Andreas Strasser, BSc

Design of a Product Safety Methodology for the Automotive Industry

Master's Thesis

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Information and Computer Engineering

submitted to

Graz University of Technology

Supervisors

Dipl.-Ing. Dr.techn. Christian Josef Kreiner
Dipl.-Ing. Dr.techn. Gerhard Griessnig (AVL List GmbH)

Institute for Technical Informatics
Graz University of Technology

confidential until 18.01.2020

Graz, January 2018

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 master's thesis.

Graz, 16. January 2018 .....

Kurzfassung

Die Automobilindustrie verwendet heutzutage den ISO 26262 Standard um System Sicherheit zu gewährleisten. Der Standard setzt seinen Fokus bei System Sicherheit auf Funktionale Sicherheit und das hauptsächlich für elektrische und elektronische Systeme. Andere Bereiche wie die Mechanik oder Chemie werden vernachlässigt. Dadurch wird das aktuelle Produktsicherheitsgesetz der Europäischen Union nicht erfüllt. Diese Arbeit beschreibt eine neue Methode für die Automobilindustrie diese Lücke zu füllen und die System Sicherheit für den kompletten Produktlebenszyklus zu gewährleisten. Weiters unterstützt diese Methode die Ingenieure während der Fehler und Risiko Analyse mit Hilfe von Fragenlisten um alle Eventualitäten zu berücksichtigen. Der Prozess befasst sich mit der Recherche nach Informationen bis hin zum Abschluss eines Produkt Sicherheits Berichtes mit der Nachvollziehbarkeit der Implementierungen der Maßnahmen zur Fehlerbehandlung in Bezug auf die Gefährdungssituationen.

Abstract

The automotive industry nowadays uses ISO 26262 to determine system safety. This standard focuses on functional safety and considers just the electrical and electronic systems. Neglecting other technical domains like chemistry and mechanics, this does not cover full system safety as required by product safety legislation. This thesis describes a new methodology for the automotive industry, which considers safety for the whole product lifecycle including safety of use. The methodology supports the engineers during failure and risk analysis using guided questioning to ensure complete analysis. The support covers the whole process from information collection to the finalization of the system safety manual as well as the creation of the final product safety report, including full traceability between the implemented safety measures and related hazardous situations.

Contents

1 Introduction **2**
- 1.1 Motivation . . . 3
- 1.2 Idea . . . 3
- 1.3 Objective target . . . 3
- 1.4 Layout . . . 4

2 Related Work **5**
- 2.1 Electrical powered Vehicles Overview . . . 5
  - 2.1.1 Contingent . . . 5
  - 2.1.2 System Overview . . . 6
  - 2.1.3 Energy Storage - Battery System . . . 7
  - 2.1.4 Risks . . . 8
- 2.2 Traditional Safety Engineering . . . 8
  - 2.2.1 *Failure Modes and Effects Analysis* . . . 8
  - 2.2.2 *Fault Tree Analysis* . . . 9
- 2.3 Scientific View of System Safety . . . 9
  - 2.3.1 General . . . 9
  - 2.3.2 Are traditional safety methods sufficient? . . . 10
  - 2.3.3 Assumptions about traditional System Safety . . . 10
- 2.4 Product Safety in the Automotive Industry . . . 11
  - 2.4.1 ISO 26262 - Road vehicle - functional safety . . . 11
- 2.5 Product Safety in other Fields . . . 12
  - 2.5.1 Product safety laws . . . 12
  - 2.5.2 Consumer Electronics Safety Standard . . . 13
  - 2.5.3 Medical Products Safety Standard . . . 15
  - 2.5.4 Machinery Construction Safety Standards . . . 16
- 2.6 Safety standards and regulations for electrical powered vehicles . . . 18

3 Summary Related Work **19**

4 Product Safety Method for Automotive Vehicles **22**
- 4.1 General Overview . . . 22
- 4.2 Information Collection . . . 26

4.2.1 General Overview . . . 26
4.2.2 Input . . . 27
4.2.3 Activity . . . 27
4.2.4 Output . . . 33
4.2.5 Process Procedure . . . 35
4.3 Information Generation . . . 36
4.3.1 General Overview . . . 36
4.3.2 Input . . . 37
4.3.3 Activity . . . 37
4.3.4 Output . . . 40
4.3.5 Process Procedure . . . 41
4.4 Analysis . . . 42
4.4.1 General Overview . . . 42
4.4.2 Input . . . 43
4.4.3 Activity . . . 43
4.4.4 Output . . . 44
4.4.5 Process Procedure . . . 45
4.5 Prevention . . . 46
4.5.1 General Overview . . . 46
4.5.2 Input . . . 47
4.5.3 Activity . . . 47
4.5.4 Output . . . 50
4.5.5 Process Procedure . . . 51
4.6 Preparation . . . 52
4.6.1 General Overview . . . 52
4.6.2 Input . . . 53
4.6.3 Activity . . . 53
4.6.4 Output . . . 54
4.6.5 Process Procedure . . . 54
4.7 Execution . . . 55
4.7.1 General Overview . . . 55
4.7.2 Input . . . 56
4.7.3 Activity . . . 56
4.7.4 Output . . . 59
4.7.5 Process Procedure . . . 60
4.8 Verification . . . 61
4.8.1 General Overview . . . 61
4.8.2 Activity . . . 62
4.8.3 Output . . . 64
4.8.4 Process Procedure . . . 64
4.9 Finalization . . . 65
4.9.1 General Overview . . . 65
4.9.2 Input . . . 66

4.9.3 Activity . . . 66
4.9.4 Output . . . 69
4.9.5 Process Procedure . . . 69

5 Practical Part & Results 70
5.1 Information Collection . . . 70
5.1.1 Define *Items* . . . 70
5.1.2 Set *Product Phases* . . . 71
5.1.3 Identify *Harm Sources* and Link *Harm Sources* with *Product Phases* . . . 72
5.1.4 Identify *Roles* . . . 72
5.1.5 Identify *Actions* . . . 72
5.2 Information Generation . . . 73
5.2.1 Generate *Hazardous Situation List* . . . 73
5.2.2 Evaluate *Hazardous Situation List* . . . 74
5.2.3 Generalize *Hazardous Situation List* . . . 75
5.3 Analysis . . . 75
5.3.1 Create FMEA and Link Hazardous Situations . . . 78
5.4 Prevention . . . 78
5.5 Preparation . . . 80
5.5.1 Pivot Analysis . . . 81
5.6 Execution and Verification . . . 86
5.7 Finalization . . . 87
5.8 Testing Parts of the Method . . . 87
5.8.1 Support the Item Definition . . . 88
5.8.2 Analysis . . . 90

6 Limitations and Future Work 96

7 Conclusion 98

Bibliography 99

A eFMEA Abstract 103

Glossary 106

Acronyms 109

List of Figures

2.1 Electrical battery powered cars by country (Source: Global EV Outlook 2017[Age17]). 6
2.2 System architecture of a common battery system in an electrical automotive vehicle (Source: Automotive Battery Technology[MLW14]). 7

3.1 Table overview of the car accidents in Germany from 1991 to 2016 (Source: Verkehrsunfälle 2016[Bun17]). 20
3.2 Graphical overview of the car accidents in Germany from 1991 to 2016 (Source: Verkehrsunfälle 2016[Bun17]). 20

4.1 General overview of the system safety process with all eight parts. . . 23
4.2 General overview of the *Information Collection* phase. 26
4.3 *Item* definition step of the *Information Collection* phase. 28
4.4 Example about the *Item* definition. 29
4.5 *Product Phases* selection step of the *Information Collection* phase. . . 29
4.6 Example about selecting product phases for specific items 30
4.7 Identification of the different *Harm Sources* in the *Information Collection* phase. 31
4.8 Example about selecting harm sources for each item 32
4.9 Identification of the different *Roles* in the *Information Collection* phase. 32
4.10 Basic example for a standard list about common *Roles* in the automotive domain. 32
4.11 Identification of the different *Actions* in the *Information Collection* phase. 33
4.12 Basic example for an *Action* list with different *Roles* in the automotive domain. 33
4.13 *BPMN* Process Procedure Overview of the *Information Collection* phase. 35
4.14 General overview of the *Information Generation* phase. 36
4.15 Generation of the *Hazardous Situation List* in the *Information Generation* phase. 38
4.16 Example of a generation of the *Hazardous Situation List* in the *Information Generation* phase. 38

