vision cameras as seen in Figure 1. In the last years Radar has already been implemented in middle-class cars for ADAS such as Adaptive cruise control (ACC)

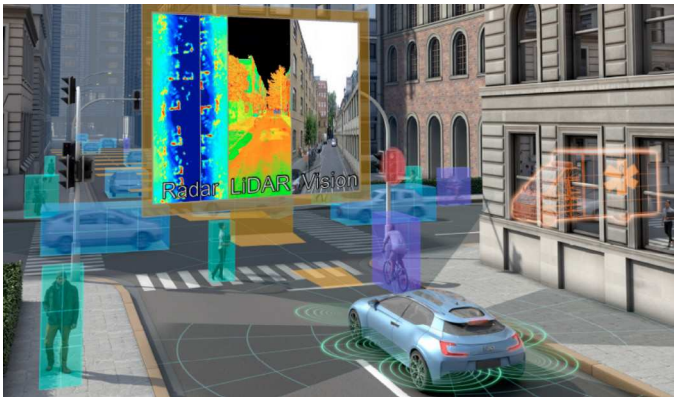

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system (Druml et al., 2018a).

2405-8963
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2019.11.645

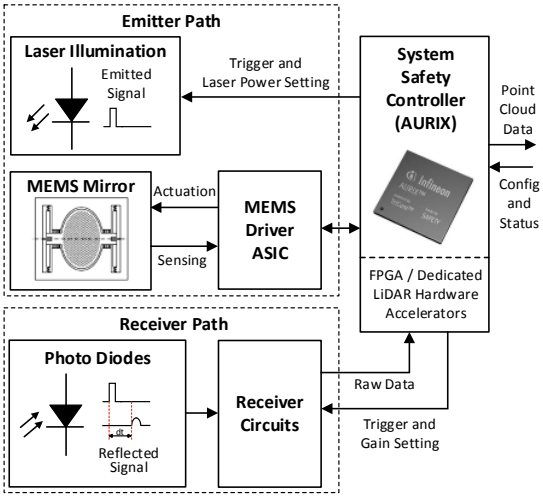

Fig. 2. Overview of a LiDAR system for autonomous driving (Druml et al., 2018b).

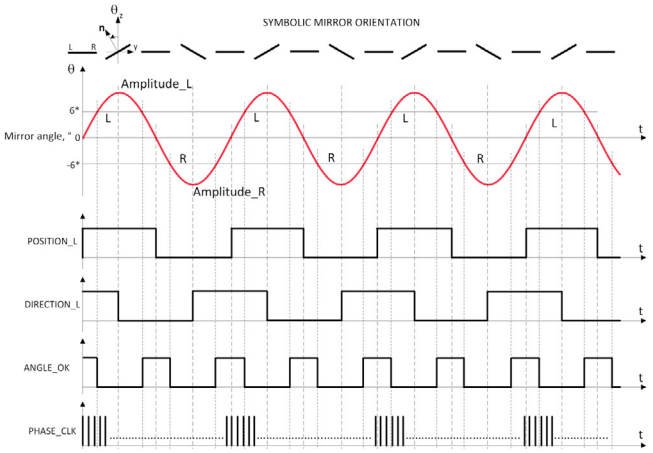

Fig. 3. Signal overview of the 1D MEMS Micro-Scanning LiDAR system (Druml et al., 2018b).

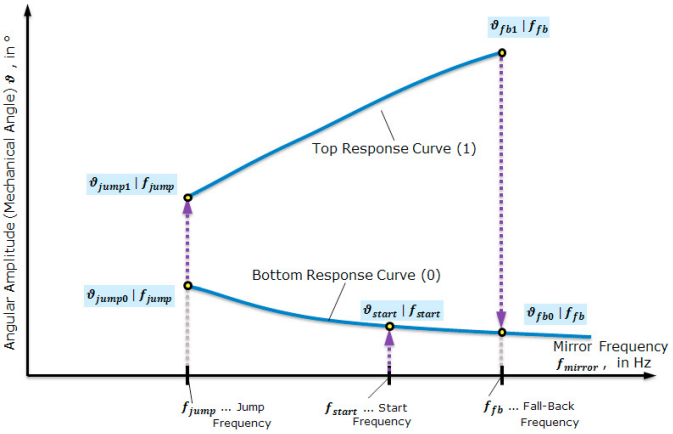

Fig. 4. Overview of both resonance curves of the MEMS mirror (Druml et al., 2018b).

(Eckersten and As (1997)). LiDAR instead has not reached middle-class cars yet, because of the high costs (Muoio (2017)). Another approach that should make LiDAR suitable for the mass of middle-class cars, is the 1D Micro-Electro-Mechanical Systems (MEMS) Micro-Scanning LiDAR system as seen in Figure 2 (Druml et al. (2018b)). Druml et al. introduced this architecture to enable self-driving functionality for Level 3 of the SAE's automation level (Druml et al. (2018a)). The whole design can be integrated in semiconductor devices and this results in a cost efficiency solution.

The design of Druml et al.'s 1D MEMS Micro-Scanning LiDAR system also evolves more complex problems than traditional LiDAR designs such as the synchronization of multiple independently MEMS mirrors. MEMS mirrors vary in their operational characteristics such as maximum operational frequency due to fabrication process variations. In the next few years, novel applications will demand a synchronous mode for independent controlled MEMS mirrors such as synchronously operating a scanning receiver and emitter.. As a result the current 1D MEMS Micro-Scanning LiDAR system should be analyzed for the following research question:

- Is it feasible to run multiple independently controlled MEMS Mirrors in phase and frequency?

2. RELATED WORK

The 1D MEMS Micro-Scanning LiDAR system consists of an Emitter- and Receiver-Path. Both paths are monitored by the system safety controller as seen in Figure 2. The Emitter Path contains the MEMS Mirror, MEMS Driver ASIC and Laser Illumination. The MEMS Driver ASIC is sensing, actuating and controlling the oscillating MEMS Mirror (Druml et al. (2018b)). An oscillation of the MEMS Mirror, as seen in Figure 3, is triggered by applying an on-off signal to the comb fingers of the MEMS Mirror. The on-off timing of the voltage controls the frequency of the MEMS Mirror. One of the characteristics is the non-linear harmonic oscillator characteristics of the MEMS Mirror as seen as top and bottom response curve in Figure 4. The whole resonance curve of the MEMS Mirror is characterized by the f_{jump} and $f_{fallback}$ frequencies and their values vary for each individual MEMS Mirror due to fabrication process variations. If the MEMS Mirror is operated on the top response curve, the frequency can be increased until the $f_{fallback}$ frequency. After reaching this frequency the MEMS Mirror is falling back on the bottom response curve. Falling back from the top response curve to the bottom response curve results in an immediate drop of the angular amplitude and this results in a lower field of view. For controlling a single MEMS Mirror this problem can be avoided by stopping the frequency increase before the $f_{fallback}$ frequency. This mitigation can not be used for running multiple independent MEMS Mirrors synchronously, because each individual Mirror has a different $f_{fallback}$ frequency. In this case, the lowest $f_{fallback}$ frequency of all MEMS Mirrors must be considered to ensure the operation on the top response curve of all MEMS Mirrors simultaneously.

The MEMS Driver ASIC is also communicating the Position and Direction signals. Both signals can be used to determine the orientation of the MEMS Mirror. If the MEMS Mirror is crossing the horizontal position to the left, then the Position signal is communicating a logical High value and for the right side a logical Low value as seen in Figure 3.

MEMS Mirrors have already been used in different do-

mains such as optical coherence tomography (Zhang et al. (2016)). Most of the research papers about MEMS Mirrors are describing the characteristics and capabilities of their current designs (Bauer et al. (2012), Liu and Xie (2012), Zhu et al. (2009)).
As of yet, no publication is available that covers the problem about synchronizing two independent MEMS Mirrors together. Therefore, in this paper we will focus on the following research tasks:

- Design of a master-slave synchronization system architecture design.
- Implementing a first feasibility study, using rapid prototyping, of a synchronous master-slave system.
- Measuring the synchronization process and evaluating the feasibility of synchronizing independently controlled MEMS Mirrors.

3. MASTER-SLAVE SYNCHRONIZATION SYSTEM ARCHITECTURE

The following Master-Slave synchronization system architecture represents a first rapid prototyping architecture that was created to perform a feasibility study on synchronizing two independently controlled MEMS Mirrors. The idea behind synchronizing two independently controlled MEMS Mirrors is depicted in Figure 5. The whole synchronization system can be separated in a master and a slave MEMS Driver. The master is communicating the actual zero crossing signal of his MEMS Mirror to the slave MEMS Driver. The slave is forwarding this signal into his Phase-locked loop (PLL). In Figure 6 the functional overview of the slave PLL can be seen and is separated in:

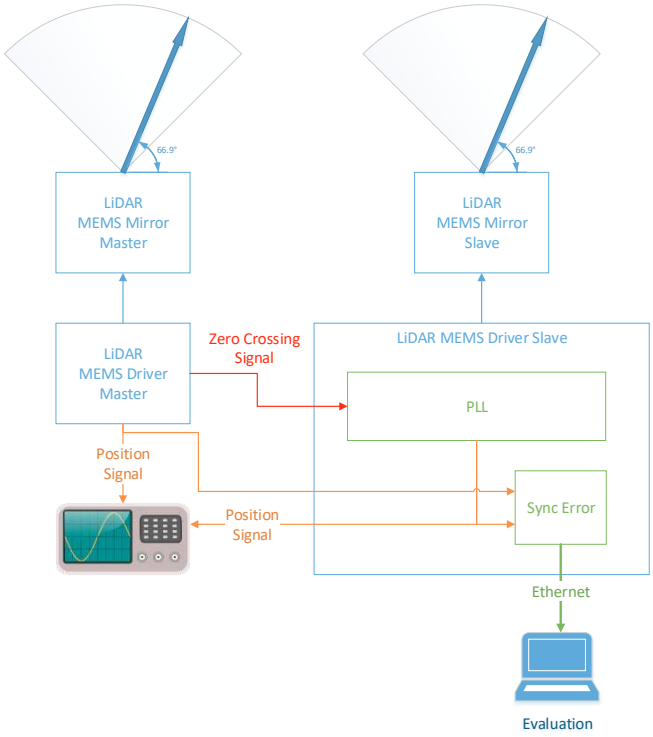

Fig. 5. Concept overview of the synchronization mode of two independently controlled MEMS Mirrors.

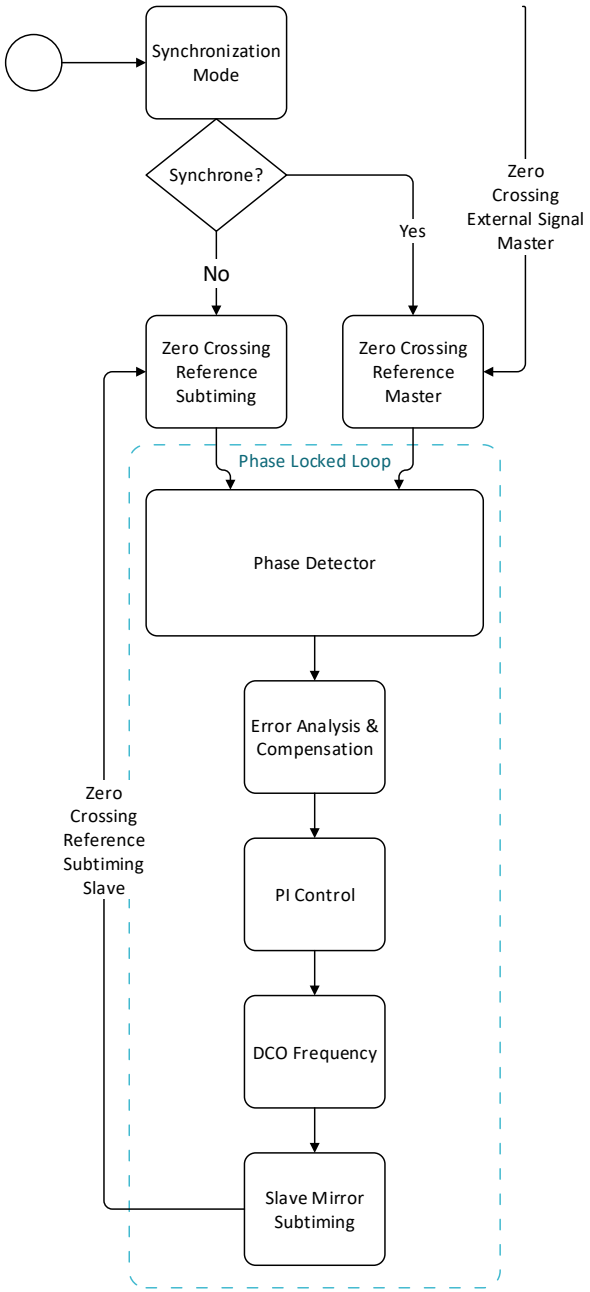

Fig. 6. Overview of the slave Phase-locked loop.

(1) **Synchronization Mode**
The slave can be configured to work synchronously or asynchronously during run-time. In asynchronous mode, the PLL of the MEMS Driver is getting a zero crossing reference signal of his own MEMS Mirror that allows him to precisely following the movement of the oscillating slave MEMS Mirror (Druml et al. (2018b)). In synchronous mode, the slave MEMS Driver receives the zero crossing reference signal of the master's MEMS Mirror.

(2) **Zero Crossing Reference**
The Zero Crossing Reference signal is a necessary input for the PLL. This signal is used as a control parameter to evaluate a mismatch such as analog delays between the MEMS Driver's internal desired

zero crossing and the actual zero crossing of the MEMS Mirror. The internal zero crossing reference is generated by the Subtiming block and the actual zero crossing reference is a comparator signal that is triggered by the analog MEMS Mirror.

(a) **Phase Detector**
The Phase Detector is responsible to detect a mismatch between the internal zero crossing signal of the MEMS Driver and the comparator signal. In this case the Phase Detector is changing an internal counter called PLL error. If the internal signal is leading in phase, than the PLL error will be decreased and for lagging in phase increased. The final error value will be transmitted to the Error Analysis and Compensation block.

(b) **Error Analysis and Compensation**
The Error Analysis and Compensation block is responsible to filter periodic error signals caused by the asymmetry of the MEMS Mirrors.

(c) **PI Control**
The filtered error value is transmitted into the PI control block that is calculating an increment value for the Digitally Controlled Oscillator (DCO) Frequency block.

(d) **DCO Frequency**
The DCO Frequency derives his own output frequency on the set increment value of the PI block. Based on this frequency the internal Mirror Subtiming counter is driven.

(e) **Slave Mirror Subtiming**
The Slave Mirror Subtiming block contains an internal counter that divides the MEMS Mirror's half period into phase slices. This counter is used as a central scheduler of all MEMS Driver's activities such as switching the power supply of the MEMS Mirror on and off. By changing the on-off values of the power supply, the MEMS Mirror can be accelerated or slowed-down.

3.1 Limitations and Challenges

The introduced novel Master-Slave synchronization system architecture is a first rapid prototyping approach that focusing on evaluating the feasibility of synchronizing two independently running MEMS Mirrors. This design still has drawbacks that must be considered in future architectures such as robustness.
In general, MEMS Mirrors are operated at a specific oscillating frequency and this frequency will be kept. The compliance between the adjusted frequency of the MEMS Driver and of the actual MEMS Mirror frequency is controlled by the MEMS Driver PLL. But there could arise circumstances that affect this control system such as strong unintended shocks. These shocks can appear during run-time and misalign the internal generated zero crossing reference and the actual zero crossing reference of the MEMS Mirror that much that both signals can not be back aligned together without specific recovery strategies. Especially, if the slave MEMS Mirror is not feed backing his own zero crossing reference because in synchronous mode the master's MEMS Mirror zero crossing signal reference is active than any unintended shock will immediately stop the synchronization mode without any chance of automatic recovery. In this case, a future robust synchronization architecture must consider the occurrence of unintended shocks and start recovering automatically.

4. RESULTS

For the test setup we have used two separate MEMS Drivers. One is used as a master that outputs his zero crossing reference of his MEMS mirror on a specific pin. The other device was used as a slave that receives the zero crossing reference on a specific pin. Both pins were connected with a single wire. Both devices output their Position signals and these pins are connected to a oscilloscope.
The test case was separated into the phases:

(1) Initialize the master and slave devices independently and run in asynchronous mode.
(2) Activate the synchronous mode on the slave device.

4.1 Initialize the master and slave devices independently and run in asynchronous mode

Firstly, we had to start the master device to run the MEMS Mirror at a specific frequency. In Figure 7 master's MEMS mirror frequency is depicted. At the whole test-run, the frequency was steady at 4620 Hz. The DL2 average measurement is necessary to check, if the MEMS Mirror is running stable. In this case the MEMS Mirror is running fine.

4.2 Activate the synchronous mode on the slave device

After the master MEMS Driver is up and running, it is necessary to start the slave device. The slave device will start-up in asynchronous mode and the slave MEMS Mirror is oscillating asynchronously to the master's MEMS Mirror. Secondly, we deactivate the feedback loop of the PLL.
After deactivation, the slave's MEMS Mirror comparator zero crossing signal and the slave's mirror subtiming

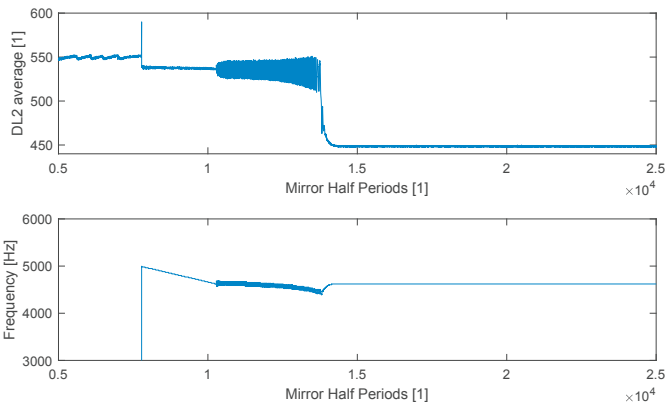

Fig. 7. Measurements of running the master at a frequency of 4620 Hz.

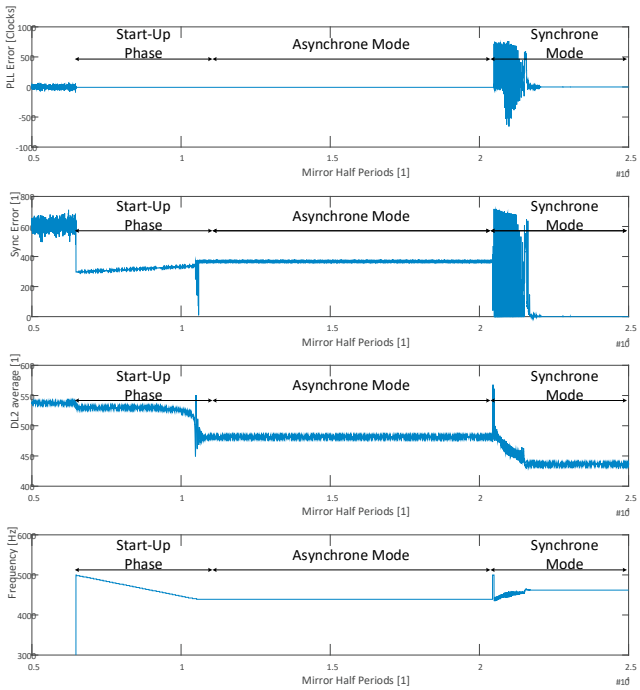

Fig. 8. Measurements of the whole slave test-run changing from asynchronous mode to synchronous mode.

generated zero crossing signal are still aligned, as long as the frequency of the MEMS Mirror is not changing due to strong shocks. The Phase Detector of the PLL is getting the Zero Crossing signal of master's MEMS Mirror. This leads to a misalignment between the slave's internal defined zero crossing reference of the Subtiming block and the master's zero crossing signal of the MEMS Mirror and results in an error value by the Phase Detector block. The PI control block is receiving this error value and transmits an incremental value to the DCO that triggers a frequency adaption of the DCO block. The DCO frequency change is influencing the subtiming counter of the slave's MEMS Driver Subtiming block. This subtiming counter is a central scheduler of all MEMS Driver's activities, in this case the MEMS Driver will adapt the on-off timings of the slave MEMS Mirror.

After this procedure, the slave's MEMS Mirror is running synchronously with master's MEMS Mirror at the same frequency and phase. The evaluation, whether both MEMS Mirrors are running at the same frequency and phase is evaluated by a Sync Error module. This module is looking for the Position signal of master and slave. If one of the signals gets high and the other is still low, then the Sync Error module is changing his counter as seen in Figure 9. Additionally, a measurement is established over an oscilloscope that gets also the Position signal of master and slave. If both signals are aligned one above the other, then the synchronization was successfully.

In Figure 8 the individual states of the slave's MEMS Driver can be observed. The first sector is called "Start-UP Phase" and is necessary to activate the oscillation of the slave's MEMS Mirror. After this phase, the slave is running asynchronously to the master. Towards the activation of the synchronous mode, the slave is receiving master's zero crossing signal and is executing the steps described in Figure 6. At the Sync Error measurement results it is

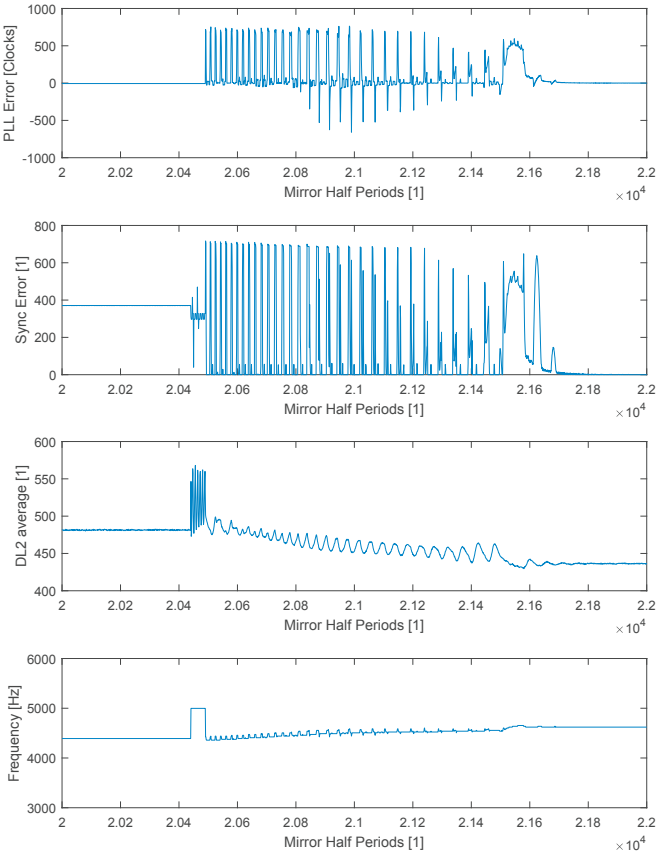

Fig. 9. Synchronization details of the slave.

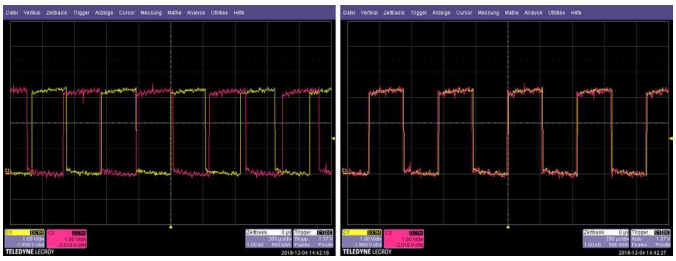

Fig. 10. Asynchronous (left) and Synchronous (right) signals of slave and master MEMS Driver.

obvious that both MEMS Mirrors are in phase and have the same frequency as the error is decreasing to zero. The oscilloscope results also show that both position signals are in phase as seen in Figure 10.

Table 1. Measurement results of the synchronization time between master and slave.

	t_{Start} in [1]	t_{Stop} in [1]	t in [ms]	f_{Start} in [Hz]	f_{Stop} in [Hz]
Master	-	-	-	4620	4620
Slave	20500	21700	125	4391	4620

Table 1 shows the timing of the synchronization process. The synchronization between slave and master took about 125 ms and changed from 4391 Hz to 4620 Hz.

The measurement results of Figure 8, clearly shows that the synchronization between two independently controlled MEMS Mirrors is possible.

5. CONCLUSION

In this paper we have introduced a novel master-slave synchronization system architecture that enables a synchronous operation of two independently controlled MEMS Mirrors. The system architecture was implemented in an FPGA that functioned as an explorative MEMS Driver prototype platform. Afterwards the system architecture was evaluated by measuring the internal states of the slave's MEMS Driver as well as measuring the Position signals of master and slave with an oscilloscope.
First of all, our results clearly depict that the synchronization of two independently controlled MEMS Mirrors is working and also that the novel master-slave synchronization system architecture is working. In our test-run we have adapted the slave MEMS Mirror frequency from 4391 Hz to 4620 Hz in 125 ms. The adaption was controlled automatically by the slave's PLL.
It is important to understand that our master-slave synchronization system architecture was used to evaluate the feasibility of synchronizing two independent MEMS Mirrors. This design is not robust and not applicable for operation mode. Consequently, further improvements are necessary to enable robustness against shocks and frequency changes of master's MEMS Mirror. But our results clearly shows that synchronization between two independent MEMS Mirrors is feasible.

6. ACKNOWLEDGMENTS

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

REFERENCES

Bauer, R., Lubeigt, W., and Uttamchandani, D. (2012). Q-switching of nd:yag solid-state laser with intra-cavity mems resonant scanning mirror. In *2012 International Conference on Optical MEMS and Nanophotonics*, 81–82.

Board, N.T.S. (2018). Car with automated vehicle controls crashes into roadway barrier. URL `https://www.ntsb.gov/investigations/Pages/HWY18FH011.aspx`.

Desima, M.A., Lindawati, Faishal, M., and Permana, Y.E. (2017). Design of smart mobility application to realize sukabumi smart cities. In *2017 International Conference on Computing, Engineering, and Design (ICCED)*, 1–4.

Dikmen, M. and Burns, C. (2017). Trust in autonomous vehicles: The case of tesla autopilot and summon. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 1093–1098.

Druml, N., Macher, G., Stolz, M., Armengaud, E., Watzenig, D., Steger, C., Herndl, T., Eckel, A., Ryabokon, A., Hoess, A., Kumar, S., Dimitrakopoulos, G., and Roedig, H. (2018a). Prystine - programmable systems for intelligence in automobiles. In *2018 21st Euromicro Conference on Digital System Design (DSD)*, 618–626.

Druml, N., Maksymova, I., Thurner, T., Van Lierop, D., Hennecke, M., and Foroutan, A. (2018b). 1D MEMS Micro-Scanning LiDAR.

Eckersten, C. and As, B.. (1997). A high performance automotive radar for adaptive cruise control and collision warning/avoidance. In *Proceedings of Conference on Intelligent Transportation Systems*, 446–451.

Faria, R., Brito, L., Baras, K., and Silva, J. (2017). Smart mobility: A survey. In *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, 1–8.

Liu, L. and Xie, H. (2012). Three-dimensional confocal scanning microscope using an mems mirror for lateral scan and an mems lens scanner for depth scan. In *2012 International Conference on Optical MEMS and Nanophotonics*, 158–159.

Lugano, G. (2017). Virtual assistants and self-driving cars. In *2017 15th International Conference on ITS Telecommunications (ITST)*, 1–5.

Muoio, D. (2017). Google just made a big move to bring down the cost of self-driving cars. URL `https://www.businessinsider.de/googles-waymo-reduces-lidar-cost-90-in-effort-to-scale-self-driving-cars-2017`.

Stewart, J. (2018). Tesla's self-driving autopilot involved in another deadly crash. URL `https://www.wired.com/story/tesla-autopilot-self-driving-crash-california/`.

Tesla (2018). Tesla autopilot overview. URL `https://www.tesla.com/autopilot`.

Zhang, X., Zhou, L., Duan, C., Zheng, D., Koppal, S., Tanguy, Q., and Xie, H. (2016). A wide-angle immersed mems mirror and its application in optical coherence tomography. In *2016 International Conference on Optical MEMS and Nanophotonics (OMN)*, 1–2.

Zhu, W.M., Zhang, W., Cai, H., Tamil, J., Liu, B., Bourouina, T., and Liu, A.Q. (2009). A mems digital mirror for tunable laser wavelength selection. In *TRANSDUCERS 2009 - 2009 International Solid-State Sensors, Actuators and Microsystems Conference*, 2206–2209.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

158

HW/SW Co-Design Approach to Optimize Embedded Systems on Reliability

Andreas Strasser, Philipp Stelzer, Christian Steger

Institute of Technical Informatics
Graz University of Technology
Graz, Austria
Email: {strasser, stelzer, steger}@tugraz.at

Norbert Druml

Infineon Technologies Austria AG
Graz, Austria
Email: norbert.druml@infineon.com

***Abstract*—Autonomous driving is disruptively changing the automotive industry. The importance of safety, reliability, and fault-tolerance is steadily increasing through the complexity and autonomy of self-driving cars. In the past, developers relied on the driver as a fail-safe backup to transfer the control and the responsibility to him in case of unexpected faults. In fully autonomous vehicles this backup solution will be not available anymore. This requires novel safety concepts and methodologies such as an optimization of high reliability of the systems. For optimization it is necessary to quantify different algorithm solutions from a safety point of view because this enables the possibility of comparing different solutions. In this publication, we are analyzing the consequences of different hardware and software algorithm implementations on component reliability. For this purpose we have designed two novel algorithm safety validation methodologies that allow the quantification of algorithms from a safety point of view and applied them to two independent use cases to evaluate the effects on component reliability. Both methodologies are used for optimizing the reliability of safety-critical automotive embedded systems for autonomous driving during Hardware/Software Co-Design.**

Keywords–Safety critical systems; Aging of circuits and systems; Safety Validation HW/SW; Failure-in-Time Analysis; Algorithm Safety Evaluation

I. INTRODUCTION

50 years ago started the future about fully autonomous driving. In the 1960s, Continental tested their driver-less car in the Contidrom in Germany. It was used as a prototype for tire testing to ensure constant testing conditions [2]. Nowadays, 50 years later this vision still exists in our society and Tesla has shown that autonomous driving is possible with their "Autopilot" [3]. Tesla has triggered the hype about autonomous driving and has pushed the society into a new era. This new era is changing the individual's daily routines about mobility and enables smart mobility.

Smart mobility will create a fully connected urban environment and will bring benefits to cities, better quality of life, reduced costs and more efficient energy usage [4]. To achieve the goal of autonomous driving and smart mobility, novel Advanced Driver-Assistance Systems (ADAS) are necessary. The two best-known ADAS are the Electronic Stability Control and the Anti-Lock Braking System, especially for their positive effect on active safety. Moreover, in the last years, a new generation of ADAS such as the Adaptive Cruise Control (ACC) has been established in middle class cars to avoid collisions. The next big step is introducing a comprehensive system enabling the perception of urban environment, which is one of the main goals of the PRYSTINE project [5].

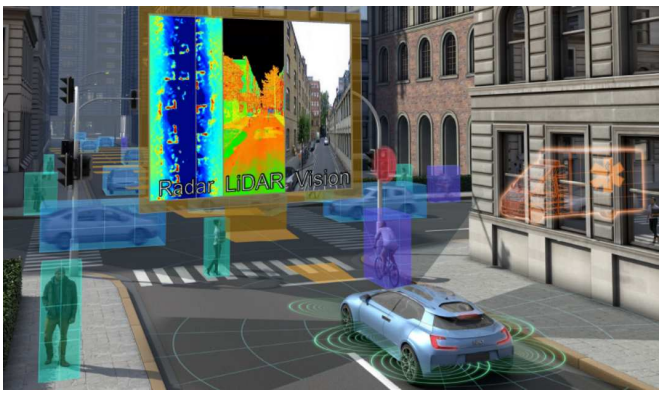

Figure 1. PRYSTINE's concept view of a fail-operational urban surround perception system [5].

PRYSTINE stands for Programmable Systems for Intelligence in Automobiles and is based on robust Radar and LiDAR sensor fusion to enable safe automated driving in urban and rural environments, as seen in Figure 1. These devices must be reliable, safe, and fail-operational to handle safety-critical situations independently [5].

In the past, developers of safety-critical automotive systems generally integrated the driver as the last safety chain link by handling over the control and the responsibility to the driver in unexpected situations or conditions. For fully autonomous vehicles, this fail-safe backup will not be available anymore because these vehicles needs to manage all critical unexpected situations on their own. This requires a rethinking of traditional safety concepts and methodologies. Novel safety-critical automotive embedded systems that will be equipped into autonomous vehicles needs to be high reliable, robust, and fail-operational [5]. One possibility that have been neglected in the past is about optimizing current systems from a safety point of view as increasing the component reliability. For this purpose, novel safety methodologies need to be developed that focus on optimizing embedded systems from a safety point of view.

This publication is an extended Version of the "FITness Assessment-Hardware Algorithm Safety Validation" [1] publication that was presented at the Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

159

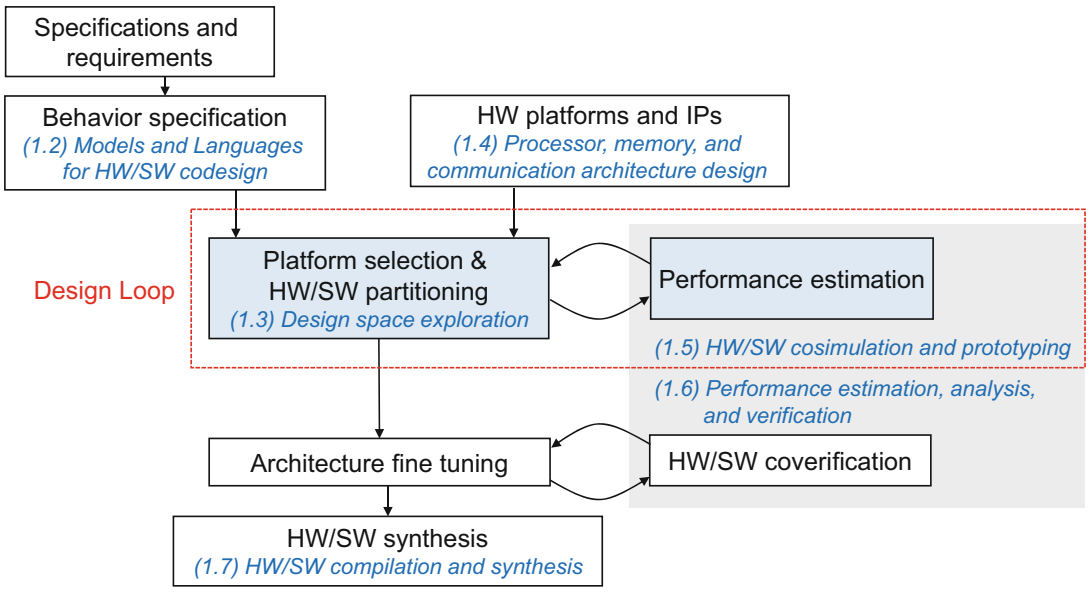

Figure 2. Overview of the HW/SW Co-Design design flow [6].

For this purpose, we will elaborate on the following two research questions:

- How can different hardware language description algorithm implementations be validated from a safety point of view?
- How can different software algorithm implementations be validated from a safety point of view?

The remainder of the paper is structured as follows. Related work will be provided in Section II. The method will be described in detail in Section IV and the results including a short discussion will be provided in Section VI. A summary of the findings will conclude this paper in Section VII.

II. Related Work

This section describes the related work in the field of component reliability considering HW/SW Co-design methodologies, software safety, hardware safety and component reliability.

A. Reliability Focused HW/SW Co-Design Methodologies

Schaumont [7] defines that the HW/SW Co-Design that is depicted in Figure 2 is used to design hardware and software components in a single design effort considering the partitioning and design of an application in terms of fixed and flexible components. In general, the most driving factor for the usage of the HW/SW Co-Design methodology is about making trade-offs, as depicted in Figure 3, between conflicting objectives such as performance, energy efficiency through fixed hardware implementations and flexibility through the usage of software implementations [7].

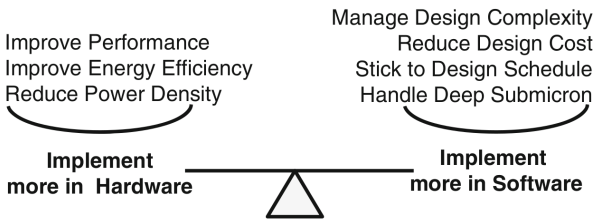

Figure 3. HW/SW Co-Design driving factors [7].

Beside the most common driving factors such as energy and performance there are also other factors that are more important in other domains such as the reliability for safety-critical embedded systems. Vargas et al. [8] introduced a novel HW/SW Co-Design approach that focus on the reliability of the overall system. Their approach decides on the basis of system reliability requirements which parts are partitioned into hardware or software including a verification of the overall reliability of the system. Vargas et al. focused in their publication on the correct function of the overall system and introduced primary hardware redundancy. Another work is the publication of Tosun et al. [9] that focus on soft errors such as bit flips. Both frameworks clearly shows that the overall reliability of safety-critical embedded systems are able to be improved by specific HW/SW Co-Design approaches. Nevertheless, both frameworks do not consider the component reliability of the hardware parts that are measured as the Failure in Time (FIT) Rate.

B. Software Design for Functional Safety

Nancy Leveson is one of the most known safety specialists and have published a book about software safety [10]. In 1995 Leveson described that in general software developers threat the computer as a stimulus-response system and that they seldom look beyond the computer. Consequently, software engineers usually constructed software without thinking about effects of the software on system safety [10]. 23 years later the perception of safety-critical software engineering has been improved and engineers are aware about the influences of software on the overall safety level [11]–[15].

Leveson [10] describes two common methodologies to

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

ensure run-time safety of safety-critical software systems: Dynamic and Static Analysis. Dynamic Analysis is a detection method for software errors or functional errors during run-time. Static Analysis by contrast focuses on formal errors such as race conditions or buffer overflows. Nowadays these two techniques have been advanced to frameworks that enhance the validation process.

Cruickshank et al. [11] have introduced a novel validation metrics framework for validating software safety requirements and have applied the method on a fictitious safety-critical surface-to-air missile system. Cruickshank et al. described that their framework supported the early identification of potential safety problems [11]. Baudin et al. [16] have described their novel tool for safety validation called "CAVEAT". CAVEAT is a statistical analysis tool to verify safety critical software and is used by Airbus to validate pieces of code as early as possible [16]. Michael et al. [15] also introduced a novel Hazard Analysis and Validation Metrics Framework. This framework is able to gauge the sufficiency of software safety requirements in the early software development process [15]. These frameworks illustrate the need of advanced methodologies to support safety-critical software development. However, these frameworks do not consider a validation of different algorithm implementations on the affects of component reliability.

Software algorithm validation is widely used to compare different implementations with respect to power consumption or run-time. Rashid et al. [17] have compared different sorting algorithms that are implemented in different programming languages on mobile devices. Their results clearly show that different implementations results in different power consumptions. Another example is the analysis of energy consumption of sorting algorithms on smartphones of Verma et al. [18]. Verma et al. have found out that the energy consumption depends on the data size as well as on the implemented sorting algorithm [18]. Bunse et al. have explored the energy consumption of data sorting algorithms in embedded environments and in their work different algorithms resulted in different power consumption. According to the automotive functional safety standard "ISO 26262" [19] power consumption is related to component reliability.

C. Hardware Design for Functional Safety

The validation of algorithms is an important method for achieving certain requirements such as area, power dissipation or run time. Therefore, there are numerous articles about enhancing efficiency of fault-tolerant mechanisms through algorithm substitution [20] [21] [22]. Rossi et al. analyze the power consumption of fault-tolerant buses by comparing different Hamming code implementations with their novel Dual Rail coding scheme [20]. Also, Nayak et al. emphasize the low power dissipation of their novel Hamming code components [21]. Another example is the work of Shao et al. about power dissipation comparison between the novel adaptive pre-processing approach for convolution codes of Viterbi decoders with conventional decoders [22]. Khezripour et al. provide another example for validating different fault-tolerant multi processor architectures by power dissipation [23]. Unfortunately, power dissipation is just one factor for reliability of safety-critical components and insufficient for safety validation.

The most important indicator for safety at hardware level is the component reliability, which is measured in failure in time (FIT) rates [19]. Component reliability is the main indicator for safe hardware components and describes the quantity of failures in a specific time interval, mostly one billion hours [19]. These values can be calculated by specific standards for electronic component reliability such as the IEC TR 62380 [24] or statistically collected by field tests. Oftentimes, these field test have already been conducted by the manufacturers and are compiled in specific data-sheets for component reliability [25]. For each component, the data-sheets usually contain the specific FIT Rate for a certain temperature. To determine the FIT Rate for other temperatures, the Arrhenius equation as seen in (1) can be used.