4.17 Example of a generation a question of the *Hazardous Situation List* in the *Information Generation* phase. 39
4.18 Evaluation of the *Hazardous Situation List* in the *Information Generation* phase. 39
4.19 Generalizing of the *Hazardous Situation List* in the *Information Generation* phase. 40
4.20 *BPMN* Process Procedure Overview of the *Information Generation* phase. 41
4.21 General overview of the *Analysis* phase. 42
4.22 Creation of the *Failure Modes and Effects Analysis (FMEA)* in the *Analysis* phase. 43
4.23 Linking between the *Hazardous Situations* and the *FMEA* in the *Analysis* phase. 44
4.24 *BPMN* Process Procedure Overview of the *Analysis* phase. 45
4.25 General overview of the *Prevention* phase. 46
4.26 Assignment of the *Technical Domain* in the *Prevention* phase. 47
4.27 Assignment of the *Safety Domain* in the *Prevention* phase. 48
4.28 Assignment of the *Protection Domain* in the *Prevention* phase. 48
4.29 Assignment of the *Protection Type* in the *Prevention* phase. 49
4.30 Identification of the *Protection Measure* in the *Prevention* phase. . . . 50
4.31 *BPMN* Process Procedure Overview of the *Prevention* phase. 51
4.32 General overview of the *Preparation* phase. 52
4.33 Separation of the *Work Packages* in the *Preparation* phase. 53
4.34 *BPMN* Process Procedure Overview of the *Preparation* phase. 54
4.35 General overview of the *Execution* phase. 55
4.36 Check Standards & Guidelines in the *Execution* phase. 56
4.37 Check dependencies to other *Technical Domain* in the *Execution* phase. 57
4.38 Implement *Protection Measure* in the *Execution* phase. 57
4.39 Justify the implemented *Protection Measure* in the *Execution* phase. . 58
4.40 Develop a *Test Method* for the implemented *Protection Measure* in the *Execution* phase. 59
4.41 Check impacts to other *Work Package* for the implemented *Protection Measure* in the *Execution* phase. 59
4.42 *BPMN* Process Procedure Overview of the *Execution* phase. 60
4.43 General overview of the *Verification* phase. 61
4.44 Perform the *Test Method* for the implemented *Protection Measure* in the *Verification* phase. 62
4.45 Document the results of the *Test Method* for the implemented *Protection Measure* in the *Verification* phase. 63
4.46 Refuse failed *Work Packages* in the *Verification* phase. 63
4.47 *BPMN* Process Procedure Overview of the *Verification* phase. 64
4.48 General overview of the *Finalization* phase. 65
4.49 Create manuals in the *Finalization* phase. 67

4.50 Create *Product Safety Report* in the *Finalization* phase. 68
4.51 Archive the *Product Safety Report* in the *Finalization* phase. 68
4.52 *BPMN* Process Procedure Overview of the *Finalization* phase. 69

5.1 *Item* definition of the basic HV battery system example. 71
5.2 *Product Phase* definition of the basic HV battery system example. . . 71
5.3 *Harm Source* definition of the basic HV battery system example. . . . 72
5.4 *Role* identification of the basic HV battery system example. 72
5.5 *Action* identification of the basic HV battery system example. 73
5.6 *Hazardous Situation List* generation of the basic HV battery system example. 74
5.7 *Hazardous Situation List* evaluation of the basic HV battery system example. 74
5.8 *Hazardous Situation List* separated by different *Harm Sources* to support the engineers. 76
5.9 *Hazardous Situation List* separated by different *Harm Sources* to support the engineers in question form. 77
5.10 Short excerpt of the linking list of *Hazardous Situation List* and *FMEA*. 78
5.11 Short excerpt of the domain assigning of the *EFMEA*. 79
5.12 Example for a single *Work Package* as result of the *Preparation* phase. 80
5.13 Example #1 of a pivot table derived from the analysis. 81
5.14 Example #2 of a pivot table derived from the analysis. 82
5.15 Example #3 of a pivot table derived from the analysis. 83
5.16 Example #4 of a pivot table derived from the analysis. 84
5.17 Example #5 of a pivot table derived from the analysis. 85
5.18 Example #6 of a pivot table derived from the analysis. 86
5.19 General overview of the extracted basic data of the item definition. . 89
5.20 Plausibility of Thermal *Hazardous Situations*. 90
5.21 Plausibility of Thermal *Hazardous Situations* in percent. 91
5.22 Distribution between *Failures* and *Hazardous Situations*. 92
5.23 Distribution between number of detection and *Failures*. 92
5.24 Distribution between number of detection and *Failures* in percent. . . 93
5.25 Overview Hazardous *Product Phases* as radar chart. 93
5.26 Overview Hazardous *Product Phases* in percent. 94
5.27 Overview Exposed *Roles* as radar chart. 94
5.28 Overview Exposed *Roles* in percent. 95

A.1 Abstract of the eFMEA, this does not cover all typical *FMEA* elements and are reduced to the most important that are necessary for this thesis. (Part 1) 104
A.2 Abstract of the eFMEA, this does not cover all typical *FMEA* elements and are reduced to the most important that are necessary for this thesis. (Part 2) 105

Chapter 1

Introduction

One of the first cars were published 100 years ago. Since then a lot has changed like design, development, manufacturing, reliability, but not everything. For all engineers the system had been complex and they had to struggle with complexity.

Nancy Leveson writes in her book called 'Engineering a safer world: Systems thinking applied to safety' that over the time a lot of methods and best practices had been introduced to the development process of an automotive car to handle complexity. Complex systems are hard to understand and to control and that they can arise accidents with lives lost. This is unacceptable and therefore the first approach in safety was done by C.O. Miller, Jerome Lederer and Willie Hammer in the 1950s. It was initiated to handle the increased level of complexity with aerospace systems. Over the time this knowledge disappeared because of engineering methods focusing on reliability engineering[Lev11].

In the engineering standard ISO 26262 that is used in the automotive domain is recognizable that currently the automotive industry is focusing on this kind of reliability engineering called functional safety[fSCI11].

Nancy Leveson mentions a false conclusion about reliability and safety in her book[Lev11]:

> *"Safety is increased by increasing system or component reliability. If components or systems do not fail, then accidents will not occur."*[Lev11]

Nancy Leveson is writing that this is one of the general assumptions of safety which is not true. There are possibilities that a reliable system is not safe and the other way around. Accidents with complex systems often base on the interaction between components, even if all the components behave correctly how they were designed. Leveson is describing a famous example for this kind of misbehave is the accident with the mars polar lander. Sometimes there even occur a conflict between the safety and the reliability. Safety is not that easy to achieve in a proper way. It is

necessary to think about beyond the edge of functions.[Lev11]

In the European Union the product safety is covered by the guideline 2001/95/EG[otEC01]. In Austria this guideline was established 2004 with the law called Produktsicherheitsgesetz. This law handles the launch and production of products over the whole product lifecycle. It is not allowed to launch products which are not safe and can cause massive injury. To achieve proper safety, in the context of the law, it is necessary to observe the legal laws, engineer standards and state of the technology and science[pro04].

1.1 Motivation

To consider the fact of the legal aspect it is not advisable to lower the safety aspects to functional safety. This shortcut is not covering the actual legal laws. Therefore it is necessary to introduce a method, to handle the remaining requirements, to fulfill the law.

1.2 Idea

The idea of this thesis is about developing a product safety methodology that supports the engineers during the development phase to identify hazardous risks that can harm human beings. Furthermore this methodology should consider all different phases of the product lifecycle with all different operators. In addition the methodology should consider different kind of system safety domains.