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \quad (1)$$

where:

DF	De-rating Factor
E_a	Activation Energy in eV
k	Boltzmann Constant (8.167303 x 10^{-5} ev/K)
T_{use}	Use Junction Temperature in K
T_{stress}	Stress Junction Temperature in K

The Arrhenius Equation requires the Junction Temperature instead of Temperature values. The Junction Temperature represents the highest operation temperature of the semiconductor and considers the Ambient Temperature, Thermal Resistance of the package as well as the Power Dissipation as seen in (2).

$$T_j = T_{amb} + P_{dis} \cdot \theta_{ja} \quad (2)$$

where:

T_{amb}	Ambient Temperature
P_{dis}	Power Dissipation
θ_{ja}	Package Thermal Resistance Value

III. Problem Statement

The validation of different algorithms is crucial for designers to optimize their systems in terms of component reliability for highly robust and safe autonomous vehicles. Designers of safety-critical embedded systems should be able to pick the most safe algorithm with the advantage of lower FIT Rates. Especially for automotive Tier-1 companies lower FIT Rates imply higher component reliability, which is crucial for the economic success or failure of the whole system as profit margins are that small that every defect matters. Therefore, to support designers of safety-critical embedded systems, this publication's contributions to existing research are:

1) Developing novel methods for safety validation of hardware and software algorithms that is based on the approved ISO 26262 2nd Edition methods.
2) Applying the novel methods to quantify the differences between different algorithm implementations from a safety point of view.

IV. Component Reliability Focused HW/SW Co-Design Methodology

This section introduces two novel design processes that support designers of safety-critical embedded systems to find the most reliable solution during the HW/SW Co-Design

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

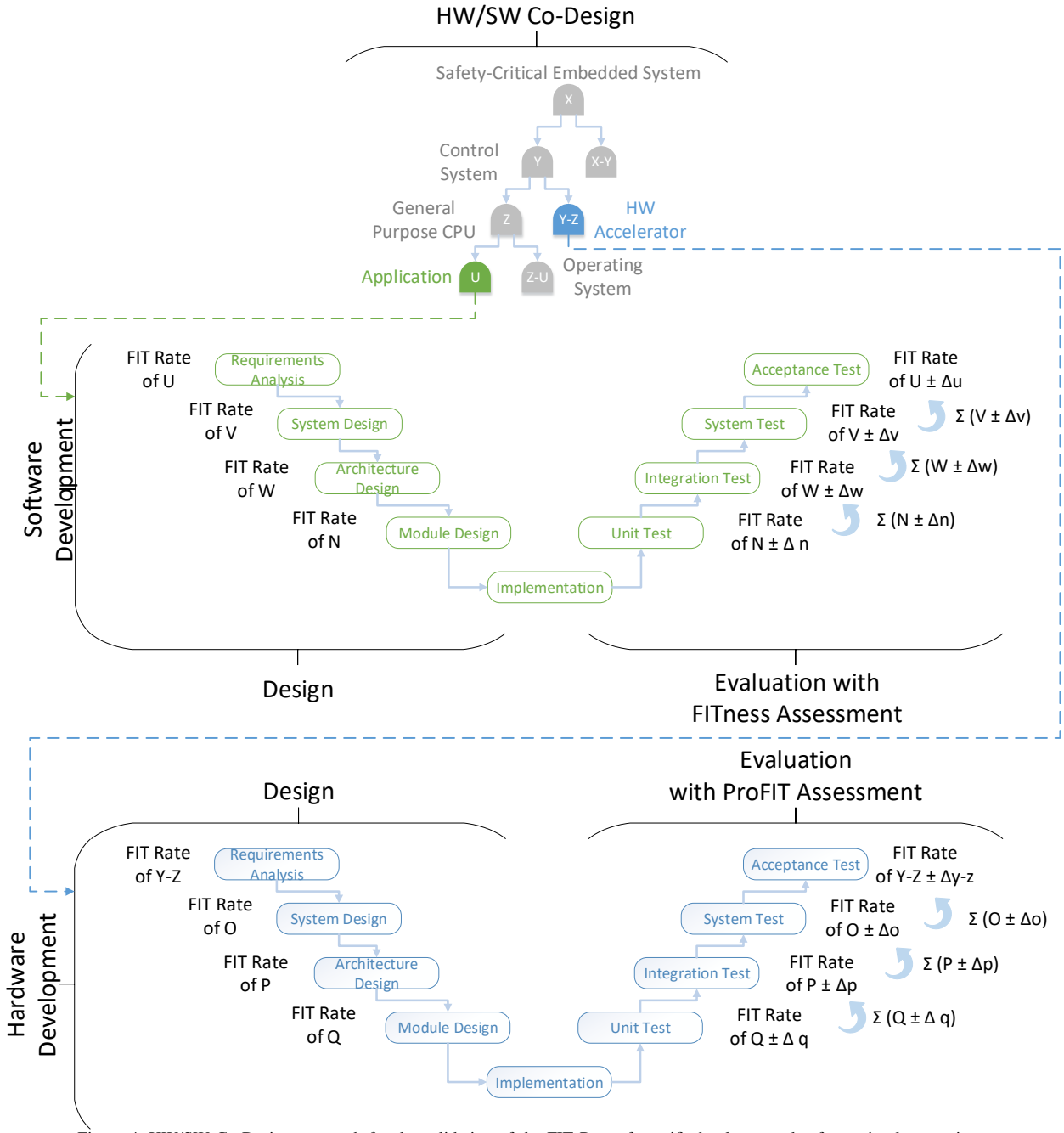

Figure 4. HW/SW Co-Design approach for the validation of the FIT Rate of specific hardware and software implementations.

process. The most reliable solution in this case is defined as the system with the lowest FIT Rate. To compare different hardware and software solutions it is necessary to measure the specific FIT Rate of each algorithm implementation. For this purpose, we need to introduce two novel measurement methodologies that enable the FIT Rate measurement. These two measurement methodologies that are presented in this publication are:

- **FITness Assessment - Hardware Reliability Evaluation** The "FITness Assessment" approach enables the FIT Rate determination of algorithms that are implemented in hardware description languages such as VHDL.
- **ProFIT Assessment - Software Reliability Evaluation** The "ProFIT Assessment" approach evaluates the FIT Rate of software implemented algorithms that are executed on micro-controller.

The FITness Assessment focuses on the estimation and validation of hardware related implementations and the ProFIT Assessment on software implementations. Both methods can easily be integrated in common HW/SW Co-Design design flows as depicted in Figure 4.

The novel HW/SW Co-Design approach that is enabled

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

through our two novel FIT Rate measurement approaches allows the evaluation of the FIT Rate of specific functionalities that are implemented in hardware or software. On the left side, a tree diagram of the overall safety-critical embedded system can be seen. The top leaf of the tree structure represents the whole embedded system and contains a FIT Rate of X. In the next hierarchical level the FIT Rate X is separated in the control system part and the additional hardware part that are represented with a FIT Rate of Y and X-Y. This strategy can be continued until we reach the smallest part of the overall system such as algorithms in software or hardware components. Based on this FIT Rate separation each designer and programmer is able to mind the overall FIT Rate of the system by complying with the given FIT Rate. Any deviance of a software algorithm can easily be recognized in the early phase of development and enables an intervention of the project team.

After the separation, each software programmer and hardware designer is able to determine if their solution matches the requirements of the designer considering the FIT Rate. Especially, the division of the overall FIT Rate into smaller sub-parts enables a reliability focused hardware-software development. A comparison between the designed reliability and the indeed reliability is possible through the summarization of the individual FIT Rates to the overall system. For this purpose, the individual FIT Rates of the software and hardware units are summed up to an overall system FIT Rate.

To enable this novel HW/SW Co-Design approach it is necessary to measure the FIT Rate of specific hardware and software implementations and this could be achieved by our novel hardware and software reliability evaluations called "FITness Assessment" and "ProFIT Assessment".

A. FITness Assessment - Hardware Reliability Evaluation

To validate different algorithms that are implemented in hardware description languages such as VHDL or Verilog, it is necessary to quantify the essential values. Based on the functional safety standard ISO 26262 2nd Edition's approved methods, the FIT Rate is the most important factor for safety-critical hardware components. As stated in the Related Work Section II, the De-rating Factor influences the FIT Rate and is expressed in the Arrhenius equation (1). Combined with the Temperature Junction equation it is obvious that the power dissipation is the most significant quantity that can be influenced by designers of digital circuits (see (3)).

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{amb} + P_{dis} \cdot \theta_{ja}})} \quad (3)$$

Consequently, by decreasing Power Dissipation the designer increases component reliability. For Field Programmable Gate Array (FPGA), the power dissipation primarily depends on static and dynamic power consumption. Based on these physical principles, our novel method FITness Assessment for algorithm safety validation on FPGAs is segmented in the following parts, as seen in Figure 5:

1) **Algorithm Implementation**
To guarantee similar conditions for different algorithms, it is necessary to implement a generic framework that allows implementing algorithms without major changes.

2) **Power Consumption Measurement**
For each algorithm, a particular measurement is recorded. It is advisable to record the generic framework without any algorithm to be able to determine the algorithms' power consumption by subtraction.

3) **Determination of Base FIT Rate**
The Base FIT Rate may be calculated by using the IEC TR 62380 [24] standard or analyzed statistically by field tests. Oftentimes, these field test have already been conducted by the manufacturers and are compiled in specific data-sheets for component reliability.

4) **De-rating Factor Calculation**
The De-rating Factor can be calculated with the Arrhenius equation and the related Thermal Junction equation as seen in (1) and (2).

5) **Identification of Effective FIT Rate**
The Effective FIT Rate reflects the Base FIT Rate for a specific temperature and can be calculated with:

$$FIT_{ef} = FIT_{base} \cdot DF \quad (4)$$

where:

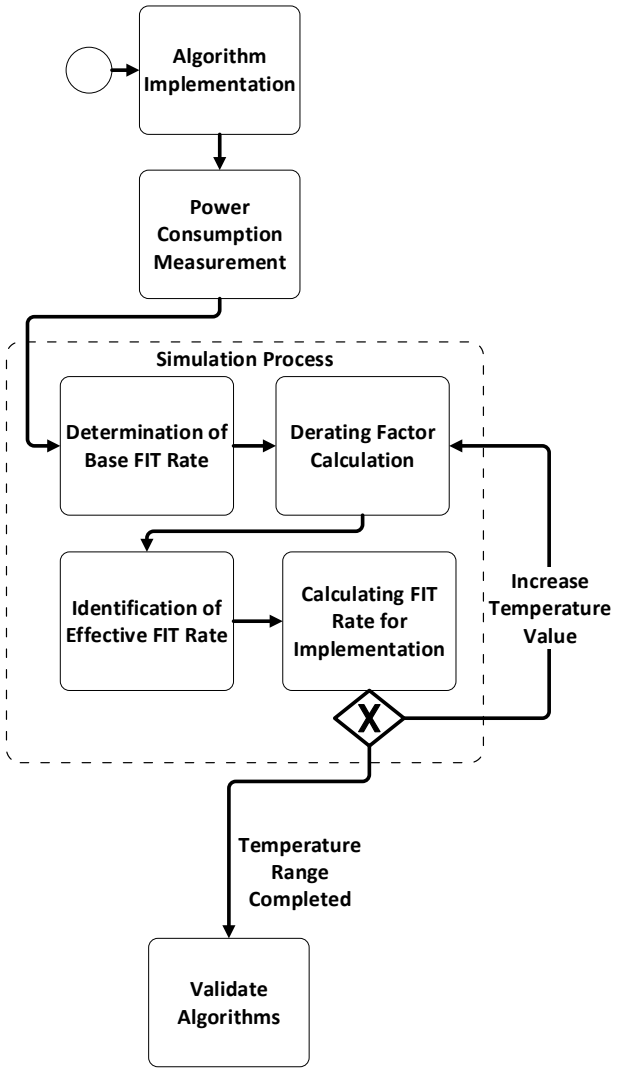

Figure 5. Workflow overview of our novel method FITness Assessment for algorithm validation from a safety point of view in Business Process Model and Notation.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

FIT_{base} Base FIT Rate from FPGA Reliability Data-sheet
DF De-rating Factor as seen in (1)

6) **Calculating FIT Rate of the Implementation**
The Effective FIT Rate as seen in (4) represents the component reliability for the whole FPGA. However, an FPGA is made up of many different logic elements. Consequently, the Effective FIT Rate can be broken down into the amount used by each logical element as seen in (5).

$$FIT_{imp} = \frac{FIT_{ef}}{N_{le}} \quad (5)$$

where:

FIT_{ef} Effective FIT Rate as seen in (4)
N_{le} Total Number of Logic Elements of the specific FPGA taken out from Data-sheet

7) **Validate Algorithms**
The resulting FIT Rate of the implementation represents the FIT Rate of the specific algorithm and can be used for validation. It is advisable to measure each algorithm once at room temperature conditions and simulate the rest of the temperature range by starting with the De-rating Factor Calculation.

B. ProFIT Assessment - Software Reliability Evaluation

Validating software algorithms for safety-critical systems from a safety point of view can be obtained by using our novel "ProFIT Assessment". This method enables the impact measurement of different software algorithm implementation on component reliability. Our novel method is using approved methods from the functional safety standard ISO 26262 2nd Edition [19] of the automotive industry. As a starting base we have used equation (3). This equation represents the impacts on the component FIT Rate as a function of the power consumption. In Related Work we have introduced scientific results that clearly shows that different software algorithm implementations results in different power consumption. Therefore, the De-rating Factor can be used to determine the specific software algorithm FIT Rate. Our "ProFIT Assessment" is using these relations and can be separated into five parts:

1) **Implementation**
Different algorithms will be implemented in software. For better results and accuracy it is advisable to implement a general framework where the algorithms can be exchanged without any major changes. The framework will be compiled and programmed onto a specific micro-controller. In general any micro-controller can be used but it is advisable to look for public available component reliability data-sheets.

2) **Measurement**
In this step the software algorithms will be run on micro-controller and the power dissipation is recorded. This step will be repeated for each implementation. As an output result a measurement report is created, which contains the measurement setup, the used micro-controller, software algorithm implementation, power consumption and ambient testing temperature. These details are necessary for further analysis.

3) **Calculating FIT**
The idea behind this step is that each software algorithm needs a specific amount of time and the power consumption is measured at a specific sampling rate. For each sample we are calculating the specific Base FIT Rate and relates it to the sampling duration. Summing up all the individual FIT Rates of each time-slice results in the specific FIT Rate of the software algorithm implementation for a specific temperature. The impacts of the different implementations over the whole temperature range will be determined through the simulation process afterwards.

a) **Junction Temperature**
At first we are calculating the specific Junction Temperature for the ambient testing temperature as seen in (2).

b) **De-rating Factor**
Secondly the specific De-rating Factor is determined with the Arrhenius equation as seen in (1).

c) **Base FIT Rate**
The base FIT Rate can be determined by multiplying the base FIT Rate from compo-

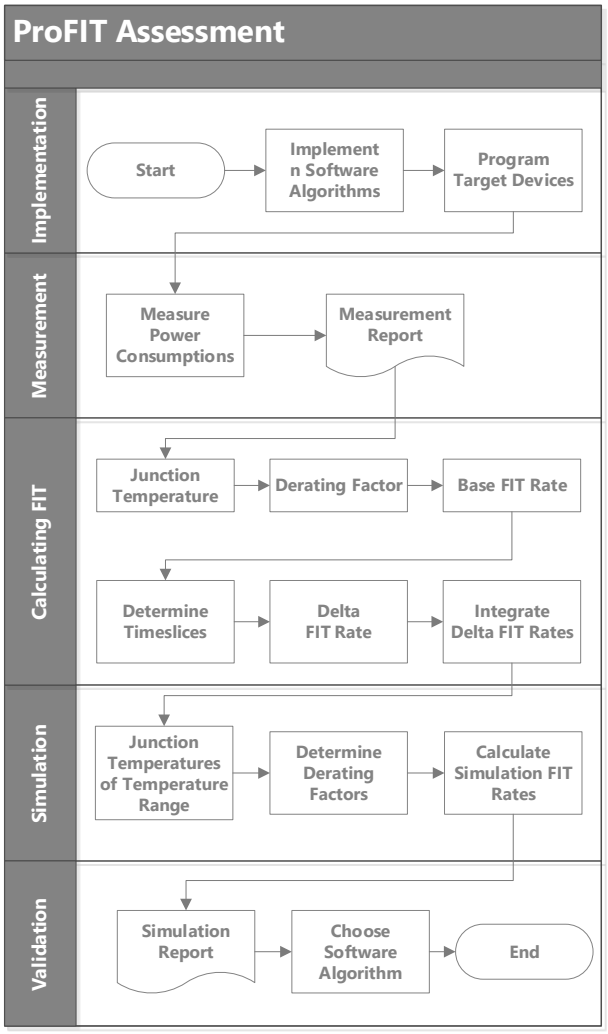

Figure 6. Work flow overview of our novel "ProFIT Assessment" method for software algorithm validation from a safety point of view.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

nent reliability data-sheet with the De-rating Factor.

$$FIT_{Base} = DF \cdot FIT_{Ds} \quad (6)$$

where:

DF De-rating Factor as seen in (1)
FIT_{Ds} Base FIT Rate of Component Reliability Data-sheet

d) **Determine Time-slices**
In this step the Base FIT Rate will be adapted to the specific run-time.

$$FIT_{Timeslice} = FIT_{Base} \cdot \frac{T_{Sampling}}{T_{Runtime}} \quad (7)$$

where:

FIT_{Base} Base FIT Rate as seen in (6)
$T_{Sampling}$ Measurement Sampling Time
$T_{Run\text{-}time}$ Run-time of the Measurement

e) **Integrate Delta FIT Rates**
To determine the Software FIT Rate it is necessary to accumulate all individual Time-slices.

$$FIT_{Algorithm} = \sum_{1}^{n} FIT_{Ts} \quad (8)$$

$$n = \frac{T_{Runtime}}{T_{SamplingRate}} \quad (9)$$

where:

FIT_{Ts} Time-slice FIT Rate as seen in (7)
$T_{Sampling}$ Measurement Sampling Time
$T_{Run\text{-}time}$ Run-time of the Measurement

4) **Simulation**
The simulation step is necessary to determine the software algorithm FIT Ratio over the whole operational temperature range. The power consumption variation will be neglected because it affects all algorithm implementations equally.
   a) **Junction Temperatures of Temperature Range**
   This step is similar as during the Calculating FIT Rate step except the use of the whole operational temperature range.
   b) **Determine De-rating Factors** This step is equal as seen in (1).
   c) **Calculate Simulation FIT Rates**
   This step is equal as seen in (6).

5) **Validation**
After the simulation there will be a Simulation Report with the specific FIT Rates for the whole operational temperature range. This can be used as a decision support to pick the most reliable software algorithm implementation.

V. Test Setup

This section describes the practical results of this publication by introducing the testing environment and the final results of the experiments. The validation of the HW/SW Co-design approach was divided in a software and hardware part and both parts have been validated independently.

A. FITness Assessment Evaluation Setup

In our research question, we analyze the differences between Single Error Correction - Double Error Detection (SEC-DED) and Double Error Correction (DEC). For this purpose, we chose the Hamming code for SEC-DED as this code is recommended in the new ISO 26262 2nd Edition and the BCH-code for DEC, especially because other ECC algorithms are often based on this concept and both algorithms fulfill the following requirements:

- 32 Bit data size
- Combinatorical Logic
- Including Fault Injection Module
- SEC-DED or DEC Functionality

The generic algorithm framework contains a test-bench with an automatic up-counter as well as a validator (see Figure 8). Both algorithms can be exchanged in the framework without any major changes. This enables a precise validation from a safety point of view.

In our test setup, we use the MAX1000 - IoT Maker Board by Trenz Electronic. This device is a small maker board for prototyping with sparse additional components. The main controller is the MAX10 10M08SAU169C8G, an FPGA device by Intel. For our research, the main advantages of using this board are:

- Small amount of additional hardware components
- Availability of Reliability Data-sheet

This board also contains an FTDI chip that draws about 50 mA on average, which we will subtract out for our analysis. The power consumption measurement is performed by the Mobile Device Power Monitor of Monsoon Solutions. The big advantage of this power monitor is the direct measurement of USB devices. The entire measurement setup is shown in Figures 7 and 9 and contains the following software and hardware parts:

- Quartus Prime 18.0 (Intel)
- Power Tool 5.0.0.23 (Monsoon Solutions)
- Mobile Device Power Monitor (Monsoon Solutions)
- MAX1000 - IoT Maker Board (Trenz Electronic)

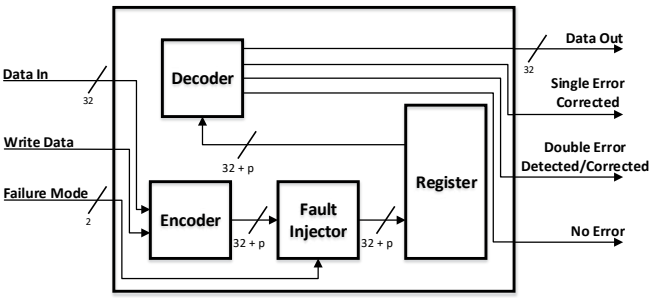

Figure 7. Pin configuration of both algorithms including an overview of functional blocks inside.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

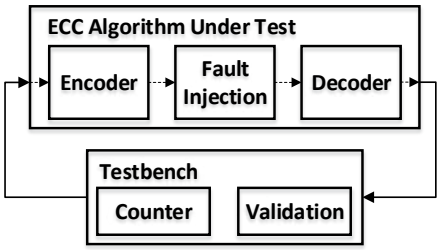

Figure 8. General framework for ECC algorithm validation including test-bench and ECC algorithm.

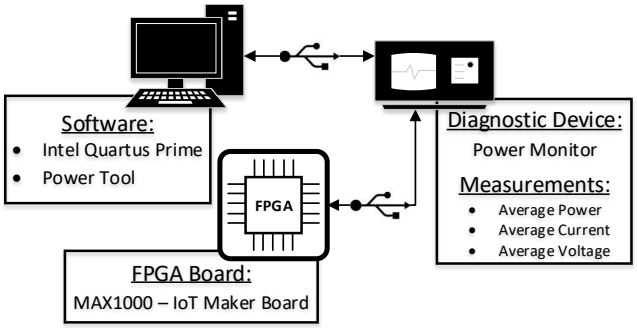

Figure 9. Overview of the entire measurement setup including software and hardware components.

B. ProFIT Assessment Evaluation Setup

For testing purpose we have chosen sorting algorithms as test candidates. The reasons for us are:

- Very often used
- Easy to understand
- Many different algorithms available
- Comparable results of power consumption available as seen in Section II-B

The sorting algorithms we chose are widely used and known and are known as:

- Binary Insertion Sort
- Heapsort
- Insertion Sort
- Mergesort
- Quicksort
- Shell Sort

All sorting algorithms were implemented in C programming language and programmed onto a micro-controller. For the micro-controller we have chosen the “MSP430 FR5969” from Texas Instruments by the following reasons:

- Measure Power Consumption with EnergyTrace++ Technology in “Code Composer Studio”
- Qualified for automotive usage
- Low-Power Device
- FIT Rates publicly available

As a operational temperature range for the simulation part we have chosen $-40°C$ up to $140°C$. This range is higher than the recommended operating conditions from the data-sheet but for our tests it is not relevant.
Test Setup Summary:

- Code Composer Studio 8.1
- MSP430 FR5969
- 6 different Sorting Algorithms
- 400 Numbers to Sort
- $-40°C$ up to $140°C$ Temperature Range for Simulation

VI. Results

A. FITness Assessment Evaluation

This section summarizes our results of the comparison of SEC-DED and DEC ECC algorithm. The validation was performed with our novel FITness Assessment method for algorithm validation from a safety point of view as described in Section IV.

The first algorithm we implemented was the Hamming code, which is a SEC-DED ECC algorithm. The implementation reserves 45 logic elements of the used FPGA and the whole board has an average power dissipation of 571.78 mW. With the second BCH-code DEC ECC algorithm, the board consumes an average of 599.05 mW and assigns 65 logic elements. The first result shows a difference between both algorithms in logic elements as well as in power dissipation resulting in a varying FIT Rate. The next step is the simulation process over the whole temperature range. We selected a temperature range between -40°C and 125°C and the values of Table I were used for the simulation process. In our simulation we neglected the alteration of power dissipation through temperature because it would affect both ECC implementations evenly.

Figure 10 points out that both algorithms vary in their FIT Rate and rise exponentially with increasing temperature. The FIT Rate may be neglected for temperatures up to 40 °C.

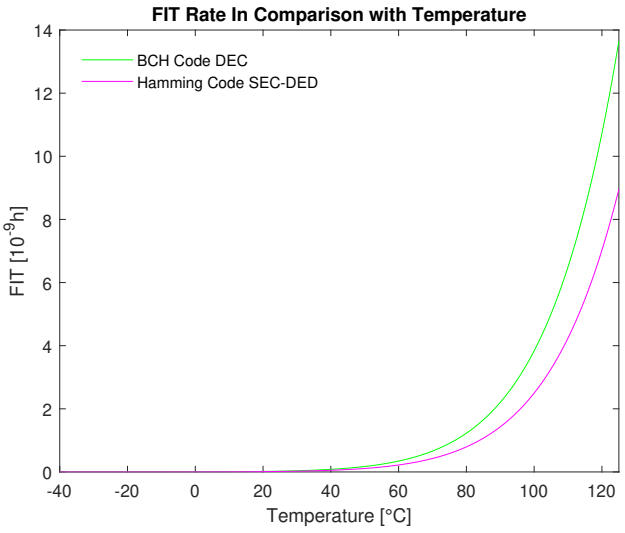

Figure 10. Simulation results of the resulted FIT Rates between -40°C and 125°C for both ECC implementations.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

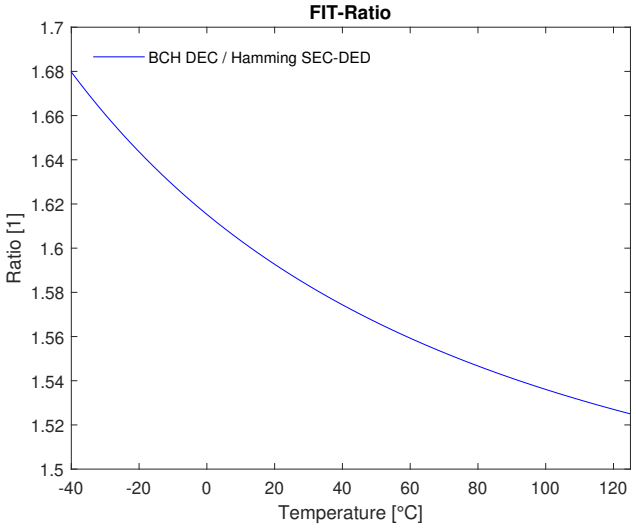

Figure 11. Overview of the FIT Rate overhead between SEC-DED and DEC ECC algorithm.

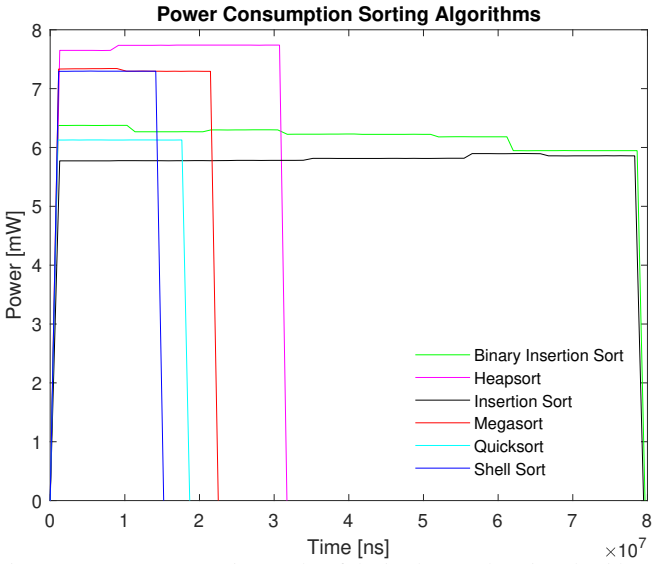

Figure 12. Power consumption results of the implemented sorting algorithms at 25°C ambient temperature.

TABLE I. RESULTS OF THE RESERVED LOGIC ELEMENTS AND AVERAGE TOTAL POWER DISSIPATION OF BOTH ECC IMPLEMENTATIONS.

	Hamming Code	BCH-Code
Used Logic Elements	45	65
Total Average Power Dissipation	571.78 mW	599.05 mW

The Hamming code with SEC-DED shows a better FIT Rate indicating more reliability of the hardware components which results in a higher safety level. The reason for this difference is the greater number of logic elements used for the DEC ECC algorithm and the resulting increase of power dissipation. The higher power dissipation results in a higher Thermal Junction temperature as seen in (2), which leads to a higher FIT Rate.

Both algorithms were implemented without any safety measures. This means that any damage to the Logic Element of the FPGA leads to failure of the whole ECC algorithm and the safe memory block. The ECC algorithm is the measure against SEU related altered flip flops inside the memory block, which decreases the specific FIT Rate of the memory block. The results of Figure 10 do not represent the FIT Rates of the memory block but the FIT Rate of the pure ECC implementation. It is important to understand that the ability of more bit error correction is not considered for the algorithm validation because it only positively influences the FIT Rate of the memory block.

Moreover, it is important to understand that the absolute values of the FIT Rate always correlate to a specific FPGA. Consequently, it is advantageous to look at the ratio between the algorithms because this gives a better overview of the overhead. The SEC-DED/DEC ECC FIT Ratio is depicted in Figure 11. The FIT Ratio overhead of the DEC ECC algorithm is slighly decreasing with increasing temperature, which is negligible in practice.

We recommend using the Hamming code algorithm for SEC-DED error correction for 32 bit memory size registers in automotive LiDAR systems. The SEC-DED algorithm used in our experiment resulted in a FIT Rate that was at least 52% lower than the DEC ECC algorithm.

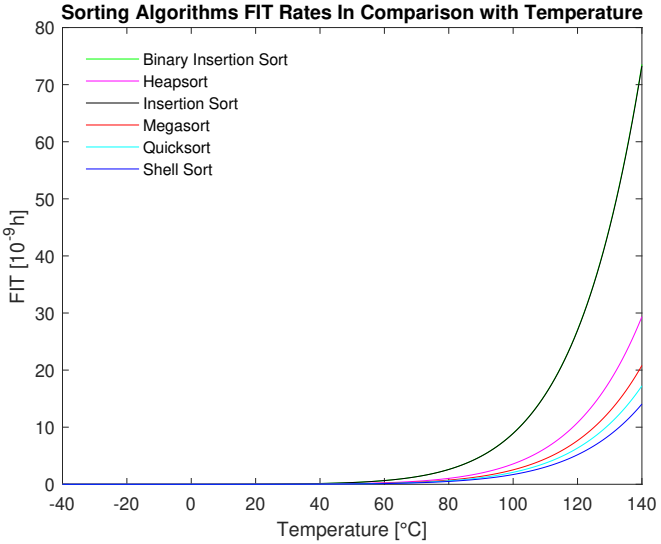

Figure 13. Simulation results of the sorting algorithms between −40°C and 140°C.

B. ProFIT Assessment Evaluation

In this section we are presenting our results of applying our novel "ProFIT Assessment" on sorting algorithms. This method enables the possibility to validate software algorithms from a safety point of view. It is important to understand that we are not comparing sorting algorithms instead we are applying our method on the sorting algorithms.

All algorithms are implemented in C and were tested on the "MSP430 FR5969" micro-controller board. This board has the possibility to measure the power consumption of each algorithm directly in the "Code Composer Studio". Table II gives an overview about our power measurement results of the implemented sorting algorithms. These algorithms were implemented in C and were executed on the "MSP430 FR5969" micro-controller board. The "Shell Sort" algorithm was in our test case the fastest at run-time and needed the least energy during run-time. Figure 12 shows the results of our power consumption measurements. In our setup "Shell Sort"

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

TABLE II. **Overview of the Power Consumption measurements of all C implemented sorting algorithms at 25°C ambient temperature.**

	Average Power in mA	Energy in uJ	Time in ms
Binary Insertion Sort	6.18	438.2	77.53
Heapsort	7.72	178.4	31.71
Insertion Sort	5.82	440.0	79.48
Mergesort	7.31	124.8	22.52
Quicksort	6.12	60.7	18.69
Shell Sort	7.30	58.5	15.20

TABLE III. **Results of the algorithm FIT Rates calculation of the implemented sorting algorithms on the MSP430 FR5969 micro-controller board.**

	FIT Rate in 10^{-9}
Binary Insertion Sort	1.87204922
Heapsort	0.747313371
Insertion Sort	1.865387949
Mergesort	0.529712728
Quicksort	0.438742916
Shell Sort	0.357627573

had the best run-time performance and "Binary Insertion Sort" had the worst run-time. This result clearly shows that different algorithm implementations result in different power consumptions. With these results the specific algorithm FIT Rates can be determined with the equations that have been introduced in IV-B.

The provided Table III represents the FIT Rate for a specific ambient temperature. In our case we have calculated the FIT Rate for the test ambient temperature of 25°C. For other temperatures a simulation over the whole temperature range is necessary. For this purpose we have used the Arrhenius equation as seen in (1). In Figure 13 the FIT Rates of the implemented algorithms is displayed with the behavior over the whole temperature range. It can be seen that "Shell Sort" has the best FIT Rate over the whole temperature range and "Binary Insertion Sort" is the worst. For temperatures up to 50°C it does not matter what kind of algorithm is used but afterwards it has an affect on the component reliability and therefore on the overall safety level.

VII. Conclusion

In this publication, we introduced a novel HW/SW Co-Design approach that is optimizing the reliability of safety-critical automotive systems. To enable this approach, we have introduced two novel reliability evaluation methodologies that are able to analyze the impacts of different hardware and software algorithms on the component reliability also called Failure-In-Time Rate.

The hardware related part of the publication introduced the FITness Assessment, a novel component reliability hardware evaluation methodology and this was used to evaluate two different error correction code algorithms (SEC-DED and DEC ECC) from a safety perspective. The software related part introduced the ProFIT Assessment, a novel component reliability software evaluation methodology and this was used to analyze the impacts of six different sorting algorithms (Binary Insertion Sort, Heapsort, Insertion Sort, Mergesort, Quicksort and Shell Sort) to the overall component reliability of the micro-controller part of the overall embedded system.

Both methods are based on approved methods of the novel automotive functional safety standard ISO 26262 2nd Edition. The result clearly shows that different hardware and software algorithms lead to different FIT Rates.

FITness Assessment allowed the measurement of each algorithm's specific FIT Rate, facilitating the selection of the most reliable ECC algorithm. Our case shows a DEC-ECC algorithm that has a higher FIT Rate than the SEC-DED ECC algorithm.

ProFIT Assessment focuses on evaluating component reliability of software algorithms on micro-controllers. In our results we have showed that safety validation of software algorithms is possible and that different algorithm implementations can result in different component reliability. These differences should not be neglected because they have an impact from a safety point of view.

The FIT Rate reflects component reliability, which is an important hardware indicator for safety. These differences should not be neglected from a safety as well as from a business point of view. The FIT Rate also statistically indicates the amount of defective components, which is an economically important indicator as lower FIT rates also result in less defect components.

Fault-tolerance, safety and reliability will become more and more important in the next years because of autonomous driving. The novel introduced FITness Assessment enables the validation of different hardware algorithms to be able to select the most reliable one, which helps improve the overall safety level of the automotive vehicle by increasing component reliability. "ProFIT Assessment", the second method we introduced in this publication enables the possibility to validate the FIT Rate of software algorithm implementations and enables the possibility to choose the most reliable one. Both methodologies can be used for HW/SW Co-design for optimizing safety-critical automotive embedded systems from a safety point of view.

VIII. Acknowledgments

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

References

[1] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "FITness Assessment-Hardware Algorithm Safety Validation," in The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications, PESARO 2019, pp. 12–17.

[2] "50 Jahre fahrerloses Fahren: Pressematerial," 2014, URL: https://publicarea.admiralcloud.com/p/a49d3d8ba92f3cdbfa864f [accessed: 2019-11-11].

[3] M. Dikmen and C. Burns, "Trust in autonomous vehicles: The case of Tesla Autopilot and Summon," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Oct 2017, pp. 1093–1098.

[4] R. Faria, L. Brito, K. Baras, and J. Silva, "Smart mobility: A survey," in 2017 International Conference on Internet of Things for the Global Community (IoTGC), July 2017, pp. 1–8.

[5] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "PRYSTINE - PRogrammable sYSTems for INtelligence in AutomobilEs," in 2018 21st Euromicro Conference on Digital System Design (DSD), Aug 2018, pp. 618–626.

International Journal on Advances in Systems and Measurements, vol 12 no 3 & 4, year 2019, http://www.iariajournals.org/systems_and_measurements/

[6] S. Ha and J. Teich, Handbook of hardware/software codesign. Springer Publishing Company, Incorporated, 2017, ISBN: 978-94-017-7268-6.

[7] P. R. Schaumont, A practical introduction to hardware/software codesign. Springer Science & Business Media, 2012, ISBN: 978-1-4614-3736-9.

[8] F. Vargas, E. Bezerra, L. Wulff, and D. Barros, "Optimizing HW/SW codesign towards reliability for critical-application systems," in Proceedings Seventh Asian Test Symposium (ATS'98)(Cat. No. 98TB100259). IEEE, 1998, pp. 52–57.

[9] S. Tosun, N. Mansouri, E. Arvas, M. Kandemir, Y. Xie, and W.-L. Hung, "Reliability-centric hardware/software co-design," in Sixth international symposium on quality electronic design (isqed'05). IEEE, 2005, pp. 375–380.

[10] N. G. Leveson and J. Diaz-Herrera, Safeware: system safety and computers. Addison-Wesley Reading, 1995, vol. 680, ISBN: 978-0201119725.

[11] K. J. Cruickshank, J. B. Michael, and M. Shing, "A Validation Metrics Framework for safety-critical software-intensive Systems," in 2009 IEEE International Conference on System of Systems Engineering (SoSE), May 2009, pp. 1–8.

[12] W. Ahmad, U. Qamar, and S. Hassan, "Analyzing different validation and verification techniques for safety critical software systems," in 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS), Sept 2015, pp. 367–370.

[13] N. G. Leveson and P. R. Harvey, "Analyzing Software Safety," IEEE Transactions on Software Engineering, vol. SE-9, no. 5, Sept 1983, pp. 569–579.

[14] E. M. E. Koursi and G. Mariano, "Assessment and certification of safety critical software," in Proceedings of the 5th Biannual World Automation Congress, vol. 14, June 2002, pp. 51–57.

[15] J. B. Michael, M. Shing, K. J. Cruickshank, and P. J. Redmond, "Hazard Analysis and Validation Metrics Framework for System of Systems Software Safety," IEEE Systems Journal, vol. 4, no. 2, June 2010, pp. 186–197.

[16] P. Baudin, A. Pacalet, J. Raguideau, D. Schoen, and N. Williams, "Caveat: a tool for software validation," in Proceedings International Conference on Dependable Systems and Networks, June 2002, p. 537.

[17] M. Rashid, L. Ardito, and M. Torchiano, "Energy Consumption Analysis of Algorithms Implementations," in 2015 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Oct 2015, pp. 1–4.

[18] M. Verma and K. Chowdhary, "Analysis of Energy Consumption of Sorting Algorithms on Smartphones," in Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018, pp. 26–27.

[19] I. n. E. ISO, "Draft 26262 2nd Edition: Road vehicles-Functional safety," International Standard ISO/FDIS, vol. 26262, 2018.

[20] D. Rossi, A. K. Nieuwland, S. V. E. S. van Dijk, R. P. Kleihorst, and C. Metra, "Power Consumption of Fault Tolerant Busses," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 5, May 2008, pp. 542–553.

[21] V. S. P. Nayak, C. Madhulika, and U. Pravali, "Design of low power hamming code encoding, decoding and correcting circuits using reversible logic," in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), May 2017, pp. 778–781.

[22] W. Shao and L. Brackenbury, "Pre-processing of convolutional codes for reducing decoding power consumption," in 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, March 2008, pp. 2957–2960.

[23] H. Khezripour and S. Pourmozaffari, "Fault Tolerance and Power Consumption Analysis on Chip-Multi Processors Architectures," in 2012 Seventh International Conference on Availability, Reliability and Security, Aug 2012, pp. 301–306.

[24] T. IEC, "Iec 62380," Reliability data handbook–universal model for reliability prediction of electronics components, PCBs and equipment (emerged from UTEC 80-810 or RDF 2000), 2004.

[25] "Intel Reliability Report," 2018, URL: https://www.intel.com/content/www/us/en/programmable/support/quality-and-reliability/reports-tools/reliability-report/rel-report.html [accessed: 2019-11-11].