1.3 Objective target

This thesis should fulfill the following targets:

- Design of a Product Safety Methodology that considers
  - Product Lifecycle
  - Various Operators
  - Various System Safety Domains
- Support Engineers during Development
- No Disturbance to the ISO 26262 Processes
- Implementing Product Safety Methodology in FSM Tool

1.4 Layout

This thesis is divided into six different sections:

- **Chapter 1** can be found on page 2 and is about the introduction in the topic of the thesis and about the objectives that should be fulfilled by this thesis.
- **Chapter 2** can be found on page 5 and is about the product safety methods and processes from the automotive domain and other industries. Furthermore this chapter provides an overview about the legal situation in the European Union.
- **Chapter 3** can be found on page 19 and is a summary about **Chapter 2** and describes an idea how to fulfill the requirements and what must to be done.
- **Chapter 4** can be found on page 22 and is about the methodology. It gives a theoretical overview about the method.
- **Chapter 5** can be found on page 70 and is a practical example of the introduced methodology and gives an overview about the method and the procedure.
- **Chapter 6** can be found on page 96 is about the limitations of the methodology and the future work that is necessary to evolve the method.
- **Chapter 7** can be found on page 98 is the last chapter and is a conclusion about this thesis.

Chapter 2

Related Work

2.1 Electrical powered Vehicles Overview

Electrical powered vehicles have already started their triumphal procession. Braess *et al.* is writing that this kind of vehicles are powered by an electrical motor that takes the energy from a battery system. There are two different kind of electrical powered vehicles[BS13]:

- *Battery-electric Vehicles* (*BEV*)
- *Hybrid electric Vehicles* (*HEV*)
  - Micro Hybrid
  - Mild Hybrid
  - Full Hybrid
  - Plug-In Hybrid

2.1.1 Contingent

As clearly depicted in the diagram 2.1 the amount of electrical battery powered cars increased significantly since 2005[Age17].

Table 5 • Battery electric cars, stock by country, 2005-16 (thousands)

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Canada							0.22	0.84	2.48	5.31	9.69	14.91
China					0.48	1.57	6.32	15.96	30.57	79.48	226.19	483.19
France	0.01	0.01	0.01	0.01	0.12	0.30	2.93	8.60	17.38	27.94	45.21	66.97
Germany	0.02	0.02	0.02	0.09	0.10	0.25	1.65	3.86	9.18	17.52	29.60	40.92
India				0.37	0.53	0.88	1.33	2.76	2.95	3.35	4.35	4.80
Japan					1.08	3.52	16.13	29.60	44.35	60.46	70.93	86.39
Korea						0.06	0.34	0.85	1.45	2.76	5.67	10.77
Netherlands				0.01	0.15	0.27	1.12	1.91	4.16	6.83	9.37	13.11
Norway			0.01	0.26	0.40	3.35	5.38	9.55	19.68	41.80	72.04	98.88
Sweden							0.18	0.45	0.88	2.12	5.08	8.03
United Kingdom	0.22	0.55	1.00	1.22	1.40	1.65	2.87	4.57	7.25	14.06	20.95	31.46
United States	1.12	1.12	1.12	2.58	2.58	3.77	13.52	28.17	75.86	139.28	210.33	297.06
Others					0.64	0.80	3.17	5.83	10.60	19.43	36.20	52.41
Total	1.37	1.69	2.15	4.54	7.47	16.42	55.16	112.94	226.78	420.33	745.61	1 208.90

Figure 2.1: Electrical battery powered cars by country (Source: Global EV Outlook 2017[Age17]).

2.1.2 System Overview

Braess *et al.* writes that *HEV* are not all able to drive electrically. Full Hybrid and Plug-In Hybrid are able to drive certain distances with a battery and of course the *BEV*. This systems behave different than traditional powertrains. The electrical powertrain systems need additional systems to fulfill the functional and the system safety requirements these systems are *BEV*[BS13]:

- Electric Machine
- Energy Storage
- Power Electronics
- High Voltage Cables
- Clutch
- Cooling Systems
- Charging Socket (Plug-In/Full Hybrid)
- Charger (Plug-In/Full Hybrid)
- All Components electrified (Plug-In/Full Hybrid)

This overview makes it obvious that the electrification of the powertrain effects a lot of systems and change the vehicle essential. One of the most important parts of an electrical vehicle is the energy storage this is usually a battery system.

2.1.3 Energy Storage - Battery System

Martin *et al.* describes a system architecture of a common battery system in the electrical vehicle. Nowadays the automotive domain is using lithium-ion battery systems. This systems contains the following modules[MLW14]:

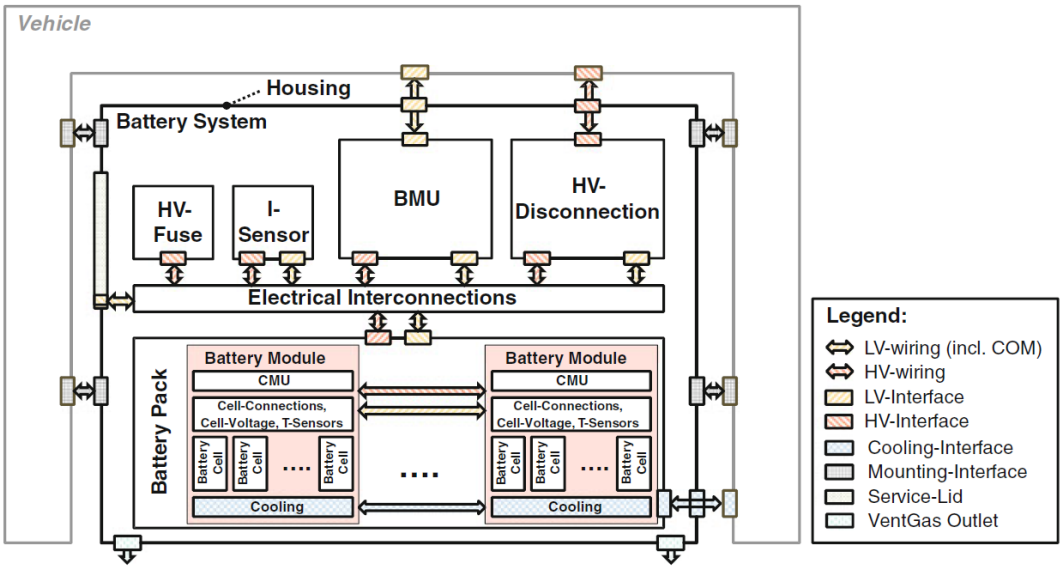


Figure 2.2: System architecture of a common battery system in an electrical automotive vehicle (Source: Automotive Battery Technology[MLW14]).

- *Battery Management System (BMS)*
- *HV* Disconnection
- *HV* Fuse
- I-Sensor
- Electrical Interconnections
- Battery Cell Pack
  - Battery Cell Module
  - Battery Cell Module Interconnection
- Housing and external interfaces

These systems are needed to ensure a safe application with *HV* battery systems. Martin *et al.* writes that these systems are interdisciplinary and to ensure an acceptable risk level it is necessary to involve different technological domains[MLW14].

2.1.4 Risks

Martin *et al.* have worked on an risk assessment and identified different technological problems that can be electrical, mechanical, thermal and chemical[MLW14]. Korthauer describes in his book that these battery system contains Lithium-Ion battery modules with highly hazardous chemicals. Furthermore he describes in his book an overview about critical aspects and risks of these systems. A short overview about different domains are[Kor13]:

- Electrical
  - Overcharging
  - Electrical shock
- Chemical
  - Exhausting toxic gases
  - Electrolyte decomposition
- Mechanical
  - Corrosion
  - Insufficient Stiffness

2.2 Traditional Safety Engineering

Georgi Popov *et al.* describe that nowadays various technological engineering fields (NASA, nuclear industry, automotive industry, semiconductor industry, food industry) are using the *Failure Modes and Effects Analysis* (*FMEA*) method to identify possible risks and failures[PLH16].

2.2.1 *Failure Modes and Effects Analysis*

The *FMEA* was one of the first introduced methods. It has been published 1949 in the MIL-P-1629 document by the US Department of Defense and has been adopted by different industries[PLH16].

The *FMEA* identifies how a system can fail and the effects of these failures and is a bottom-up approach.[PLH16]. The *FMEA* can be separated into different types of *FMEA*[PLH16]:

- Design-FMEA
- System-FMEA
- Process-FMEA
- Service-FMEA

Every *FMEA* has its own focus on different product views.

2.2.2 *Fault Tree Analysis*

Clif Ericson describe in his paper that the *Fault Tree Analysis* (*FTA*) was developed 1961 by H.A. Watson of Bell Labs for the United States Air Force. Boeing discovered the method and used it for safety evaluation 1966 on the design. Nowadays this method has been established in different engineering fields. The *FTA* is a method to analyze failure paths of systems and is a top-down approach[Eri99].
These two methods completes the overall safety view. The *Fault Tree Analysis* (*FTA*) is starting from a top level failure and identifies all relevant causes in an top-down approach. The *FMEA* starts from the cause and identifies which effects and failures can occur in a bottom-up approach.

2.3 Scientific View of System Safety

This part is primary about the work of system safety expert Nancy Leveson. Leveson does research in this field since decades. Her ideas and approach is widely accepted and reused. The next chapters summarize her ideas and thoughts of the system safety fibula 'Engineering a safer world: Systems thinking applied to safety'[Lev11].

2.3.1 General

Leveson describes that the first steps of system safety was done by aerospace engineering pioneers in the 1950s. Aerospace systems have always been highly complex systems and safety was one important focus. In other domains this concepts and ideas have been replaced with more common engineering practices that focusing on reliability. Nowadays the technological world has changed and small embedded devices become more and more complex like aerospace systems. But the way of safe engineering has not changed over the past years. They are still using basic techniques like the *FTA* or the *FMEA*. These techniques have been established in a time where systems existed of almost analog parts. Nowadays this parts have been widely replaced by digital systems, these systems behave differently[Lev11].

2.3.2 Are traditional safety methods sufficient?

Leveson describes that traditional systems have been sufficient for simple analog systems. The systems have changed over the time and nowadays they became more complex. Leveson thinks the the traditional methods are out of scope because of the following reasons[Lev11]:

- Fast pace of technological change
- Reduced ability to learn from experience
- Changing nature of accidents
- New types of hazards
- Increasing complexity and coupling
- Decreasing tolerance for single accidents
- Difficulty in selecting priorities and making tradeoffs
- More complex relationships between humans and automation
- Changing regulatory and public views of safety

2.3.3 Assumptions about traditional System Safety

Leveson asserts that in the system safety domain there are assumptions that are established in the minds of engineers[Lev11]. Nancy Leveson analyze this assumptions and adjust them with new assumptions. This section describes the most important for this thesis and her recommendations.

Confusing Safety with Reliability

Leveson announces the assumption:

> *"Safety is increased by increasing system or component reliability. If components or systems do not fail, then accidents will not occur."*[Lev11]

Leveson writes that this assumption is false and reliability does not necessarily affect system safety and vice-versa sometimes they even conflict[Lev11]. In the past there have been enough examples with the following situations[Lev11]:

- Reliable but Unsafe
- Safe but Unreliable
- Conflicts between Safety and Reliability

Leveson announces a new Assumption:

> *"High reliability is neither necessary nor sufficient for safety."*[Lev11]

Leveson describes that systems engineering with focus on safety does not stop at the component level. For system safety the system needs to be analyzed as a whole[Lev11].

The Role of Operators in Accidents

Leveson announces the assumption:

> *"Most accidents are caused by operator error. Rewarding safe behavior and punishing unsafe behavior will eliminate or reduce accidents significantly."*[Lev11]

Leveson describes that if some accident happens usually the operators are held responsible. The problem is that the guidelines are often written based on the model but not on the real world system. If an accident can be avoided by breaking the rules than everything is fine and if not the operator gets in deep trouble. Therefore it is necessary to think about the operator from the beginning of the development process[Lev11].

Leveson announces a new Assumption:

> *"Operator behavior is a product of the environment in which it occurs. To reduce operator " error " we must change the environment in which the operator works."*[Lev11]

2.4 Product Safety in the Automotive Industry

2.4.1 ISO 26262 - Road vehicle - functional safety

In the automotive industry there is already an engineering standard which covers the safety of automotive systems. This standard is called ISO 26262: 'Road vehicles - functional safety'. The standard is focusing on electrical components and the related failures to this systems. The standard does not cover mechanical, chemical or thermal safety[fSCI11].

2.5 Product Safety in other Fields

Product safety in general is not a blank page. Science already developed ideas and methods to handle and achieve safety in different fields. There are even industry standards and product safety laws in the European Union active. This chapter describes product safety in different point of views and summarize the current achievements in this important field.

2.5.1 Product safety laws

The initial importance for product safety started in the beginning of the 1990s. Lach and Polly describe in their book about product safety that the European union released in June 1992 a guideline about product safety. Nowadays all members of the European union already have established this guideline in their national law[LP15]. In Austria this is covered by the Produktsicherheitsgesetz established in 2004[pro04].

Product safety law in Austria 'Produktsicherheitsgesetz'

In this subsection the law of the product safety in Austria will be reviewed. This section will cover all important parts in consideration of this master thesis, there are many more rules and instructions which are not covered here.

What does the law cover
The Produktsicherheitsgesetz is describing in §1 that the law covers the safety requirements for products, to protect humans against health- and life threatening, behavior. The producer and distributor are responsible for providing evidence[pro04].

What is a product
The law is describing in §3 a product is a moving thing. A product is also a part of another moving or non-moving think[pro04].

What is a producer
The law describes that a producer is someone who has his headquarter in the European Union and launches at least one product[pro04].

How is a product safe
The Produktsicherheitsgesetz defines in §4 that a safe product will not lead to an accident as long as it is used in a normal way, basically for the whole product lifecycle[pro04].

How to determine if the product is safe in general
The Produktsicherheitsgesetz defines in §5 that a product is assumed to be safe as long as it meets following safety requirements[pro04]:

- No obligatory territorial standard specification
- Territorial standard specifications
- Guidelines from the European union about product safety
- Code of conduct in the specific industry
- State-of-the-art of science and technology
- Safety which are expected from the customers
- References from the national product safety board of advisers

Responsibilities of the producer/distributor
§6 of the Produktsicherheitsgesetz declares that both the producer and distributor is responsible for unsafe products[pro04].

How to prove that a product is safe
In §6 of the Produktsicherheitsgesetz is declared that every producer and distributor are responsible for providing evidence for product safety on request[pro04].

2.5.2 Consumer Electronics Safety Standard

This part covers the current product safety standard for electronic equipment in the audio/video- and telecommunication technology. This section describes the standard from third party paper. The reason is because there was no possibility to get the original standard.

IEC 62368

Schulz describes in his paper that the standard is covering safety with the *Hazard Based Safety Engineering* (*HSBE*) concept. This concept helps to identify the most severe risks. There is no possibility or need to decrease the risk to zero. The ambition is to achieve a safety level which is general accepted[Sch09].

Prevent hazards

Schulz describes that the safety concept is based on a model with three steps. This model illustrates the injury through energy transfer between an energy source and a body part. To prevent this energy transfer a *Safeguard* is introduced in the system to prevent the transfer procedure. Avoiding the energy transfer avoids the possibility of an injury. This kind of *Safeguard* can be implemented in different domains[Sch09].