Enabling Live State-of-Health Monitoring for a Safety-Critical Automotive LiDAR System

Andreas Strasser†, Philipp Stelzer†, Christian Steger† and Norbert Druml*
†Graz University of Technology, Graz, Austria
email:{strasser, stelzer, steger}@tugraz.at
*Infineon Technologies Austria AG, Graz, Austria
email:{norbert.druml}@infineon.com

***Abstract*—In the next few years, modern vehicles will integrate the next level of Advanced Driver-Assistance Systems (ADAS) such as Light Detection and Ranging (LiDAR) which will be one of the key enabler for autonomous driving. Autonomous driving will be in charge for controlling the vehicle without any inputs of a passenger. This requires highly robust and reliable components and systems. In general, mechanical defects are detectable through vibrations or noise changes but for semiconductor components these capabilities are not available. Semiconductor components fail silently and abrupt without any prior information and this could lead to fatal accidents when systems fail during autonomous driving phases. In this publication, we are introducing a novel state-of-health monitoring system for automotive LiDAR system that is capable to economically record the component history and automatically processes these data to the statistical Failure-In-Time (FIT) Rate that is primarily used in the Automotive domain such as in the "ISO 26262 - Road Vehicle Safety" standard.**

***Index Terms*—FIT Monitor, Reliability Monitor, Aging Monitor, LiDAR, Safety**

I. Introduction

In the next decades, Smart Mobility will become more and more important for urban environments to manage environmental pollution, scarcity of raw materials and traffic congestion [1]. The amount of citizens that are using individual road vehicles to travel to work are steadily increasing and this causes extra costs for the individual as well as to the community. For this purpose, Smart Mobility applications such as car sharing or street light control are attempting to optimize the energy and ressource usage as well as to reduce costs with the benefit of increasing the quality of life [2]. The next big hope in the area of Smart Mobility are autonomous vehicles. Autonomous vehicles have the capability of controlling the vehicle independently without any intervention of a human person. This would enable citizens to call vehicles from car sharing companies that are autonomously driving to the pick-up address of the customer and drive them safely and comfortable to the destination address anytime and anywhere [3]. For enabling autonomous driving, next generation vehicles needs to be equipped with additional environmental perception sensors such as Radar, Light Detection and Ranging (LiDAR) and Vision Cameras to percept the proximity. One possible solution of such an perception system is PRYSTINE's concept of a fail-operational urban surround perception system (FUSION) as depicted in Figure 1. The FUSION system combines the data of the individual Radar, LiDAR and Vision Cameras with sensor fusion and enables a safe and robust perception of other road participants [1]. Nowadays, there is no commercial middle-class car available that is equipped with a LiDAR system yet. One possible reason could be that traditional spinning mechanical LiDAR systems are quite expensive such as the Velodyne LiDAR system that still costs thousands of dollar but with optical phased array LiDAR systems the costs could be dropped to 250 US Dollar in larger volumes [5]. One possible solution of a robust low-cost automotive LiDAR system is the 1D MEMS Micro-Scanning LiDAR system as seen in Figure 2. The 1D MEMS Micro-Scanning LiDAR system from Druml et al. is a robust and safe automotive LiDAR system that will cost below 250 US Dollar and will

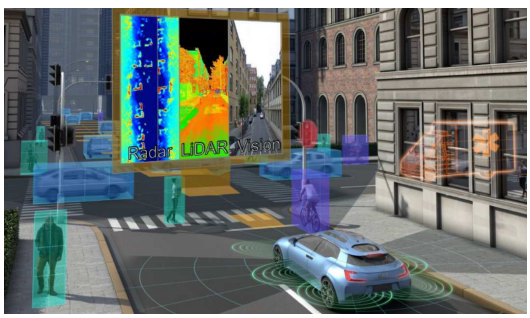

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

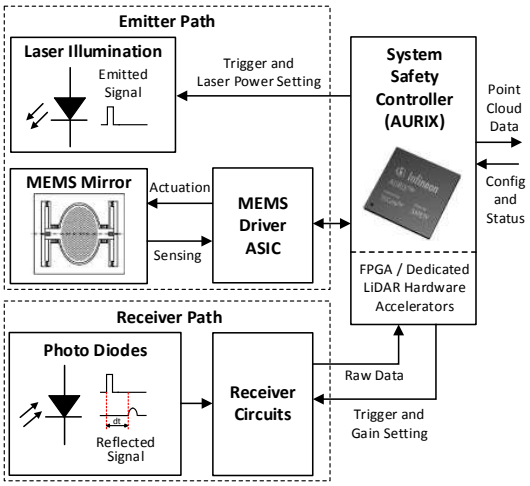

Fig. 2. Overview of a LiDAR system for automonomous driving [4].

be the key enabler for autonomous driving functionalities in middle-class cars [4]. The system focus on highly robustness and safety and will achieve the Automotive Safety Integrity Level (ASIL) C.

In general, modern safety-critical automotive embedded systems are developed with high safety standards such as the ISO 26262 - Road Vehicle Safety standard [6]. But there is a drawback that the designers needs to determine a temperature mission profile which describes the estimated usage. Any major variation has a big influence on the reliability of the component such as higher reliability for lower temperature and lower reliability for higher temperature [7]. Both cases are not desirable due to higher manufacturing costs for the producer or less operation time for the customer. In worst case, safety-critical autonomous systems fail during operation and causes an accident. To prevent accidents that are caused by abrupt failing environmental perception systems such as LiDAR it would be preferable to monitor the lifetime usage of a component and detect and signalize overstressed microelectronic devices.

To prevent accidents that are caused by overstressed LiDAR components we want to contribute on the following research question:

- How can overstressed LiDAR components be detected during run-time and monitored the whole lifecycle efficiently?

II. Related Works

Safety and robustness is one of the most important key-factors for the overall acceptance of the next generation ADAS such as the FUSION platform of the PRYSTINE project [1]. The FUSION platform is able to percept the close environment of the vehicle and based on this data decisions for autonomous driving will be made. These decisions needs to be reliable because any mistake could lead to a fatal accident considering the vehicle is driving autonomously on a highway. To prevent fatal accidents, one possibility is to add redundancy and diversity to the overall system and increase the overall reliability but from an economical point-of-view it is not that simple [6]. Redundancy and diversity is mostly connected to higher costs and this results in less cost efficiency. To focus on the cost efficiency it would be preferable to detect failures before the overall system fails.

The correct functionality of a system is specified as Mean Time Between Failures (MTBF) and is a statistical value that indicates the time the system is able to perform without any present failure. The automotive domain is using the inverse value of the MTBF and is calling these value the Failure-In-Time (FIT) Rate. Based on the Automotive Safety Integrity Level (ASIL) that is derived from the Hazard and Risk Analysis (HARA), the FIT Rate of the system will be specified [6]. In general, the overall FIT Rate of systems can be determined by statistical field tests or specific reliability standards such as the IEC 62380 [8]. The IEC 62380 [8] and ISO 26262 [6], specifies that the reliability of hardware components are temperature dependent and is expressed in the Arrhenius Equation as seen in (1).

$$DF = e^{\frac{E_a}{k} \cdot (\frac{1}{T_{use}} - \frac{1}{T_{stress}}))} \quad (1)$$

where:

DF	is Derating Factor
E_a	is Activation Energy in eV
k	is Boltzmann Constant (8.167303 x 10^{-5} ev/K)
T_{use}	is Use Junction Temperature in K
T_{stress}	is Stress Junction Temperature in K

The Derating Factor of the Arrhenius Equation is the key impact factor of the hardware component that is stressed by higher temperature and because of the exponential relation even slighty temperature increases should not be neglected. For that reason, temperature is one of the key factors for reliable hardware components and always had a special focus in the industry for safety-critical systems [6], [8].

Temperature affects the hardware components the most in terms of reliability and this is the reason why researcher added sensors to record and analyze temperature changes in safety-critical systems [9]–[13]. Vazqeuz et al. [10] describe in their publication the approach of a built-in an aging monitor. The monitor is implementing a redundant sensor that is only activated in car power-up and this enables the detection of aging. Another approach of Johannsson et al. [9] introduced a novel FPGA-based temperature monitoring system that is used to continously logging temperature during real-time operation. The logging data is used for estimaiting the remaining useful lifetime in a reliability tool. One drawback of the temperature logging implementation of Johannsson is the huge amount of data that needs to be collected during the system operation time of ten to fifteen years.

To establish an aging monitor in the automotive domain it is necessary to introduce an efficient temperature monitoring system that is able to record the temperature history of fifteen operation years efficiently. Strasser et al. [14] introduced a State-of-Health safety monitor that is optimized for systems in the automotive domain and is recording the temperature data efficiently in a histogram. Their method is considering the FIT Rate as a credit system that is consumed by the system and the specific cost of a point of time depends on the current system temperature. This enables the detection of a mismatch between the defined temperature mission profile and the real operation temperature profile as well as utilization deviations of the system caused by system updates [14].

To enable robust and efficient state-of-health safety monitoring for future ADAS we want to contribute on the following research work:

- Hardware Implementation of the memory efficient state-of-health safety monitor system of Strasser et al. [14] in an automotive LiDAR rapid prototyping platform including the design of a graphical front end to support mechanics and engineers to detect reliability issues.

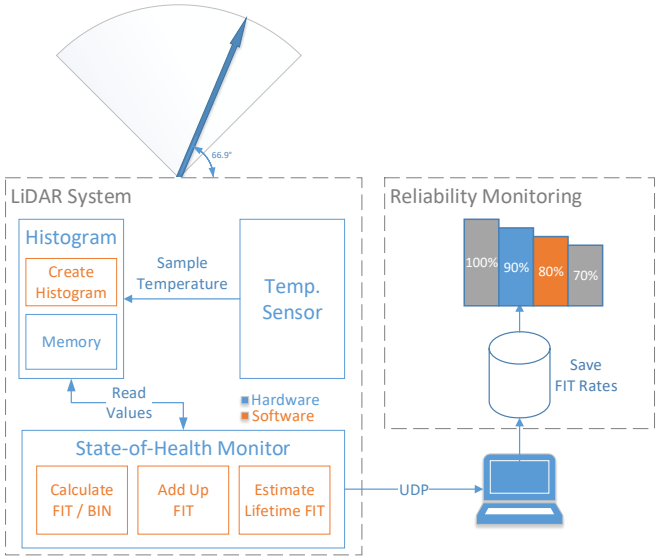

Fig. 3. Overview of the modified LiDAR system containing the state-of-health safety monitor.

III. Live State-of-Health Monitoring for Automotive LiDAR System

In the next few years, novel automotive LiDAR system, such as the 1D MEMS Micro-Scanning LiDAR system of Druml et al. [4], will become a major key-enabler for safe and robust autonomous driving. As depicted in Figure 2, the LiDAR system is composed of the Emitter and Receiver Path in which the Emitter Path is the most safety-critical because of the MEMS Driver application-specific integrated circuit (ASIC). The MEMS Driver ASIC is responsible to sense, control and to actuate the MEMS Mirror and any failure could result in an abrupt halt of the MEMS Mirror. An abrupt halt leads to an outage of the 3D point-cloud data of the LiDAR system and in worst-case could lead to an accident. For this reason, we want to prevent such an situation of an abrupt failure of the MEMS Driver ASIC by implementing a State-of-Health Safety Monitoring system that notifies the driver in case of overstress.

A. System Architecture

In Figure 3, the adapted 1D MEMS Micro-Scanning LiDAR system can be depicted. The novel system architecture contains an additional State-of-Health (SoH) Safety Monitor that was introduced as a concept by Strasser et al. [14].

The SoH Safety Monitor is sampling the value of the internal temperature sensor at a specific frequency and maps the sampled temperature value inside a histogram, as depicted in Figure 5. The histogram is mandatory to reduce the amount of memory for the temperature logging and enables the recording of long-running data efficiently. There is a single drawback of using the histogram for logging temperature data namely loosing the chronological data of the specific temperature data; But, the chronological order of the temperature is not necessary for our use-case.

The temperature data that is sampled by the Histogram module gets further processed by the State-of-Health Monitor and calculates the estimated Lifetime Failure-In-Time Rate, the current FIT Rate and the usage Ratio.

This data can be transmitted to another system such as a workstation that is receiving the processed data over User Datagram Protocol (UDP). The UDP data is saved into a database and graphically edited to support mechanics and engineers to detect usage anomalies.

B. Mission Temperature Profile Example

Figure 4 depicts an example of a temperature mission profile of a safety-critical automotive system. The diagram illustrates the temperature distribution on the first y-axis and the related FIT Rate on the second y-axis.

For each temperature value a specific De-Rating Factor needs to be calculated as seen in (1). In due consideration of the temperature distribution and the De-Rating Factor at a specific temperature the FIT Rate at this temperature value can be calculated. The plot in Figure 4 clearly depicts that with increasing temperature the De-Rating Factor increases and further the specific FIT Rate of that temperature point.

Summing up the individual FIT Rates of each temperature value results in the overall FIT Rate of the specific safety-critical automotive system. Figure 5 depicts the histogram of the Temperature Distribution of Figure 4. The histogram is used for efficiency reasons because it requires less memory and this will save production costs.

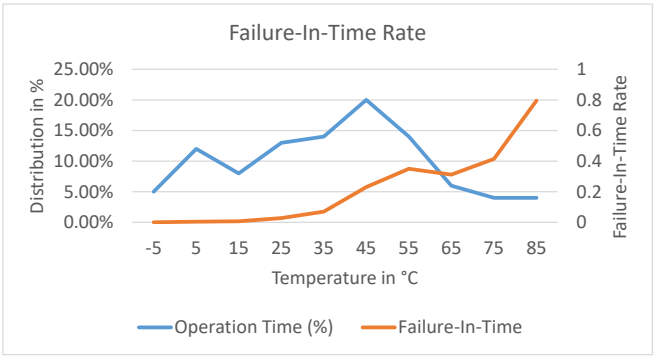

Fig. 4. Overview of the temperature distribution and the Failure-In-Time Rate at specific temperatures.

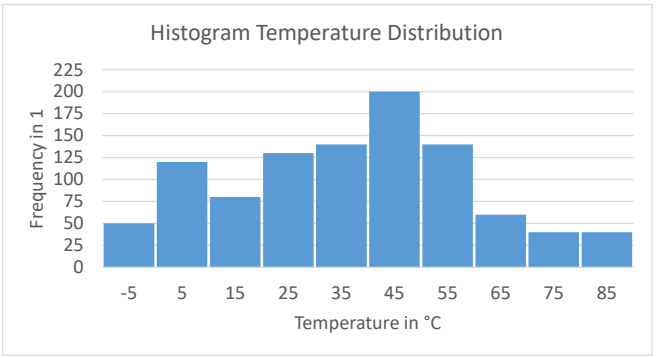

Fig. 5. Derived histogram from the operation temperature mission profile that is depicted in Figure 4.

C. Control Flow

The overall State-of-Health Monitor LiDAR platform is separated in two parts: LiDAR System and Reliability Monitor. The LiDAR system represents the rapid prototyping platform including the MEMS Driver ASIC and MEMS Mirror that is depicted in Figure 2. Additionally we have implemented the Histogram and State-of-Helath Monitor modules in the LiDAR System that are illustrated in Figure 3. In general, the State-of-Health Monitor is able to calculate the estimated Lifetime FIT but for research purpose we transmit the raw histogram values to the Reliability Monitoring device over UDP. The Reliability Monitoring is responsible to process the raw histogram values and calculate the specific FIT Rates such as expected lifetime, current rate and the ratio. These processed data gets saved in a database and displayed in a specific graphical user interface (GUI) that simplifies the work of mechanics and engineers by depicting the data as graphs. Figure 6 gives a detailed overview of the asynchronous processing steps of the LiDAR System and the Reliability Monitor:

- **LiDAR System**
  1) **Sample Temperature**
     The temperature sensor is sampling the current temperature of the semiconductor device based on the sampling frequency that is set by the configuration file.
  2) **Save Temperature Value in Histogram**
     The sampled temperature value gets pre-processed by normalizing the sampling on specific temperature values such as integer values. Afterwards the value is saved inside the temperature histogram inside a non-volatile memory.
- **Reliability Monitor**
  1) **Fetch Histogram Data**
     The histogram data of the non-volatile memory that is integrated inside the LiDAR system is transmitted to the Reliability Monitor over the UDP protocoll.
  2) **Determine Current FIT Rate**
     The current FIT Rate represents the currently "used" FIT. For this purpose the FIT Rate is construed as a credit system that can be consumed by the semiconductor device. Reaching a specific value that needs to be set individually for each device and depends on the ASIL as well as on the reliability requirements. Further information, especially the specific formulates, on calculating the Current FIT Rate can be consulted in publication [14]. The calculation can be separated in the following three processing steps:
     a) **Time Span Histogram Bins**
        The histogram bins represents different temperature values and therefore different run-times of the system at this specific temperature. Consequently, the distribution of the individual temperature bins must be calculated considering the current operation time of the system. Based on these time spans the specific FIT Rates for each histogram bin can be calculated.
     b) **Calculate FIT Rate Histogram Bins**
        Each temperature value correlates to a different De-Rating Factor as already described in equation (1). For this purpose, it is necessary to calculate the FIT Rate of each Histogram Bin separately.
     c) **Summing Up FIT Rates Histogram Bins**
        In the previous processing steps the FIT Rates for each individual histogram bin, representing a specific temperature value, have been calculated. These single values are summed up to calculate the overall FIT Rate of the current operation time of the system.
  3) **Determine Theoretical FIT Rate**
     The Theoretical FIT Rate represents the approximated FIT Rate that will be reached at the end of lifetime of the safety-critical automotive LiDAR

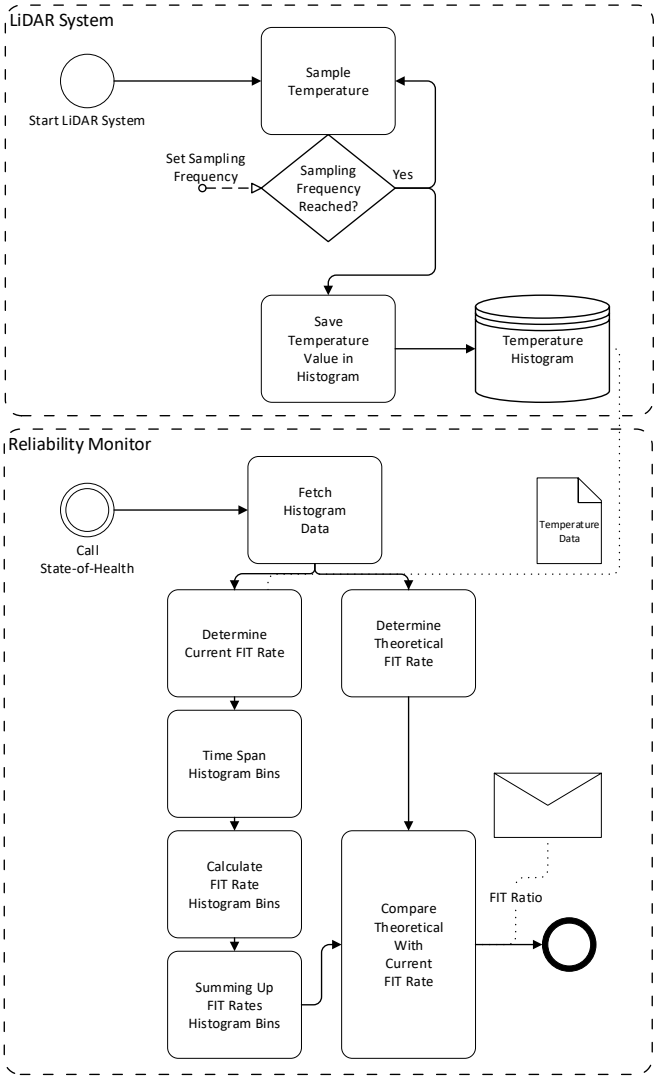

Fig. 6. Control flow of the state-of-health safety monitor that is integrated in the automotive LiDAR system.

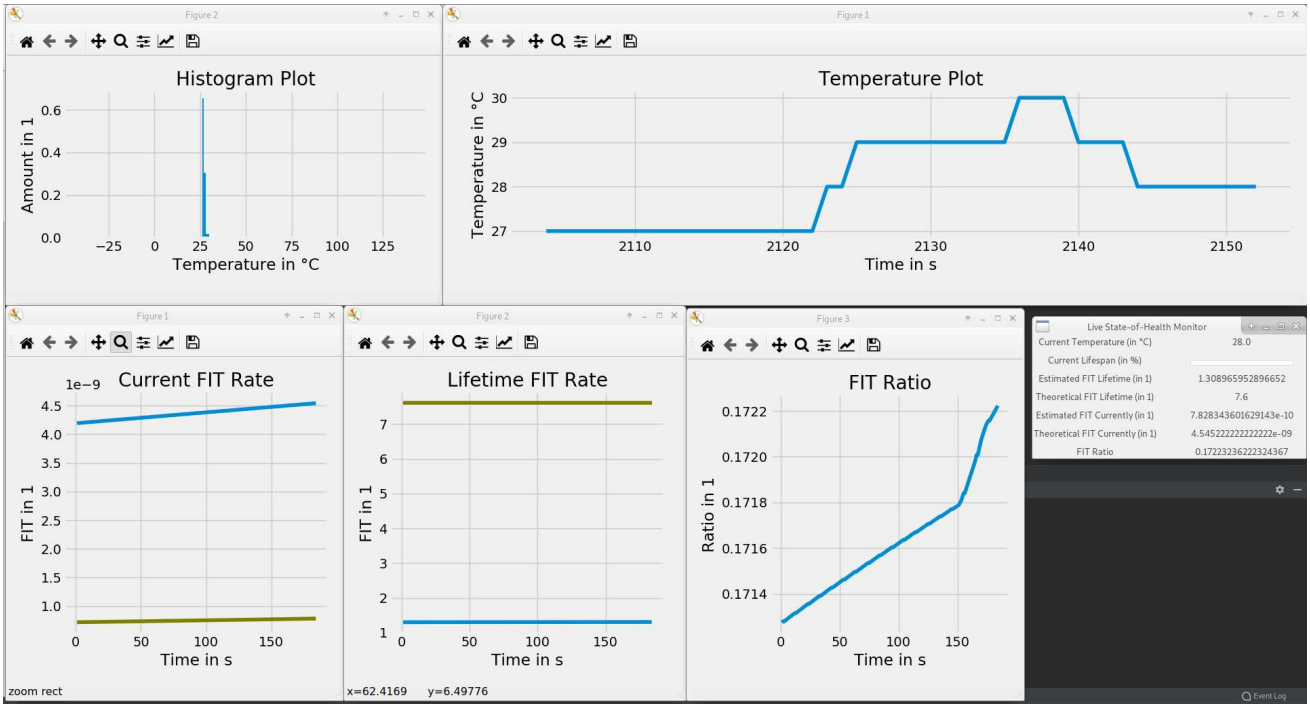

Fig. 7. Graphical User Interface of the live state-of-health monitor that was integrated in a safety-critical automotive LiDAR system.

system. This value is important to detect mismatches between the desired and indeed safety requirements and could result in an ASIL degradation.