Hazardous energy sources

Emery describes that the standard is covering six different hazardous domains which can cause injury[Eme15]:

- Electrical shock
- Electrical caused fire
- Chemical
- Mechanical
- Thermal
- Radiation

Safeguards

Schulz describes that the standard specifies *Safeguards* to prevent energy transfer causing injuries. This *Safeguards* can be implemented in different domains and views[Sch09]:

- Basic *Safeguard*
  Schulz describes that this *Safeguard* covers safety at the base of operation (Isolation)[Sch09].
- Supplementary *Safeguard*
  Schulz describes that this *Safeguard* covers single point failures[Sch09].
- Reinforced *Safeguard*
  Schulz describes this *Safeguard* as a combination between a basic- and a supplementary *Safeguard*[Sch09].

Schulz describes that the right *Safeguard* depends on the operation and the operator. The most important part about operator is his knowledge and education therefore it is necessary to consider this in the *Safeguard* decision[Sch09]. In the paper of Emery are different types of *Safeguards* described[Eme15]:

- Equipment *Safeguard*
  Emery describes that this *Safeguard* keeps the operator safe without any intervention[Eme15].
- Installation *Safeguard*
  Emery describes that this *Safeguard* will be installed during the startup phase and will only be operational afterwards[Eme15].
- Personal *Safeguard*
  Emery describes that this *Safeguard* will be worn by the operator[Eme15].
- Instructional *Safeguard*
  Emery describes that this *Safeguard* will provide information to the operator about possible hazards[Eme15].

2.5.3 Medical Products Safety Standard

The medical product industry is using the international standard ISO 14971 as safety standard[Heg11]. This section describes the standard from a third party paper. The reason is because there was no possibility to get the original standard.

ISO 14971

Hedge describes in his paper that the standard contains a process about risk identification of medical products. The identified risks are rated and classified and the engineers gets supported by a question list. The whole process can be exemplified by the following steps[Heg11]:

- Risk Analysis
- Risk Evaluation
- Risk Control
- *Risk Management Report*
- Post-Production Information

Risk Analysis

The first steps are identical and already known from other domains. It starts with the identification of foreseeable uses and misuses. Furthermore the standard demands the identification and definition of the product limits. For this purpose

the standard is offering an annex with standard questions to identify all potential hazards. Furthermore the standard recommends to create a list with possible hazards[Heg11].

Risk Control
This step is about the mitigation of the risk. Therefore the standard contains the categorization of measure implementations concerning three different types[Heg11]:

- Inherent Safety by Design
- Protective Measures in the Device or in the Manufacturing Process
- Information for Safety

The implemented measures are documented in the *Risk Management File* and offer an overview about the measures. Furthermore the proof of effectiveness of the measures are also documented in this file. If there are any risks left after the measure implementation, the remaining risk needs to be documented in the *Risk Management File*[Heg11].

Risk Management Report
The standard introduces a second document called *Risk Management Report* that summarizes the results of the risk analysis and provides traceability between the hazards and the implementation of the measures[Heg11].

2.5.4 Machinery Construction Safety Standards

The machinery construction domain covers safety with the engineering standard ISO 12100. This standard supports constructing engineers with methods and guidelines, to consider system safety[DDIfN11]. The method can be divided in two steps, applied to the whole product lifecycle[DDIfN11]:

- Risk Assessment
  - Information for Risk Assessment
  - Determination of limits of machinery
  - Hazard identification
  - Risk estimation
  - Risk evaluation
- Risk reduction
  - Designer

- User

Risk Assessment

The Risk Assessment is very similar to other domains. The standard provides the following information about the collection of safety related information to evaluate the risk[DDIfN11]:

- Information about the machine
- Guidelines and standards
- Information about previous and similar machines
- Ergonomical principles

Another important step is about finding the machine limitations. To consider the following points[DDIfN11]:

- Use Limits
- Space Limits
- Time Limits
- Other Limits

Protective Measures Implementation

The standard offers three ways to mitigate a risk for the designer[DDIfN11]:

- Inherently Safe Design Measures
- Complementary Protective Measures
- Information for Use

For the user the standard offers two ways to mitigate the risk[DDIfN11]:

- Organizational Measures
- Personal Measures

The standard provides the engineer with an appendix comprised of examples and guidelines which kinds of hazardous events could occur. The standard considers ten different hazard types i.e. mechanical or electrical hazards. Furthermore it describes a list of expected product phases with related operational actions[DDIfN11].

2.6 Safety standards and regulations for electrical powered vehicles

In the automotive industry there are already a vast number of standards and regulations which focus on safety in electrical and hybrid powered vehicles. The standards offer guidelines and best practices for the development and testing phases. There are a lot of standards for different markets and regions for electrical cars and components. This standards include:

- ISO 6469 - Electrically propelled road vehicles - Safety specifications

  Part 1: On-board rechargeable energy storage system (RE SS)

  Part 2: Vehicle operational safety means and protection against failures

  Part 3: Protection of persons against electric shock

  Part 4: Post crash electrical safety

- ISO 20653 - Road vehicles - Degrees of protection (IP code) - Protection of electrical equipment against foreign objects, water and access
- ISO 12405 - Electrically propelled road vehicles - Test specification for lithium-ion traction battery packs and systems

  Part 1: High-power applications

  Part 2: High-energy applications

  Part 3: Safety performance requirements

- IEC 62660 - Secondary lithium-ion cells for the propulsion of electric road vehicles

  Part 1: Performance testing

  Part 2: Reliability and abuse testing

  Part 3: Safety requirements

- VW 80303 - Elektrische Eigenschaften und elektrische Sicherheit von Hochvolt-Komponenten in Kraftfahrzeugen
- ECE R10 - Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility
- ECE R100 - Uniform provisions concerning the approval of vehicles with regard to specific requirements for the electric power train
- ECE R121 - Uniform provisions concerning the approval of vehicles with regard to the location and identification of hand controls, tell-tales and indicators

Chapter 3

Summary Related Work

Chapter 2 shows undeniably that system safety is not an unworked domain. There are already many guidelines, engineering standards, books and scientific papers in this domain[Lev11, fSCI11, Heg11, PLH16, Eri99, DDIfN11]. To support the engineers in the system safety process there are different methods. They can be categorized in two major categories:

- *Traditional System Safety Methods (TSSM)*
  This methods are widely known by almost any engineer. Engineers usually learn them in university or during their work they include the *FMEA* and *FTA* among others.
- *Specific System Safety Methods (SSSM)*
  This methods are used in specific domains and are used additionally or extend the *TSSM*.

SSSM are needed because *TSSM* can not fit the requirements of specific systems. The reasons are mentioned in section 2.3.2 on page 10 and are understandable. System safety has been pushed of to the operators responsibility[Lev11]. Nowadays this point of view has changed and governments introduced laws that force companies to engineer safe systems, as mentioned in section 2.5.1 on page 12[Lev11, otEC01, pro04, LP15]. Therefore it is necessary for every producer or distributor to prove that the systems they launch on European markets fulfill a certain safety standard. The law is very strict but unspecific at once, as mentioned in section 2.5.1 on page 13[pro04]. Mostly the producer or distributor has to determine what is necessary to make a safe product.

The automotive industry has introduced a general standard for system safety as mentioned in section 2.4.1 on page 11, but this standard is not enough to fulfill the safety level required by new regulations. The reason is the absence of other technological domains as mentioned in section 2.4.1 on page 11. Therefore the industry

has introduced many standards concerning system safety for specific vehicle components, as mentioned in section 2.6 on page 18, that cover more than the electrical domain and support the engineers. Therefore the current system safety process in the automotive domain and the required product safety level by the government do not match. It is necessary to introduce something new or extend the current processes to a holistic approach of product safety. This has already been tried in the automotive domain with the STPA method of Leveson[Mal15]. This is not useful because introducing something new introduces new problems and failures and it is questionable if it is useful to introduce new processes.

The German Federal Statistical Office releases every year statistics about car accidents including the separation of different causes.

	1991	1995	2000	2005	2010	2012	2013	2014	2015	2016
Technical issues (AVC)	6213	5486	5015	4402	3918	3726	3559	3624	3636	3586
Misbehavior (car)	378373	374181	342684	287173	242307	250895	244151	248712	253504	255391

Figure 3.1: Table overview of the car accidents in Germany from 1991 to 2016 (Source: Verkehrsunfälle 2016[Bun17]).

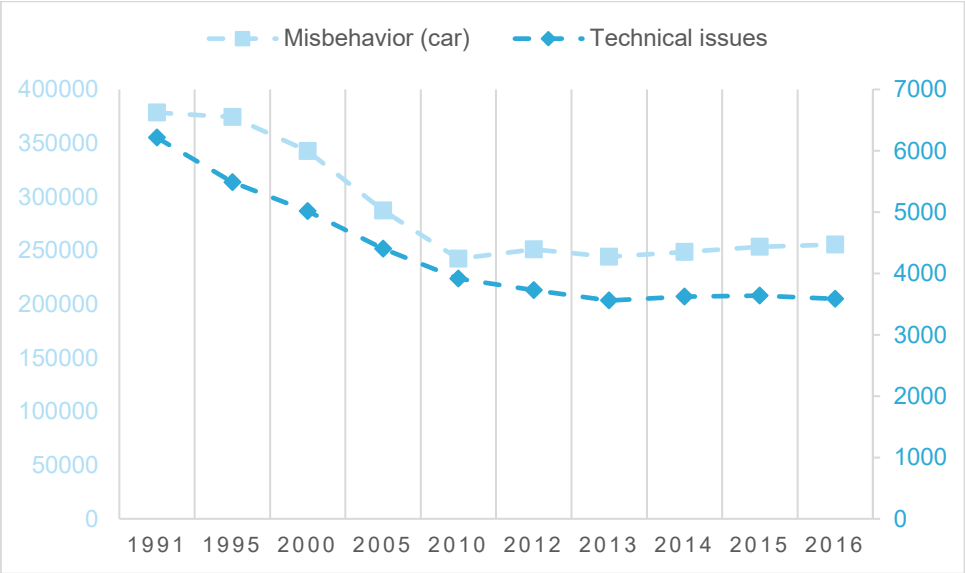


Figure 3.2: Graphical overview of the car accidents in Germany from 1991 to 2016 (Source: Verkehrsunfälle 2016[Bun17]).

In Figure 3.2 it is clearly evident that most accidents are caused by personal misbehavior and that the technical causes are much smaller and decrease annually. Therefore it is not useful to introduce new processes. The current system safety process from the automotive sector covers the technical part good enough in consideration

of the acceptable level of risk. The biggest part are the personal misbehavior and it is questionable if the persons are all acting careless. It could be that some accidents are caused by misunderstandings between the operator and the vehicle[Lev11]. Therefore this has to be considered in the system safety process and the current ISO 26262 process needs to be extended with at least the following aspects:

- Include additional technological domains
- Include the driver and his behavior in the risk analysis

Chapter 4

Product Safety Method for Automotive Vehicles

Product safety is important and as mentioned in section 2.5.1 on page 12 it is obligatory for every producer and distributor that are launching new products in Austria or in the European Union. Automotive vehicles are dangerous, complex, huge systems. This can be realized if you take an insight at the provided standards from different standardization organizations. An excerpt of these standards can be found in section 2.6 on page 18. Leveson describes that complex systems also can have a big impact on individual persons or even an impact on person groups. Our society does not tolerate deadly accidents as mentioned in Section 2.3.2 on Page 10[Lev11]. Therefore it is necessary to rethink the current methods and adapt them to increase the safety level considering all different phases of a product. The next sections describe a new method for product safety in the automotive domain that considers the whole product lifecycle of an automotive vehicle. Furthermore the method considers the typical *Technical Domains* that are present in all modern automotive vehicles as mentioned in Section 2.1 on Page 5.

4.1 General Overview

In general every product is specifically designed for certain specifications depending on the target markets. This specification probably does not meet the requirements of similar markets, as inn most cases the legal laws and the national engineering standards are too different. Therefore a product could be considered safe in the European Union but unsafe in the United States simultaneously and vice versa. Furthermore the automotive domain is connected world wide and parts are shipped around the globe. This leads to the fact that parts are exposed to different environmental conditions. For product safety this and many other facts have to be consid-

ered. Introducing something new must offer the possibility to collect all necessary information at the beginning and focus on the target markets with the corresponding environmental and social conditions. Therefore the new product safety method is divided into eight main parts that focus on these aspects starting with the collection of information and ends with the summarizing of all identified information as well as providing a step-by-step guideline to support engineers during development of a safe product.

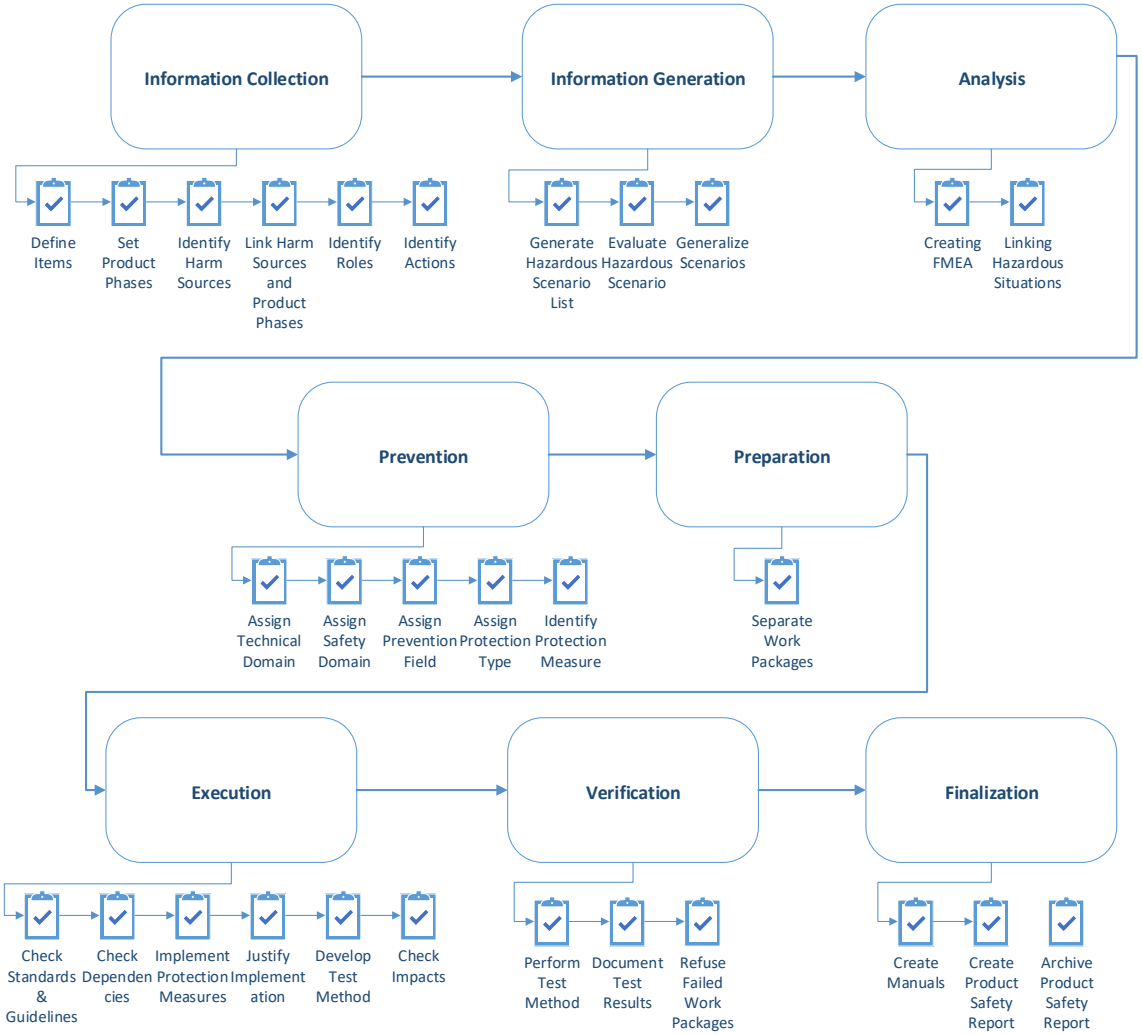


Figure 4.1: General overview of the system safety process with all eight parts.