4) **Compare Theoretical With Current FIT Rate** The comparison between the theoretical and the current FIT Ratio enables a detection of overstressing the semiconductor devices. This value can be used as an alarm after software or firmware updates.

IV. Results

In this section, we are presenting the practical results of the live state-of-health monitoring system that has been introduced in Section III. The novel monitoring concept was integrated into the 1D MEMS Micro-Scanning LiDAR system. The platform was heated and cooled within an environmental chamber.

Figure 7 depicts the GUI of the live state-of-health safety monitoring system that was implemented for providing reliability information to engineers and mechanics. The graphical interface provides live run-time data in diagrams as well as an overview plot of the different FIT Rates such as the current FIT Rate. In the Temperature Plot the temperature profile that was applied to the 1D MEMS Micro-Scanning LiDAR system during the experiment can be depicted. Based on this temperature data the Histogram Plot is created and represents the complete temperature profile of the overall run-time. The Current and Lifetime FIT Rate plot represents a line for the current and theoretical value of the specific FIT Rate and is used as an optical indicator if the current FIT Rate is exceeding the designed usage of the system. Additionally, to increase the comprehensibility engineers and mechanics are also able to use the FIT Ratio that provides the possibility to detect overstress anomalies that are caused by software or firmware updates. In the FIT Ratio plot it can be seen that there was an intense increase of the FIT Rate and this can be one of the key indicators of a mismatch between the designed temperature mission profile and the real one. The data that are plotted in the diagrams are also displayed as values. These results of the experimental attempt can also be seen in Table I. The experiment resulted in an estimated lifetime FIT of about 1.3 and considering the theoretical lifetime FIT of 7.6 results in a FIT Ratio of 0.17. This ratio means that if the 1D MEMS Micro-Scanning LiDAR system operates in the same environmental conditions will result in an overdesigned system. Future redesigns of the system could be used to optimize the materials to reduce costs.

TABLE I
Results of the experimental attempt of the live state-of-health monitor for the automotive LiDAR system.

Data	Value
Current Temperature in Degree Celsius	28.0
Estimated FIT Lifetime in 1	1.309
Theoretical FIT Lifetime in 1	7.6
Estimated FIT Currently in 1	7.23E-10
Theoretical FIT Currently in 1	4.55E-09
FIT Ratio	0.17

V. Conclusion

In this publication, we have introduced a novel live state-of-health safety monitoring system for a safety-critical automotive LiDAR system that will be used for autonomous driving.

One of the key-challenges was to record the reliability data efficiently and to consider the whole operation time of the system.

In Section II, we introduced the physical backgrounds of reliability in terms of semiconductor devices. Based on these physical backgrounds we provided an overview about previous research work with a similar focus of reliability monitoring. In contrast to the previous researchers, this publication focus on a reliability monitor concept that is in compliance with the automotive ISO 26262 Road vehicle safety standard. Furthermore, the work of previous researchers also did not focus on recording the reliability data efficiently.

The next Section III introduced the novel 1D MEMS Micro-Scanning LiDAR system architecture including the novel state-of-health safety monitor. For this purpose, we implemented additional modules inside the LiDAR system and an UDP interface to an external device that is responsible for fetching the reliability data and provide a graphical visualization for engineers and mechanics. A detailed overview of the control flow of both systems can be depicted in Figure 6.

The results of Section IV clearly depicts the feasibility of this monitor system and provides live reliability data of the LiDAR system. In our case, we have observed that the LiDAR system was highly robust considering the temperation mission profile of our test case. This resulted in a FIT Ratio of about 0.17 and this can be used as an indicator for redesigns possibilities to save production costs.

In the next few years, autonomous driving will disruptively change the automotive industry. In the past, the driver was the most important backup for failures but this backup solution will be missing with fully-autonomous driving vehicles. Future semiconductor devices must be higly reliable and any failures must be detected in prior to prevent hazardous situations. The novel live state-of-health monitoring system for LiDAR systems we have introduced in this publication is one solution for solving this key problem of autonomous driving. This safety monitor can also be used for any other safety-critical automotive system because of the compliance with the automotive safety standard ISO 26262.

VI. Acknowledgments

The authors would like to thank all national funding authorities and the ECSEL Joint Undertaking, which funded the PRYSTINE project under the grant agreement number 783190.

PRYSTINE is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2018 and April 2021 (grant number 865310). More information: https://iktderzukunft.at/en/.

References

[1] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "Prystine - programmable systems for intelligence in automobiles," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, Aug 2018, pp. 618–626.

[2] R. Faria, L. Brito, K. Baras, and J. Silva, "Smart mobility: A survey," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, July 2017, pp. 1–8.

[3] N. Lang, M. Rüßmann, A. Mei-Pochtler, T. Dauner, S. Komiya, X. Mosquet, and X. Doubara, "Self-driving vehicles, robo-taxis, and the urban mobility revolution," *The Boston Consulting Group*, vol. 7, p. 2016, 2016.

[4] N. Druml, I. Maksymova, T. Thurner, D. Van Lierop, M. Hennecke, and A. Foroutan, "1D MEMS Micro-Scanning LiDAR," in *Conference on Sensor Device Technologies and Applications (SENSORDEVICES)*, 09 2018.

[5] J. Hecht, "Lidar for self-driving cars," *Optics and Photonics News*, vol. 29, no. 1, pp. 26–33, 2018.

[6] I. n. E. ISO, "Draft 26262 2nd Edition: Road vehicles-Functional safety," *International Standard ISO/FDIS*, vol. 26262, 2018.

[7] D.-G. Yang, F. Wan, Z. Shou, W. D. van Driel, H. Scholten, L. Goumans, and R. Faria, "Effect of high temperature aging on reliability of automotive electronics," *Microelectronics Reliability*, vol. 51, no. 9-11, pp. 1938–1942, 2011.

[8] T. IEC, "62380," *Reliability data handbook–universal model for reliability prediction of electronics components, PCBs and equipment (emerged from UTEC 80-810 or RDF 2000)*, 2004.

[9] C. Johansson, J. Arwidson, and T. Månefjord, "An fpga-based monitoring system for reliability analysis," in *Additional Conferences (Device Packaging, HiTEC, HiTEN, & CICMT)*, vol. 2017, no. NOR. International Microelectronics Assembly and Packaging Society, 2017, pp. 1–4.

[10] J. C. Vazquez, V. Champac, A. Ziesemer, R. Reis, I. C. Teixeira, M. B. Santos, and J. P. Teixeira, "Built-in aging monitoring for safety-critical applications," in *2009 15th IEEE International On-Line Testing Symposium*. IEEE, 2009, pp. 9–14.

[11] K. Arabi and B. Kaminska, "Built-in temperature sensors for on-line thermal monitoring of microelectronic structures," in *Proceedings International Conference on Computer Design VLSI in Computers and Processors*. IEEE, 1997, pp. 462–467.

[12] S. Majerus, X. Tang, J. Liang, and S. Mandal, "Embedded silicon odometers for monitoring the aging of high-temperature integrated circuits," in *2017 IEEE National Aerospace and Electronics Conference (NAECON)*. IEEE, 2017, pp. 98–103.

[13] M. Civilini, "Reliability and field aging time using temperature sensors," in *2010 Fourth International Conference on Sensor Technologies and Applications*. IEEE, 2010, pp. 210–213.

[14] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "Live state-of-health safety monitoring for safety-critical automotive systems," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*, Aug 2019.

Enabling Fail-Operational Behavior and Degradation for Safety-Critical Automotive 3D Flash LiDAR Systems

Omitted for Blind Review

***Abstract*—Advancing the current Advanced Driver Assistance Systems (ADAS) is coupled with introducing novel technologies into the automotive domain such as Light Detection and Ranging (LiDAR). LiDAR is attributed as a key-technology that will be one of the key enablers for safe and reliable automated driving. Considering the fact that vehicles nowadays rely on the driver in safety-critical situations leads to the problem that in a fully-automated driving scenario the vehicle needs to control every possible situation on its own. This increases the requirements and the overall safety level of the system but also for each component and needs a gradual transition from fail-safe to fail-operational behvior at least as long as the occupants and other road participants could be endangered.**

This publication introduces a novel system architecture of a fail-operational 3D Flash LiDAR System that enables dynamic system degradation during run-time as well as internal built-in self-test (BIST) for automated failure injection tests. The novel fail-operational system architecture is able to handle critical temperature ranges as well as long-term memory faults.

***Index Terms*—Automotive LiDAR, Fail-Operational, Degradation, Dynamic Safety, Memory Faults**

I. Introduction

The concept of fail-safe behavior is one of the key methodology that is used in the automotive domain for safety-critical systems to handle failures during run-time [2]. But this concept will not fullfill the requirements of future fully-automated driving vehicles because of the need of a human driver as a fall-back scenario who is able to control the vehicle. Future fully-automated driving vehicles that are able to provide driving services at SAE Automated Driving Level 4 or 5 will control all possible driving scenarios on their own, including situations in which safety-critical systems partly fail [4]. This

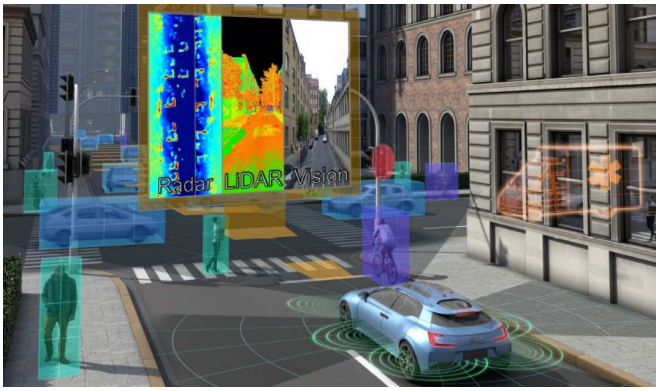

Fig. 1. PRYSTINE's concept view of a fail-operational urban surround perception system [1].

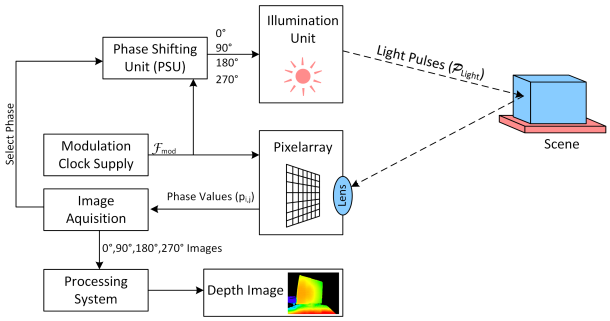

Fig. 2. Conceptional overview of a 3D Flash LiDAR system [3].

fact will force a paradigma change and requires a transition from fail-safe behavior to fail-operational behavior. Especially sensors that are responsible for providing environmental perception data needs to be highly robust and safe. This key requirement for future automated driving systems has already been identified by the European research project PRYSTINE (Programmable Systems for Intelligence in Automobiles). One of the key goals of PRYSTINE is about introducing a novel Fail-Operational Urban Surround perception (FUSION) which is based on LiDAR and RADAR sensors as seen in Figure 1. FUSION will be an enabler for safe automated driving in urban and rural environments [1].

In contrast to RADAR, which is already widely used in the automotive domain for ADAS such as Adaptive Cruise Control (ACC), is LiDAR not very common in the aumotive domain yet because of the highly costs of the current mechanical spinning LiDAR systems [5], [6]. One possible key changer could be the novel 1D MEMS Micro-Scanning LiDAR system concept, as seen in Figure 2, by Druml et al. which will reduce the costs to approximately 250 Dollar and enables robust and safe automated driving functionalities for middle class vehicles [7]. This novel system is based on a scanning technology which is enabled by an oscillating MEMS mirror. On the other hand there are also non-scanning LiDAR systems such as the diffuse light cone Flash LiDAR system as seen in Figure 2 that are already available on the market.

This publication describes a novel fail-operational, safety-critical Automotive 3D Flash LiDAR system architecture that enables degradation of specific functions to guarantee the correct behavior of the system in case of failures. Our provided solution makes the following fundamental contributions:

- Describing 3D Flash LiDAR degradation possibilities that enables correct data for other ADAS and ensures safe driving.
- Providing a prototype that proves feasibility of a novel fail-operational 3D Flash LiDAR system architecture that enables degradation from a safety point of view.
- Introducing a novel Testplatform that is able to verificate the novel introduced degradation functions of the 3D Flash LiDAR prototype.

This paper is structured as follows. Section I gives a short introduction into the topic and what research output is provided by this publication. In Section II, we are providing information about current challenges and other related work in the topic of fail-operational 3D Flash LiDAR systems. Section III introduces our novel fail-operational 3D Flash LiDAR system architecture that enables degradation of safety-critical functions. The evaluation and results can be seen in Section IV such as the Graphical Control Interface that enables the testing of the novel degradation functions of the implemented prototype. Finally, we concluded our results in Section V.

II. Related Work

The change from traditional controlled vehicles by the driver to autonomous driving vehicles requires higher safety standards. The discontiunation of the driver as a control backup in case of a failure will enforce a disruptive change of designing safe and robust vehicles [8]. Any failure that appears during driving must be handled by the system itself and is also known as fail-operational behavior [9], [10]. For this purpose, specific functions must be degraded to a point at which the vehicle still can operate in a safe way that decreases the probability of an accident to the lowest possible limit.

In the next few years, Light Detection and Ranging (LiDAR) will be one of key sensors for environmental perception in automated driving vehicles [1], [7]. LiDAR scans the front scene of the sensor by emiting a laser pulse that is reflected by the objects of the scenery and is received by a photo diode. The measurement range from the LiDAR system is primary defined from the output power of the laser. Because of eye-, and skin-safety the laser must guarantee a specific maximal output power. For that reason, the maximal possible distance is already limitied through that safety specification and can not be extended by increasing the laser power [7]. One negative side effect is that the output power of a laser is affected by the overall temperature. Yulianto et al. [11] described that with a Distributed Feedback Laser (DFL) with an operation wavelength of 1550 nm the slope of the output power was -0.33 mW/°C. Additionally, also the wavelength is varying by the laser temperature with a slope of 0.094nm/°C. Transfered to the automotive LiDAR system would result in a possible decrease of the maximum operation distance. In worst case, this would vary during operation based on the current temperature that is mostly influenced by the current weather conditions.

Volatile Memory such as Random-Access Memory is necessary to cache sensor data as well as computation results. Especially for LiDAR big on-chip memory arrays are needed [12]. Maksymova et al. [13] described that the amount of data that needs to cached depends on several key parameters of the LiDAR system such as image and range resolution, frames per second, sampling frequency, and others. The last trends in the automotive domain is to use for highly computational tasks consumer modified hardware components such as the Intel Atom A3900 [14]. In the A3900 datasheet [15] the supported memory technology are DDR3L/ECC and LPDDR4. The DDR3L/ECC technology is the same technology that are used in business servers. For Dynamic Random Access Memory (DRAM) technology several research studies are already available that are describing potential soft errors, transient errors and failures in these modules and counter measures [16]–[19]. Especially the large-field study of Schroeder et al. [19] must be emphasized that describes a study of DRAM errors within two years considering multiple vendors, generations, technologies and capacities. Most of the annual incidence errors that appeared were corrected by the internal Error Correction Code (ECC) but there were about 1.3% of uncorrectable errors per machine and 0.22% uncorrectable errors per DIMM. An interesting fact is that temperature does not impact the incidence of memory errors but utilization does [19]. This results in the requirement to consider the utilization of the volatile memory module of the LiDAR system.

In general, fail-operational behavior of safety-critical embedded systems can be achieved by introducing redundant subsystem design and diversity, as described in the IEC 61508 safety standard of Electronic systems [20]. Fail-Operational behavior is particularly important for systems that do not have the possibility of a mechanical fallback. For that specific systems novel system design approaches have been introduced such as the 2-out-of-3 architecture. In this case, three indepentend systems perform the same tasks and a voting system decides about the correctness of the output [9]. But there are also researchers in the field of fail-operational systems that are enabling this function by introducing a dynamic configuration of their system [21], [22]. For that reason, we are inclined to take the path of dynamically reconfiguring the 3D Flash LiDAR system during operation, in case of failure, and enable a continuous performance of the system to keep up the overall automated driving service as long as needed to prevent any fatal damages. Additionally, we want to decrease the possibility of material fatigue of the components and increase the mean-time-between failures. This will increase the overall safety of the whole system as well as decrease possible costs caused by guarantee services.

III. Fail-Operational 3D Flash Lidar System

This Section gives an overview about the novel developed fail-operational 3D Flash Lidar system architecture that supports automatic degradation in failure cases as well as to take care of safety-critical hardware parts to extend lifetime.

The main focus of the novel system architecture is to focus on a safe behavior in any possible situation. For this purpose, we identified that one of the worst scenarios is driving with

high speed on a highway, fully-autonomous and the driver is distracted while the Lidar system is loosing environmental perception. In this particular situation, the vehicle is not able to recover from this situation on its own. Traditional developed vehicles that rely on the driver as a backup system would cause a crash with all consequences such as harmed passengers or worse. Modern vehicles with functionalities that consider self-driving behavior such as Adaptive Cruise Control (ACC) require higher standards for safety-critical components such as fail-operational behavior. For this reason, we decided to develop a novel system architecture for an environmental perception system that is based on Lidar that fulfills the requirement of a fail-operational behavior and is able to degrade functions in specific context such as driving in an overcrowded city or on a highway.

A. System Architecture

In Figure 4 an overview of the novel fail-operational 3D Flash Lidar system architecture can be depicted. The system is divided in two main parts:

- **System Control**
  This sub-system is handling the configuration of the overall system as well as controlling the overall fail-operational processes and application.
- **Memory Manager**
  The Memory Manager is responsible to store data on the memory and continously checks integrity of individual memory blocks.

The system receivs raw input data from the 3D Flash Lidar system to the Memory Manager. The Memory Manager is able to disable specific memory blocks in case of failures and this allows a longer lifetime of the system because faulty memory blocks can be disabled and does not infect higher layers of the processing chain. This data is processed by the application that is fetching the data from the memory. The system controller can be configured by external configuration with focus on preserving memory faults and temperature caused faults. To achieve these targets the control system is able to modify frames per second of the output data, frequency of the processor or resolution of the output image.

1) Preserving Memory Faults: As we have described the common problem with worn out EMMC chips from Tesla vecicles in the Section about Related Work clearly depicts that memory faults could be one of the most common faults for future fully-autonomous vehicles that are using centralized computation platforms for computational tasks [23]. To prevent this circumstance the novel system architecture focusses on this specific problem by enabling an automatic degradation mode for memory faults.