Overall the new product safety method is generally divided in eight phases:

- *Information Collection*
- *Information Generation*
- *Analysis*

- *Prevention*
- *Preparation*
- *Execution*
- *Verification*
- *Finalization*

The objects of the *Analysis* and *Verification* phases are related, because the failures and causes that are identified in the *Analysis* are covered by the measures. These measures are validated in the *Verification* phase and prevent the arising of the identified failures. There is also a relation between the *Information Collection* and *Information Generation* phases as well as the *Finalization* phase, because the product fulfills the specification and therefore will be safe for this kind of application.

Information Collection
In the first process phase, general information about the product is collected and assorted. This is one of the most critical parts of the whole product development especially for safe products. This step defines the system-borders and limits of the product and established the base for all further failure and risk analysis. It is not easily possible to change these conditions at the end of the development process. It is necessary to put enough effort in this phase and think about future markets and possible environmental conditions or changes in product application[Lev11].

Information Generation
Using the collected information from the previous phase the *Hazardous Situation List* is generated to support the further steps of the product safety method[Heg11].

Analysis
In this phase the failure and risk analysis takes place. Consequently the well known *FMEA* method is used[PLH16]. This method is supported by the previously generated information phase and is an important key for the traceability of product safety.

Prevention
In this phase detected *Failures* are handled by defining *Measures* that prevent the *Failure* to occur and the *Measure* is assigned to different domains for classification.

Preparation
This phase divides the detected *Measures* into *Work Packages* to split the work into small pieces that can be done by individual engineers.

Execution
In this phase the defined *Work Packages* are executed. This step considers all information related to the specific *Measure* that are specified in the previous phases.

Verification
This phase is focusing on the verification of the *Measures* implemented in the *Execution* phase. This is necessary to prevent the possible failures and ensure product safety.

Finalization
The last phase is about summarizing all generated information and work into a *Product Safety Report* to complete the product safety traceability and evidence[Heg11].

4.2 Information Collection

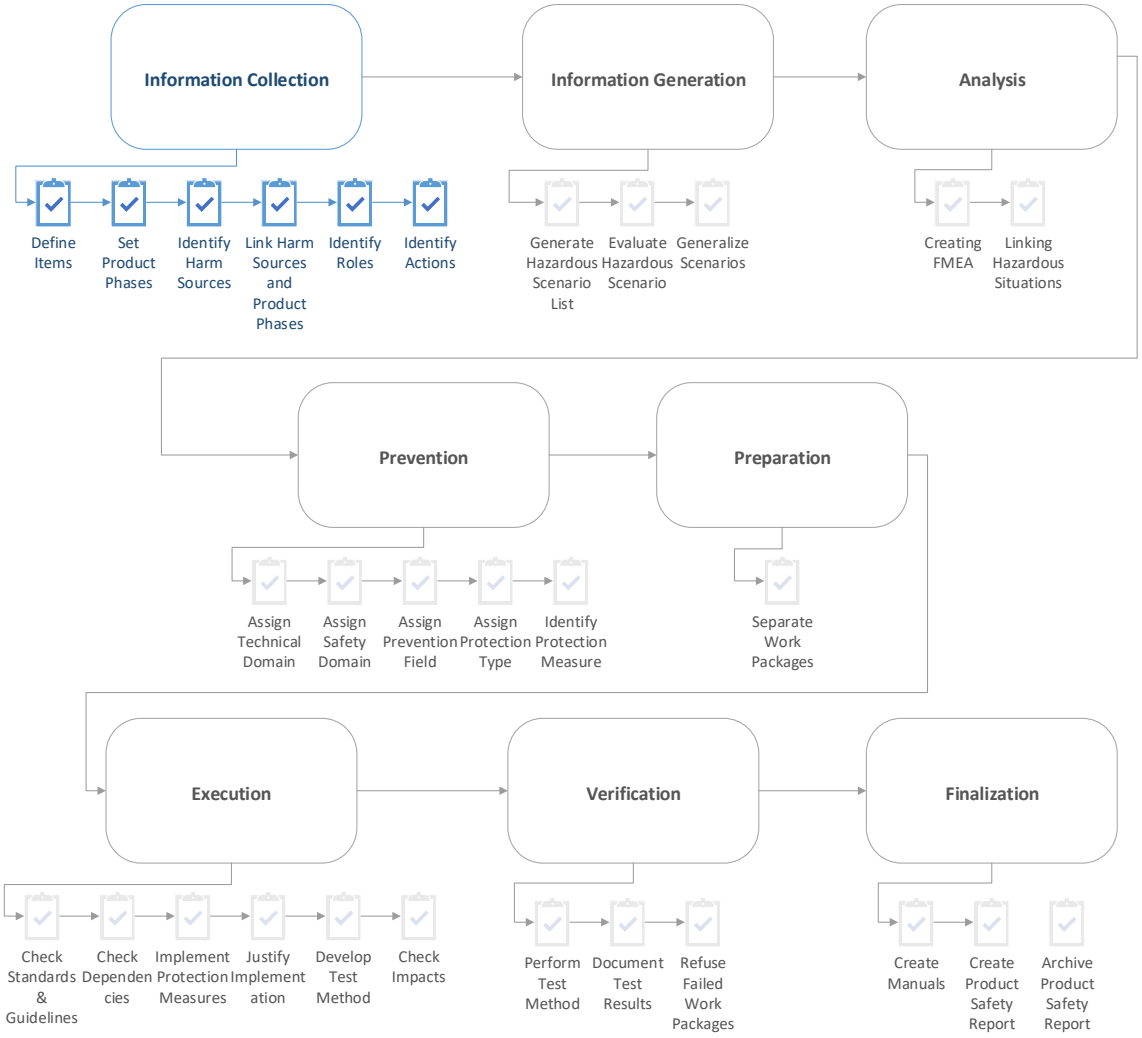


Figure 4.2: General overview of the *Information Collection* phase.

4.2.1 General Overview

This phase is the base for all further phases and collects information about the *Item* in development, the environmental conditions and legal aspects. This phase is also very important to ensure a safe product. Making mistakes or doing it neglectful can lead to an unsafe product and further changes can not be done without restarting the whole process. Therefore it is necessary to put enough effort and time in this phase to ensure a safe product in the end of this process.

4.2.2 Input

This phase is the first phase of the whole process but this does not mean that there is no input. Developing a new *Item* is always combined with requirements of different departments. This departments can be very different and also their requirements. In the automotive domain there are usually three basic departments that have to be considered:

- Customers
  - Specifications
  - Requirements
- Companies
  - Guidelines
  - Code of Conduct
  - Company norms
- Governments
  - Laws
  - Standards

Every department have their own visions and point of views. It is necessary to start the research and find out what is necessary to satisfy all needs and requirements of all different departments. Furthermore it is necessary to define in what region and countries the *Item* will be launched to select the appropriate standards and laws.

4.2.3 Activity

As already mentioned this phase is focused on gathering information about the *Item* and the related circumstances. To support this important phase the following information should be investigated:

- *Item* Definition[fSCI11]
- *Product Phases*[DDIfN11]
- *Harm Sources*[Sch09, DDIfN11]
- *Roles*[Sch09]
- *Actions*[DDIfN11]

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Define the *Items*
2. Set the required *Product Phases* for each *Item*
3. Identify the potential *Harm Sources* for every considered *Item*
4. Create a link between the *Harm Sources* and the *Product Phases* when this sources can occur
5. Identify all potential *Roles* in every *Product Phase*
6. Identify all possible *Actions* from all different *Roles* in every *Product Phase*

Item definition

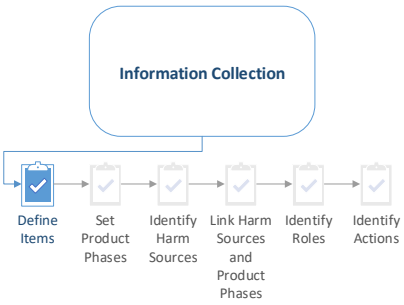


Figure 4.3: *Item* definition step of the *Information Collection* phase.