The novel memory monitoring system can be depicted in Figure 5 and is storing the raw data from the 3D Flash Lidar system into the memory block according the index array. Any fault inside the memory block that gets detected triggers the automatic memory degradation algorithm that is deciding about the further processing of the faulty memory block. For this purpose, the algorithm is introducing a generation based memory management. In the first generation are memory blocks without any occuring error. The second generation are memory blocks that are classified as suspicious and the memory blocks get verified more frequently. This prevents that memory blocks are getting excluded because of external events such as soft errors. In the third generation are memory blocks

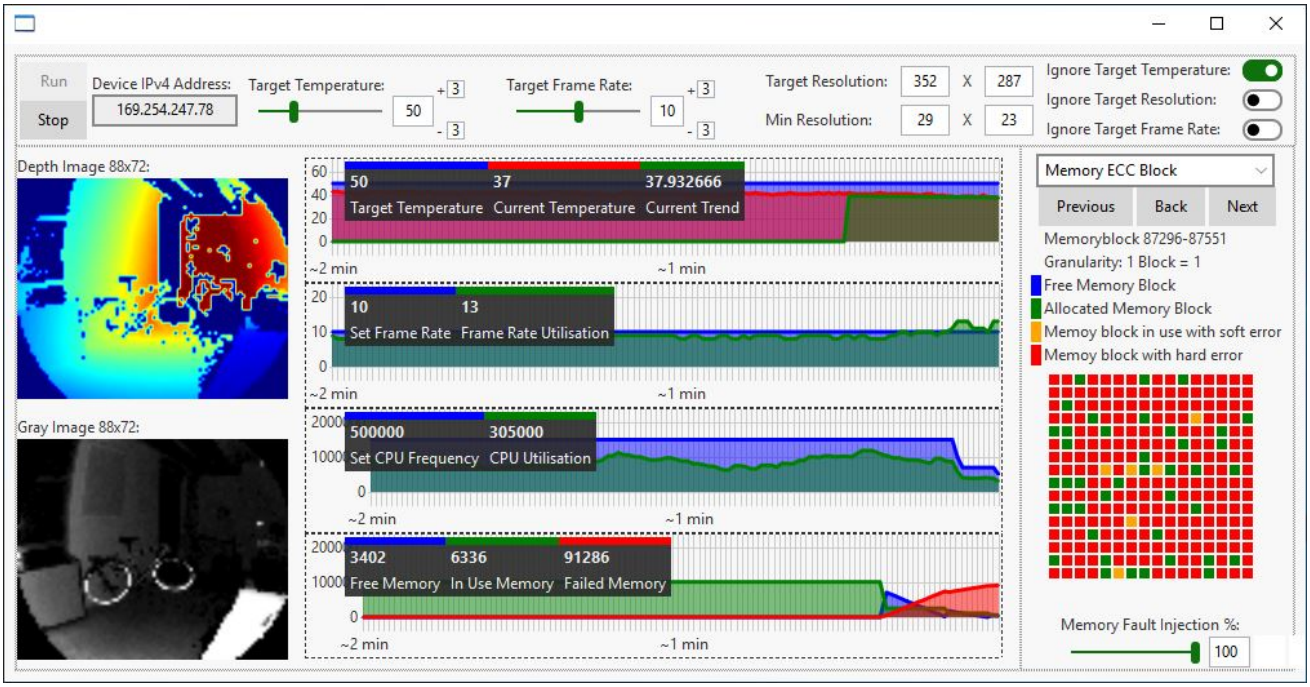

Fig. 3. Graphical Control Interface that depicts the current live camera data, settings, and current monitoring data.

placed that are not reliable enough anymore and are excluded from storing data.

2) Efficient and Effective Resolution Adaption: One of the most effective ways of reducing computational utilization is about reducing raw pixel data. For this purpose, the novel system architecture is reducing the amount of pixels by skipping a specific amount of pixels as depicted in Figure 6. The system is able to automatically degradate the resolution between the factor one to four. The main focus from a safety point of view was to still provide enough information inside the image that computer vision algorithm are still able to interpret the data in a correct way as seen in Figure 7. Additionally, the system is not able to reduce the amount of pixels in each situation. In specific situations, such as driving in an overcrowded city the system should not be able to reduce the pixels on purpose. Just in emergency cases, if the system would otherwise result in a total failure a degradation is allowed. In other non safety-critical cases like driving on a highway the system is allowed to reduce the resolution on purpose. This guarantees a safe behavior for passengers as well as other road participants.

B. Integrated Testing Functions

1) Realistic Scenario Simulations: Testing is necessary to provide information about reliability and utilization of hardware components. Nowadays, most of these tests are performed by statistical tests in which specific road types are mapped to a specific time. In the near future, these tests can be advanced to more sophisticated real data scenarios that can be obtained by using data from the European eCall system or similar systems that are able to provide GPS data. These data sets can be used to test the real utilization of the hardware components and enable more precise optimization of specific components with the positive side-effects of reducing ressource usage and costs.

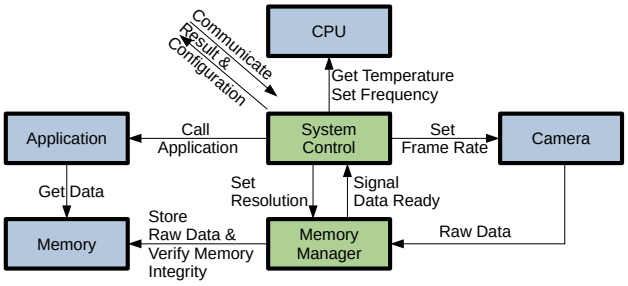

Fig. 4. Overview of the novel fail-operational 3D Flash Lidar system architecture.

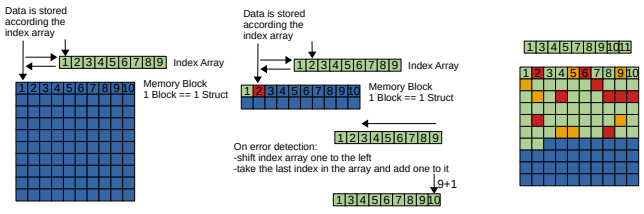

Fig. 5. Concept of the preserving memory fault system architecture that has been integrated in the novel fail-operational 3D Flash Lidar platform.

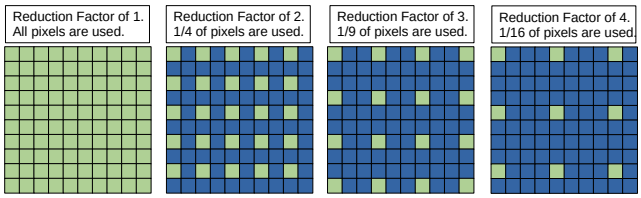

Fig. 6. Overview of the efficient and effective resolution adaption algorithm that is implemented in the novel fail-operational 3D Flash Lidar system.

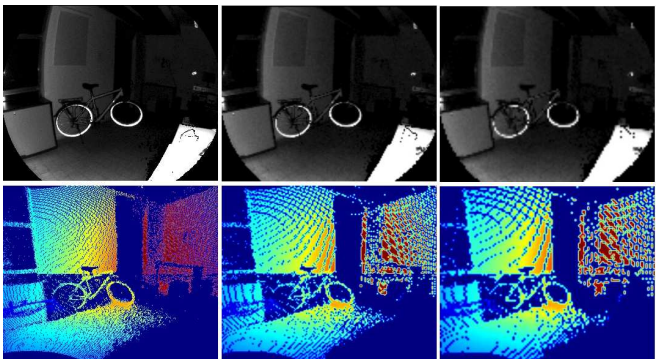

Fig. 7. Adaptive resolution example containing grey images and depth information images of the 3D Flash Lidar system of a bicycle scene. The resolution is reduced from 352x287 (left photo) to 118x96 (right photo).

For this reason, our novel system architecture is able to test real-life usage scenarios in which road trips can be defined and virtually driven. The system will automatically change the configuration of the 3D Flash Lidar system based on the actual road type. This enables the testing of the system in real scenarios to increase the trustiness of the resulting reliability estimation.

2) Memory Fault Injection: Memory is necessary to store data from the sensors as well as computational results. The integrity of the stored values inside volatile memory is crucial for correct computation and reliable quality of the output results. If individual memory blocks get corrupted over time results in an unpredictable behavior of the whole system. For that reason, the novel system architecture has built-in a memory fault injection module that is able to disable a variety of memory blocks as seen in Figure 5. This enables us to verfivy the degradation and fail-operational behavior functions of the novel system.

C. Graphical Control Interface

The novel system-architecture offers a TCP/IP interface which offers a service providing environmental perception data as well as monitoring data to external systems. As a client we have developed a Graphical Control Interface (GCI) as seen in Figure 3 that displays the current live data from the 3D Flash LiDAR system as well as current safety-critical sensor values such as temperature, frame rate, memory usage, and CPU frequency. The GCI also provides settings for testing specific usage scenarios of the whole platform to derive behavioral patterns such as temperature trends and CPU throttling.

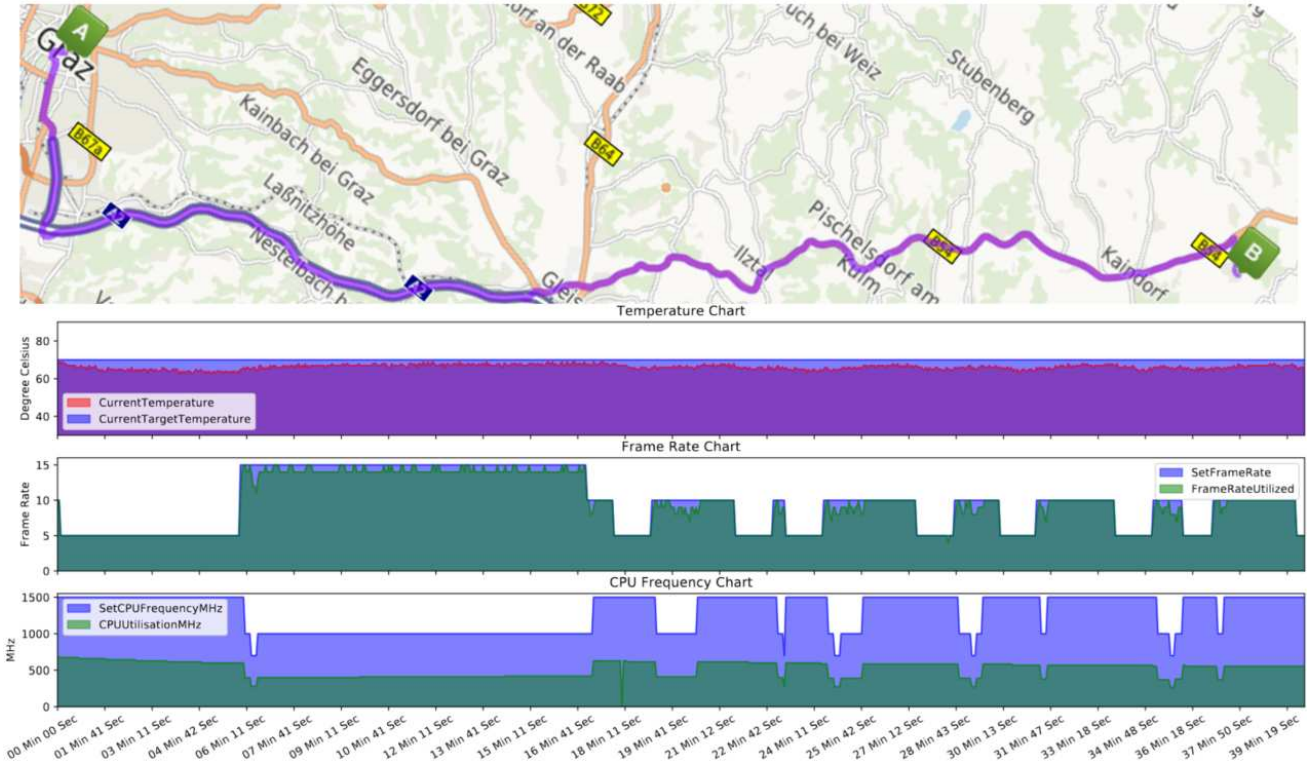

Fig. 8. Test run of a an average commuter route between Graz and Hartberg and the related monitoring data.

IV. Results

This Section describes the results of the novel fail-operational 3D Flash Lidar system architecture that enables the degradation of the environmental perception functionality and enables a safe driving for SAE Automated Driving Level 4 vehicles.

Figure 3 clearly depicts the graphical monitoring system of the novel implemented system-architecture. On the left side, the current environmental perception data (Depth Image and Gray Image) can be seen and is continously updating with a specific frame rate. The target frame rate can be specified in the upper section of the GCI as well as the maximal targeted temperature and the preferred resolution including the minimum allowed resolution. This resolution can be adapted according driving scenarios such as urban areas or highways. Additionally the framework allows to ingore individual parameters such as temperature, resolution or frame rate. In the middle section of the GCI the current sensor values of the overal system architecture temperature, frame rate of the live 3D Flash LiDAR data, CPU frequency and memory usage can be seen. On the right side is the memory fault injection module that is able to disable a specific amount of memory blocks for testing degradation and fail-operational behavior considering memory faults.

The novel system architecture was tested with the integrated realistic scenario simulation with a virtual test run between Graz and Hartberg. The route was separated into specific sections with meta information about road type and speed limit. Generally these values would be provided by additional ADAS that are common available in middle-class cars nowadays.

In Figure 8 the route can be depicted on map as well as the resulting monitoring results of the test run. The main focus in this scenario was the strict adherence of the specific system architecture temperature of 70°C because temperature is one of the most crucial parameters for reliability. Higher temperature directly results in lower reliability and higher FIT Rates. Higher FIT Rates could potentially degrade the overall Automotive Safety Integrity Level. The temperature diagram clearly depicts that this limit was strictly adhered by the system architecture by dynamically adapting the CPU frequency of the computation platform as well the frame rate of the 3D Flash LiDAR sensor.

V. Conclusion

In this publication we have introduced a novel fail-operational 3D Flash LiDAR system architecture. The architecture enables the system to dynamically adapt specific parameters to strictly adherence safety-critical parameters such as temperature.

In Section III we have described the general system-architecture and implemented built-in self tests. Considering the last trends of the automotive industry of using EMMC memory and the resulting faults [23] we have integrated a memory fault injection module that is able to simulate faults in multiple memory blocks to test the direct and indirect impacts of these failures. The resulting degradation of the system by

adapting the environmental perception data resolution shows that the scene still could be properly interpreted by higher level computer vision algorithms as seen in Figure 6.

The test scenario of an average commuter route test run between Graz and Hartberg that is described in Section IV clearly indicates the effective performance of the dynamic degradation of the platform considering specific safety-critical parameters. In this case, we have set the limit of the general system architecture temperature range because this is one of the most crucial parameters for reliability for hardware components.

In the next few years, vehicles will perform the transformation from SAE Automated Driving Level 3 to 4 and this will require higher safety standards because of the absence of a human driver that is able to retake the driving control. For this reason, reliability and fail-operational behavior will become to the most important parameters for the general safety of road vehicles. The novel introduced fail-operational 3D Flash LiDAR system architecture proves feasibility and gives an overview of a possible solution for safety-critical environmental perception sensors such as LiDAR.

VI. Acknowledgments

Omitted for blinded review.

References

[1] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, S. Kumar, G. Dimitrakopoulos, and H. Roedig, "Prystine - programmable systems for intelligence in automobiles," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, Aug 2018, pp. 618–626.

[2] I. n. E. ISO, "Draft 26262 2nd Edition: Road vehicles-Functional safety," *International Standard ISO/FDIS*, vol. 26262, 2018.

[3] H. Plank, T. Egger, C. Steffan, C. Steger, G. Holweg, and N. Druml, "High-performance indoor positioning and pose estimation with time-of-flight 3d imaging," in *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Sep. 2017, pp. 1–8.

[4] J. Dokic, B. Müller, and G. Meyer, "European roadmap smart systems for automated driving," *European Technology Platform on Smart Systems Integration*, p. 39, 2015.

[5] S. Tokoro, K. Kuroda, A. Kawakubo, K. Fujita, and H. Fujinami, "Electronically scanned millimeter-wave radar for pre-crash safety and adaptive cruise control system," in *IEEE IV2003 Intelligent Vehicles Symposium. Proceedings (Cat. No. 03TH8683)*. IEEE, 2003, pp. 304–309.

[6] J. Hecht, "Lidar for self-driving cars," *Optics and Photonics News*, vol. 29, no. 1, pp. 26–33, 2018.

[7] N. Druml, I. Maksymova, T. Thurner, D. Van Lierop, M. Hennecke, and A. Foroutan, "1D MEMS Micro-Scanning LiDAR," in *Conference on Sensor Device Technologies and Applications (SENSORDEVICES)*, 09 2018.

[8] M. Kyriakidis, J. C. de Winter, N. Stanton, T. Bellet, B. van Arem, K. Brookhuis, M. H. Martens, K. Bengler, J. Andersson, N. Merat *et al.*, "A human factors perspective on automated driving," *Theoretical Issues in Ergonomics Science*, vol. 20, no. 3, pp. 223–249, 2019.

[9] A. Kohn, M. Käßmeyer, R. Schneider, A. Roger, C. Stellwag, and A. Herkersdorf, "Fail-operational in safety-related automotive multi-core systems," in *10th IEEE International Symposium on Industrial Embedded Systems (SIES)*, June 2015, pp. 1–4.

[10] N. Druml, O. Veledar, G. Macher, G. Stettinger, S. Selim, J. Reckenzaun, S. E. Diaz, M. Marcano, J. Villagra, R. Beekelaar, J. Jany-Luig, M. M. Corredoira, P. Burgio, C. Ballato, B. Debaillie, L. van Meurs, A. Terechko, F. Tango, A. Ryabokon, A. Anghel, O. Icoglu, S. S. Kumar, and G. Dimitrakopoulos, "Prystine - technical progress after year 1," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*, Aug 2019, pp. 389–398.

[11] N. Yulianto, B. Widiyatmoko, and P. S. Priambodo, "Temperature effect towards dfb laser wavelength on microwave generation based on two optical wave mixing," *Int. J. Optoelectron. Eng.*, vol. 5, no. 2, pp. 21–27, 2015.

[12] I. Maksymova, C. Steger, and N. Druml, "Extended delta compression algorithm for scanning lidar raw data handling," *International Conference on Intelligent Robots and Systems*, 2019.

[13] I. Maksymova, N. Druml, and C. Steger, "Review of lidar sensor data acquisition and compression for automotive applications," in *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 2, no. 13, 2018, p. 852.

[14] S. Han, Y. Wang, S. Liang, S. Yao, H. Luo, Y. Shan, and J. Peng, "Reconfigurable processor for deep learning in autonomous vehicles," 2017.

[15] Intel, "Intel Atom Processor E3900 and A3900 Serie Datasheet," 2019.

[16] R. Baumann, "Soft errors in advanced computer systems," *IEEE Design Test of Computers*, vol. 22, no. 3, pp. 258–266, May 2005.

[17] C.-L. Chen and M. Hsiao, "Error-correcting codes for semiconductor memory applications: A state-of-the-art review," *IBM Journal of Research and development*, vol. 28, no. 2, pp. 124–134, 1984.

[18] A. H. Johnston, "Scaling and technology issues for soft error rates," 2000.

[19] B. Schroeder, E. Pinheiro, and W.-D. Weber, "Dram errors in the wild: a large-scale field study," *ACM SIGMETRICS Performance Evaluation Review*, vol. 37, no. 1, pp. 193–204, 2009.

[20] I. E. Comission, "IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems," 2009.

[21] T. Ishigooka, S. Honda, and H. Takada, "Cost-effective redundancy approach for fail-operational autonomous driving system," in *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*, May 2018, pp. 107–115.

[22] F. Oszwald, J. Becker, P. Obergfell, and M. Traub, "Dynamic reconfiguration for real-time automotive embedded systems in fail-operational context," in *2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, May 2018, pp. 206–209.

[23] T. Nardi, "Worn Out EMMC Chips Are Crippling Older Teslas," Oct 2019. [Online]. Available: https://hackaday.com/2019/10/17/worn-out-emmc-chips-are-crippling-older-teslas/

Bibliography

[1] "Car Costs - Automotive Electronics Costs Worldwide 2030, [online]." www.statista.com/ statistics/ 277931/ automotive-electronics -cost-as-a-share -of-total-car -cost-worldwide/. [09.07.2020].

[2] N. Druml, G. Macher, M. Stolz, E. Armengaud, D. Watzenig, C. Steger, T. Herndl, A. Eckel, A. Ryabokon, A. Hoess, *et al.*, "Prystine-programmable systems for intelligence in automobiles," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, pp. 618–626, IEEE, 2018.

[3] N. Druml, I. Maksymova, T. Thurner, D. van Lierop, M. Hennecke, and A. Foroutan, "1d mems micro-scanning lidar," in *International Conference on Sensor Device Technologies and Applications (SENSORDEVICES)*, 2018.

[4] "V-Model (software development), [online]." `https://en.wikipedia.org/wiki/V-Model_(software_development)`. [09.07.2020].

[5] S. P. Roger, *Software engineering: a practitioner's approach*. McGraw-Hill Education, 2019.

[6] "Levels of Automation for Autonomous Ground Vehicles, [online]." medium.com/ @BabakShah/ levels -of -automation -for -self -driving -cars -d410a4f679b7. [09.07.2020].

[7] Z. H. Khan and A. Khan, "Perspectives in automotive embedded systems: From manual to fully autonomous vehicles," 11 2015.

[8] "Bathtub curve, [online]." `https://en.wikipedia.org/wiki/Bathtub_curve`. [09.07.2020].

[9] A. Webber, "Calculating Useful Lifetimes of Embedded Processors," in *Application Report SPRABX4B*, Texas Instruments, 2020.

[10] I. n. E. ISO, "ISO 26262 2nd Edition: Road vehicles-Functional safety," *International Standard ISO/FDIS*, vol. 26262, 2018.

[11] A. Sadula, "Design and implementation of a high precision instrumentation system," 2016.

[12] A. Strasser, "Overview of the ISO 26262 Semiconductor Guideline, [Internal Seminar Paper]," 2020.

[13] A. Webber, *Calculating FIT for a MissionProfile*. Texas Instruments, 2015.

[14] G. P. Pandian, D. Diganta, L. Chuan, Z. Enrico, and M. Pecht, "A critique of reliability prediction techniques for avionics applications," *Chinese Journal of Aeronautics*, vol. 31, no. 1, pp. 10–20, 2018.

[15] T. C. AEC, "AEC-Q100: Failure Mechanism Based Stress Test Qualification For Integrated Circuits," vol. 100, 2014.

[16] C. Johansson, J. Arwidson, and T. Månefjord, "An fpga-based monitoring system for reliability analysis," in *Additional Conferences (Device Packaging, HiTEC, HiTEN, & CICMT)*, vol. 2017, pp. 1–4, International Microelectronics Assembly and Packaging Society, 2017.

[17] S. Mhira, V. Huard, A. Jain, F. Cacho, D. Meyer, S. Naudet, A. Bravaix, and C. Parthasarathy, "Mission profile recorder: An aging monitor for hard events," in *2016 IEEE International Reliability Physics Symposium (IRPS)*, pp. 4C–3, IEEE, 2016.

[18] M. Civilini, "Reliability and field aging time using temperature sensors," in *2010 Fourth International Conference on Sensor Technologies and Applications*, pp. 210–213, IEEE, 2010.

[19] K. Takeuchi, M. Shimada, T. Okagaki, K. Shibutani, K. Nii, and F. Tsuchiya, "Wear-out stress monitor utilising temperature and voltage sensitive ring oscillators," *IET Circuits, Devices & Systems*, vol. 12, no. 2, pp. 182–188, 2017.

[20] A. Abdulkhaleq, D. Lammering, S. Wagner, J. Röder, N. Balbierer, L. Ramsauer, T. Raste, and H. Boehmert, "A systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles," *Procedia Engineering*, vol. 179, no. Supplement C, pp. 41–51, 2017.

[21] M. Berk, O. Schubert, H.-M. Kroll, B. Buschardt, and D. Straub, "Reliability assessment of safety-critical sensor information: Does one need a reference truth?," *IEEE Transactions on Reliability*, vol. 68, no. 4, pp. 1227–1241, 2019.

[22] S. Khastgir, H. Sivencrona, G. Dhadyalla, P. Billing, S. Birrell, and P. Jennings, "Introducing asil inspired dynamic tactical safety decision framework for automated vehicles," in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–6, IEEE, 2017.

[23] R. Salay, M. Angus, and K. Czarnecki, "A safety analysis method for perceptual components in automated driving," in *2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE)*, pp. 24–34, IEEE, 2019.

[24] I. Colwell, B. Phan, S. Saleem, R. Salay, and K. Czarnecki, "An automated vehicle safety concept based on runtime restriction of the operational design domain," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1910–1917, IEEE, 2018.

[25] P. R. Schaumont, *A practical introduction to hardware/software codesign*. Springer Science & Business Media, 2012.

[26] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "HW/SW Co-Design Approach to Optimize Embedded Systems on Reliability," *The International Journal On Advances in Systems and Measurements*, vol. 12, no. 3-4, pp. 158–168, 2019.

[27] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "FITness Assessment-Hardware Algorithm Safety Validation," 2019.

[28] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "Live state-of-health safety monitoring for safety-critical automotive systems," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*, pp. 102–107, IEEE, 2019.

[29] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "Towards synchronous mode of multiple independently controlled mems mirrors," *IFAC-PapersOnLine*, vol. 52, no. 15, pp. 31–36, 2019.

[30] A. Strasser, F. Warmer, P. Stelzer, C. Steger, and N. Druml, "Enabling Fail-Operational Behavior and Degradation for Safety-Critical Automotive 3D Flash LiDAR Systems," in *2020 23nd Euromicro Conference on Digital System Design (DSD)*, IEEE, 2020.

[31] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "Speed-up of mems mirror's transient start-up procedure," in *2019 IEEE Sensors Applications Symposium (SAS)*, pp. 1–5, IEEE, 2019.

[32] A. Strasser, P. Stelzer, C. Steger, and N. Druml, "Enabling live state-of-health monitoring for a safety-critical automotive lidar system," in *2020 IEEE Sensors Applications Symposium (SAS)*, pp. 1–6, IEEE, 2020.

[33] F. Warmer, *Design and Implementation of a Fail-Operational Environmental Perception System*. Master Thesis - Graz University of Technology, 2020.

[34] T. Inagaki and T. B. Sheridan, "A critique of the sae conditional driving automation definition, and analyses of options for improvement," *Cognition, technology & work*, vol. 21, no. 4, pp. 569–578, 2019.

[35] W. Payre, J. Cestac, and P. Delhomme, "Intention to use a fully automated car: Attitudes and a priori acceptability," *Transportation research part F: traffic psychology and behaviour*, vol. 27, pp. 252–263, 2014.

[36] J. Dokic, B. Müller, and G. Meyer, "European roadmap smart systems for automated driving," *European Technology Platform on Smart Systems Integration*, vol. 39, 2015.

[37] C. J. Kahane, "Lives saved by the federal motor vehicle safety standards and other vehicle safety technologies, 1960-2002-passenger cars and light trucks-with a review of 19 fmvss and their effectiveness in reducing fatalities, injuries and crashes," tech. rep., 2004.

[38] E. Liebemann, K. Meder, J. Schuh, and G. Nenninger, "Safety and performance enhancement: The bosch electronic stability control (esp)," tech. rep., SAE Technical Paper, 2004.

[39] M. Kaneyasu, D. Eng, H. Kondoh, N. Hataoka, Y. Nakatsuka, and M. Hoshino, "Semiconductor products for its applications," *Hitachi Review*, vol. 49, no. 3, p. 121, 2000.

[40] "EU-Verordnung zu Assistenzsystemen, [online]." https://www.autobild.de/artikel/eu-verordnung-zu-assistenzsystemen-14873009.html. [09.07.2020].

[41] M. Dikmen and C. M. Burns, "Autonomous driving in the real world: Experiences with tesla autopilot and summon," in *Proceedings of the 8th international conference on automotive user interfaces and interactive vehicular applications*, pp. 225–228, 2016.

[42] R. Faria, L. Brito, K. Baras, and J. Silva, "Smart mobility: A survey," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, pp. 1–8, IEEE, 2017.

[43] I. n. E. ISO, "ISO 21448: Road vehicles - Safety of the intended functionality," *International Standard ISO/FDIS*, vol. 21448, 2019.

[44] M. Kyriakidis, J. C. de Winter, N. Stanton, T. Bellet, B. van Arem, K. Brookhuis, M. H. Martens, K. Bengler, J. Andersson, N. Merat, *et al.*, "A human factors perspective on automated driving," *Theoretical Issues in Ergonomics Science*, vol. 20, no. 3, pp. 223–249, 2019.

[45] D. M. Buede and W. D. Miller, *The engineering design of systems: models and methods*. John Wiley & Sons, 2016.

[46] "IHS Markit: Sales Of Automotive Ecus To Hit $211B In 2030, 5% CAGR, [online]." https://www.greencarcongress.com/2019/05/20190515-ecu.html. [09.07.2020].

[47] "Google Is 2 Billion Lines Of Code—And Its All In One Place, [online]." https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place. [09.07.2020].

[48] "FPGA designers QuickStart Guide, [online]." https://www.mobt3ath.com/uplode/book/book-54117.pdf. [09.07.2020].

[49] B. J. LaMeres, "Introduction: Analog vs. digital," in *Introduction to Logic Circuits & Logic Design with Verilog*, pp. 1–5, Springer, 2017.

[50] D. J. Smith and A. Foreword By-Zamfirescu, *HDL Chip Design: A practical guide for designing, synthesizing and simulating ASICs and FPGAs using VHDL or Verilog*. Doone publications, 1998.

[51] T. IEC, "Iec 62380," *Reliability data handbook–universal model for reliability prediction of electronics components, PCBs and equipment (emerged from UTEC 80-810 or RDF 2000)*, 2004.

[52] W. Torell and V. Avelar, "Mean time between failure: explanation and standards. white paper 78," 2011.

[53] M. Held and K. Fritz, "Comparison and evaluation of newest failure rate prediction models: Fides and riac 217plus," *Microelectronics Reliability*, vol. 49, no. 9-11, pp. 967–971, 2009.

[54] L. Yang, P. A. Agyakwa, and C. M. Johnson, "Physics-of-failure lifetime prediction models for wire bond interconnects in power electronic modules," *IEEE Transactions on Device and Materials Reliability*, vol. 13, no. 1, pp. 9–17, 2013.

[55] J. McLeish, "Physics of failure based simulated aided/guided accelerated life testing," in *2018 Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1–5, 2018.

[56] J. Lan and M. Wu, "Physics of failure based simulation and experimental testing of quad flat no-lead package," in *2019 IEEE 69th Electronic Components and Technology Conference (ECTC)*, pp. 2144–2149, 2019.

[57] G. Caswell, "Using physics of failure to predict system level reliability for avionic electronics," in *2014 IEEE Aerospace Conference*, pp. 1–9, 2014.

[58] K. Ma, H. Wang, and F. Blaabjerg, "New approaches to reliability assessment: Using physics-of-failure for prediction and design in power electronics systems," *IEEE Power Electronics Magazine*, vol. 3, no. 4, pp. 28–41, 2016.

[59] Y. Shao and R. Kang, "A life prediction method for o-ring static seal structure based on physics of failure," in *2014 Prognostics and System Health Management Conference (PHM-2014 Hunan)*, pp. 16–21, 2014.

[60] H. Li, H.-Z. Huang, Y.-F. Li, J. Zhou, and J. Mi, "Physics of failure-based reliability prediction of turbine blades using multi-source information fusion," *Applied Soft Computing*, vol. 72, pp. 624–635, 2018.

[61] S.-P. Zhu, H.-Z. Huang, W. Peng, H.-K. Wang, and S. Mahadevan, "Probabilistic physics of failure-based framework for fatigue life prediction of aircraft gas turbine discs under uncertainty," *Reliability Engineering & System Safety*, vol. 146, pp. 1–12, 2016.

[62] F. He and H. Qi, "A method of estimating network reliability using an artificial neural network," in *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, pp. 57–60, 2008.

[63] A. Gula, C. Ellis, S. Bhattacharya, and L. Fiondella, "Software and system reliability engineering for autonomous systems incorporating machine learning," in *2020 Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1–6, 2020.

[64] B. Song and Z. Peng, "Comparative investigation of bp and rbf neural network on identifying reliability of communication networks," in *2008 International Symposium on Computer Science and Computational Technology*, vol. 2, pp. 376–379, 2008.

[65] R. Yang, L. Zhang, W. Cai, Y. Liu, and H. Huang, "Using neural network to predict reliability of lithography machine," in *2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)*, pp. 308–311, 2013.

[66] Z. Wang, B. Wang, S. Zhou, Y. Sun, X. Wang, and H. Luo, "Effect of high temperature storage and harden accelerated storage test on reliability of flip chip bumps," in

2020 21st International Conference on Electronic Packaging Technology (ICEPT), pp. 1–4, 2020.

[67] J. Yao and H. Li, "Design of reliability qualification test based on acceleration model," in *2015 First International Conference on Reliability Systems Engineering (ICRSE)*, pp. 1–5, 2015.

[68] K. C. C. Cheng, K. Shu-Min Li, A. Y. A. Huang, J. W. Li, L. L. Y. Chen, N. Cheng-Yen Tsai, S. J. Wang, C. S. Lee, L. Chou, P. Y. Y. Liao, H. C. Liang, and J. E. Chen, "Wafer-level test path pattern recognition and test characteristics for test-induced defect diagnosis," in *2020 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 1710–1711, 2020.

[69] J. Park, J. Kim, M. Choe, H. Shim, W. Kim, S. Park, S. Shin, Y. Kim, J. Jeong, H. Shin, H. Lee, and S. Pae, "Scenario-based set-level htol test (ash iii) for product quality and reliability qualifications on high-speed aps," in *2016 IEEE International Reliability Physics Symposium (IRPS)*, pp. 7C–3–1–7C–3–4, 2016.

[70] J. Guo, Z. Li, and M. Pecht, "A bayesian approach for li-ion battery capacity fade modeling and cycles to failure prognostics," *Journal of Power Sources*, vol. 281, pp. 173–184, 2015.

[71] D. Liu, Y. Luo, Y. Peng, X. Peng, and M. Pecht, "Lithium-ion battery remaining useful life estimation based on nonlinear ar model combined with degradation feature," in *Annual conference of the prognostics and health management society*, vol. 3, pp. 1803–1836, 2012.

[72] D. Liu, J. Pang, J. Zhou, Y. Peng, and M. Pecht, "Prognostics for state of health estimation of lithium-ion batteries based on combination gaussian process functional regression," *Microelectronics Reliability*, vol. 53, no. 6, pp. 832–839, 2013.

[73] "Teslas new Smart Summon feature is drawing scrutiny from US traffic safety agency as people use it in crowded parking lots, [online]." https://www.cnbc.com/2019/10/02/nhtsa-looking-into-tesla-accidents-with-smart-summon-feature.html#close. [03.11.2020].

[74] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

[75] M. A. Khan and H. G. Kerkhoff, "An indirect technique for estimating reliability of analog and mixed-signal systems during operational life," in *2013 IEEE 16th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, pp. 159–164, IEEE, 2013.

[76] J. C. Vazquez, V. Champac, A. Ziesemer, R. Reis, I. C. Teixeira, M. B. Santos, and J. P. Teixeira, "Built-in aging monitoring for safety-critical applications," in *2009 15th IEEE International On-Line Testing Symposium*, pp. 9–14, IEEE, 2009.

[77] K. Arabi and B. Kaminska, "Built-in temperature sensors for on-line thermal monitoring of microelectronic structures," in *Proceedings International Conference on Computer Design VLSI in Computers and Processors*, pp. 462–467, IEEE, 1997.

[78] S. Majerus, X. Tang, J. Liang, and S. Mandal, "Embedded silicon odometers for monitoring the aging of high-temperature integrated circuits," in *2017 IEEE National Aerospace and Electronics Conference (NAECON)*, pp. 98–103, IEEE, 2017.

[79] A. Listl, D. Mueller-Gritschneder, F. Kluge, and U. Schlichtmann, "Emulation of an asic power, temperature and aging monitor system for fpga prototyping," in *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, pp. 220–225, IEEE, 2018.

[80] P. Bratek and A. Kos, "Fault diagnosis and fault localisation in integrated circuit by thermal method," in *ICM 2001 Proceedings. The 13th International Conference on Microelectronics.*, pp. 230–233, IEEE, 2001.

[81] M. Beckler and R. Blanton, "On-chip diagnosis for early-life and wear-out failures," in *2012 IEEE International Test Conference*, pp. 1–10, IEEE, 2012.

[82] J. Li and M. Seok, "Robust and in-situ self-testing technique for monitoring device aging effects in pipeline circuits," in *Proceedings of the 51st Annual Design Automation Conference*, pp. 1–6, 2014.

[83] C. Wenzhi, H. Xiaohui, G. Zhendong, and L. Chengrong, "The design of temperature monitoring system for power cable joint," in *2012 IEEE International Conference on Condition Monitoring and Diagnosis*, pp. 671–676, IEEE, 2012.

[84] P. Chauhan, M. Osterman, M. Pecht, and Q. Yu, "Use of temperature as a health monitoring tool for solder interconnect degradation in electronics," in *Proceedings of the IEEE 2012 Prognostics and System Health Management Conference (PHM-2012 Beijing)*, pp. 1–4, IEEE, 2012.

[85] I. Y. Noy, D. Shinar, and W. J. Horrey, "Automated driving: Safety blind spots," *Safety science*, vol. 102, pp. 68–78, 2018.

[86] R. Kianfar, P. Falcone, and J. Fredriksson, "Safety verification of automated driving systems," *IEEE Intelligent Transportation Systems Magazine*, vol. 5, no. 4, pp. 73–86, 2013.

[87] S. international, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," *SAE International,(J3016)*, 2016.

[88] T. Helmer, L. Wang, K. Kompass, and R. Kates, "Safety performance assessment of assisted and automated driving by virtual experiments: Stochastic microscopic traffic simulation as knowledge synthesis," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, pp. 2019–2023, IEEE, 2015.

[89] P. Junietz, W. Wachenfeld, K. Klonecki, and H. Winner, "Evaluation of different approaches to address safety validation of automated driving," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 491–496, IEEE, 2018.

[90] S. Riedmaier, T. Ponn, D. Ludwig, B. Schick, and F. Diermeyer, "Survey on scenario-based safety assessment of automated vehicles," *IEEE Access*, vol. 8, pp. 87456–87477, 2020.

[91] P. Junietz, F. Bonakdar, B. Klamann, and H. Winner, "Criticality metric for the safety validation of automated driving using model predictive trajectory optimization," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 60–65, IEEE, 2018.

[92] J. Yu and F. Luo, "Fallback strategy for level 4+ automated driving system," in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, pp. 156–162, IEEE, 2019.

[93] W. Xue, B. Yang, T. Kaizuka, and K. Nakano, "A fallback approach for an automated vehicle encountering sensor failure in monitoring environment," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1807–1812, IEEE, 2018.

[94] Y. Emzivat, J. Ibanez-Guzman, P. Martinet, and O. H. Roux, "Dynamic driving task fallback for an automated driving system whose ability to monitor the driving environment has been compromised," in *2017 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1841–1847, IEEE, 2017.

[95] A. K. Saberi, J. Vissers, and F. P. Benders, "On the impact of early design decisions on quality attributes of automated driving systems," in *2019 IEEE International Systems Conference (SysCon)*, pp. 1–6, IEEE, 2019.

[96] M. Giammarini, M. Conti, and S. Orcioni, "System-level energy estimation with powersim," in *2011 18th IEEE International Conference on Electronics, Circuits, and Systems*, pp. 723–726, IEEE, 2011.

[97] R. Damaševičius, "Estimation of design characteristics at rtl modeling level using systemc," *Information technology and Control*, vol. 35, no. 2, 2006.

[98] K. L. Man, "Systemc/sup fl: a formalism for hardware/software codesign," in *Proceedings of the 2005 European Conference on Circuit Theory and Design, 2005.*, vol. 1, pp. I–193, IEEE, 2005.

[99] W. Chong, Z. Hong, and L. Zhen, "Hardware/software co-design of embedded image processing system using systemc modeling platform," in *2011 International Conference on Image Analysis and Signal Processing*, pp. 524–528, IEEE, 2011.

[100] P.-J. Ma, Q.-H. Zhao, Y. Fan, M. Liu, and K. Li, "The design and verification of packet processing engine model using systemc," in *2011 International Conference on Electronics, Communications and Control (ICECC)*, pp. 1099–1101, IEEE, 2011.

[101] M. F. Chen, J. Y. Zhou, X. W. Liu, and H. Q. Yin, "Avs video decoder system modeling and design based on systemc," in *2008 2nd International Conference on Anti-counterfeiting, Security and Identification*, pp. 382–386, IEEE, 2008.

[102] T. S. Shatat, B. A. Abdullah, and A. Salem, "Systemc based simulation of autosar software components," in *2015 Tenth International Conference on Computer Engineering & Systems (ICCES)*, pp. 105–110, IEEE, 2015.

[103] H. R. Zarandi and S. G. Miremadi, "Fault tree analysis of embedded systems using systemc," in *Annual Reliability and Maintainability Symposium, 2005. Proceedings.*, pp. 77–81, IEEE, 2005.

[104] S. Reiter, A. Viehl, O. Bringmann, and W. Rosenstiel, "White-box error effect simulation for assisted safety analysis," in *2015 Euromicro Conference on Digital System Design*, pp. 534–538, IEEE, 2015.

[105] H. Kaeslin, *Digital integrated circuit design: from VLSI architectures to CMOS fabrication*. Cambridge University Press, 2008.

[106] "Airbus A350-941 braucht regelmaessig einen Reboot, [online]." www.golem.de/news/ luftfahrt -airbus -a350-941 -braucht -regelmaessig-einen -reboot-1907 -142810.html. [09.08.2020].