One of the most basic steps is the definition of the *Items*. The term *Item* is well known in the automotive industry and is one of the first steps of the ISO 26262. The product safety method is using the existing item of the ISO 26262. The item is providing at least the following information[fSCI11]:

- Functions and Non-Functions
- Interfaces
- Environmental Conditions
- Expected Countries and Regions
  This point was added to be able to determine the legal regulations.

Overview	Name	Description
Item	Item #1	Description of Item #1
Item	Item #2	Description of Item #2

Requirements	Name	Description
Functional	Functional Requirement #1	Description of Functional Requirement #1
	Functional Requirement #2	Description of Functional Requirement #2
Non-Functional	Non-Functional Requirement #1	Description of Non-Functional Requirement #1
	Non-Functional Requirement #2	Description of Non-Functional Requirement #2
	Non-Functional Requirement #3	Description of Non-Functional Requirement #3
	Non-Functional Requirement #4	Description of Non-Functional Requirement #4

Environmental Conditions	Spalte1	Spalte2
Condition #1	Min	Max
Condition #2	Min	Max

Expected Countries and Regions
Country #1
Country #2

Figure 4.4: Example about the *Item* definition.

The environmental conditions is an important information for system safety. It is necessary to understand what kind of forces affect the item. This is essential for system safety measure definitions. The expected countries and regions are necessary to consider the local legislation. Each region has different kinds of engineering standards and laws to fulfill the required product safety levels.

Product Phases

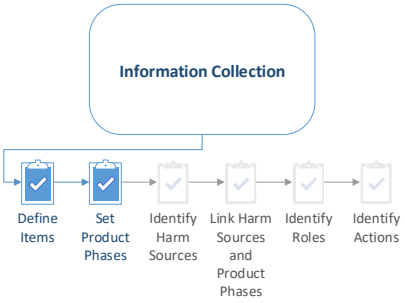


Figure 4.5: *Product Phases* selection step of the *Information Collection* phase.

The product undergoes specific phases in its lifetime[DDIfN11]. Each phase has different needs and requirements, especially when considering safety. To provide the possibility to ensure system safety for the whole lifetime it is necessary to consider all different stages. Therefore this method is determining what kind of phases need to be consider for the system safety purpose. In the automotive domain there are basically eleven individual phases that an *item* can undergo during lifetime. These are well known from industry standard ISO 12100 and field research[DDIfN11]:

- Manufacturing

- Development
- Crash
- Repair/Maintenance
- 2nd Life Repair/Maintenance
- Installation
- Transport
- Storage
- Operation
- 2nd Life Operation
- Decommissioning

Some of them are hopefully never reached while some others can be reached several times. The individual phases are distinguished in length and operators. Every phase has to be considered for product safety. Especially the operators have a large impact on safety as mentioned in Section 2.3.2 on Page 10 [Lev11, Sch09].

Identify Product Phases	Item #1	Item#2	Item #3
Manufacturing	X	X	X
Development		X	X
Crash	X	X	X
Repair/Maintenance	X	X	X
2nd Life Repair/Maintencance		X	
Installation	X	X	X
Transport	X	X	X
Storage	X	X	X
Operation	X	X	X
2nd Life Operation		X	
Decomissioning	X	X	X

Figure 4.6: Example about selecting product phases for specific items

Harm Sources

Figure 4.7: Identification of the different *Harm Sources* in the *Information Collection* phase.

Operators are part of product phases and they are operating with the product. The operations and the risks depend on the product phase. The operator can be hurt by different kinds of harm sources. The harm sources have been summarized to six different hazardous energy sources by the consumer electronic safety domain in the standard IEC 62368 as mentioned in the Section 2.5.2 on Page 14[Sch09]. The identified hazardous energy sources which are in this method called *Harm Sources* are[Sch09]:

- Electrical shock
  - Circuits
  - Connectors
  - Cables
- Electrically coursed fire
  - Overcurrent
  - Overvoltage
- Chemical
  - Chemical burn
  - Inhalation
- Mechanical
  - Rotating parts
  - Sharp corners
- Thermal

  - Hot surfaces
- Radiation
  - Laser

Item	Electrical shock	Electrically coursed fire	Chemical	Mechanical	Thermal	Radiation
Item #1	X	X	X	X	X	
Item #2			X			
Item #3				X		

Figure 4.8: Example about selecting harm sources for each item

Roles

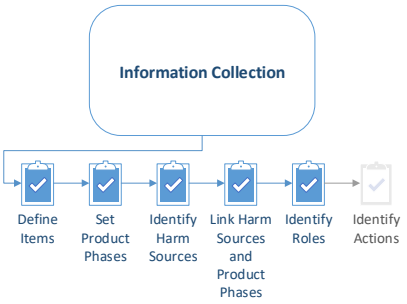


Figure 4.9: Identification of the different *Roles* in the *Information Collection* phase.

Product safety includes all phases of the lifecycle. As mentioned in Section 2.5.1 on Page 12 it is necessary to ensure safe products during each product lifecycle stage[pro04]. The automotive domain identifies many more stages as mentioned in 4.2.3. Every phase has specific operators and every operator has different level of knowledge and education[Sch09]. This idea already has been introduced by other domains for product safety aspects as mentioned in Section 2.5.2 on Page 14. It is necessary to take this into consideration to keep a product safe for the whole lifecycle. Therefore the product safety method is identifying all possible *Roles* for all *Product Phases*.

Roles	Manufacturing	Development	Crash	Repair/Maintenance	2nd Life Repair/Maintencance	Installation	Transport	Storage	Operation	2nd Life Operation	Decomissioning
Driver			X						X		
Road users			X						X		
Aides			X							X	
Domain variant Worker	X	X		X	X		X	X		X	X
Fully-Trained Worker	X	X		X	X	X	X	X		X	X

Figure 4.10: Basic example for a standard list about common *Roles* in the automotive domain.

This standard list can be used as an example and first try-out. It can easily be adopted and expanded for personal needs. This list already identifies what *Product Phases* involve what kind of *Roles*.

Action

Figure 4.11: Identification of the different *Actions* in the *Information Collection* phase.

Then for every *Role* the expected *Actions*, for every product phase, are registered[DDIfN11]. This idea has already been introduced in the machinery construction domain as mentioned in Section 2.5.4 on Page 16. This is necessary to understand how the product will be treated and what is expectable from the specific *Role*. *Roles* are interacting with the product in different ways. This depends on the function of the *Role* and the active *Product Phase*. As mentioned in section 2.3.3 on page 11 it is necessary to involve the *Roles* and their behavior to ensure a safe product[Lev11]. The more *Actions* are identified, the more *Hazardous Scenarios* can be analyzed and investigated.

Product Phase	Role #1	Role #2
Operation		
Actions	Action #1.1	Action #2.1
Actions	Action #1.2	Action #2.2

Figure 4.12: Basic example for an *Action* list with different *Roles* in the automotive domain.

4.2.4 Output

The first phase of the product safety method needs a lot of research effort and puts the *Item* in a frame. This means that the *Item* will be developed for a certain market with certain requirements. After this phase the following details are determined and are available for the further steps:

- *Item* Description
- Considered *Product Phases*
- Identified *Harm Sources*

- Identified *Roles*
- Identified *Actions* in combination with the specific *Roles*
- Identified Standards & Guidelines
- Identified Laws

This documents are the groundwork for all further phases and have a big impact on the end result. The more effort is put in this phase, the more valuable the end result will be.

4.2.5 Process Procedure

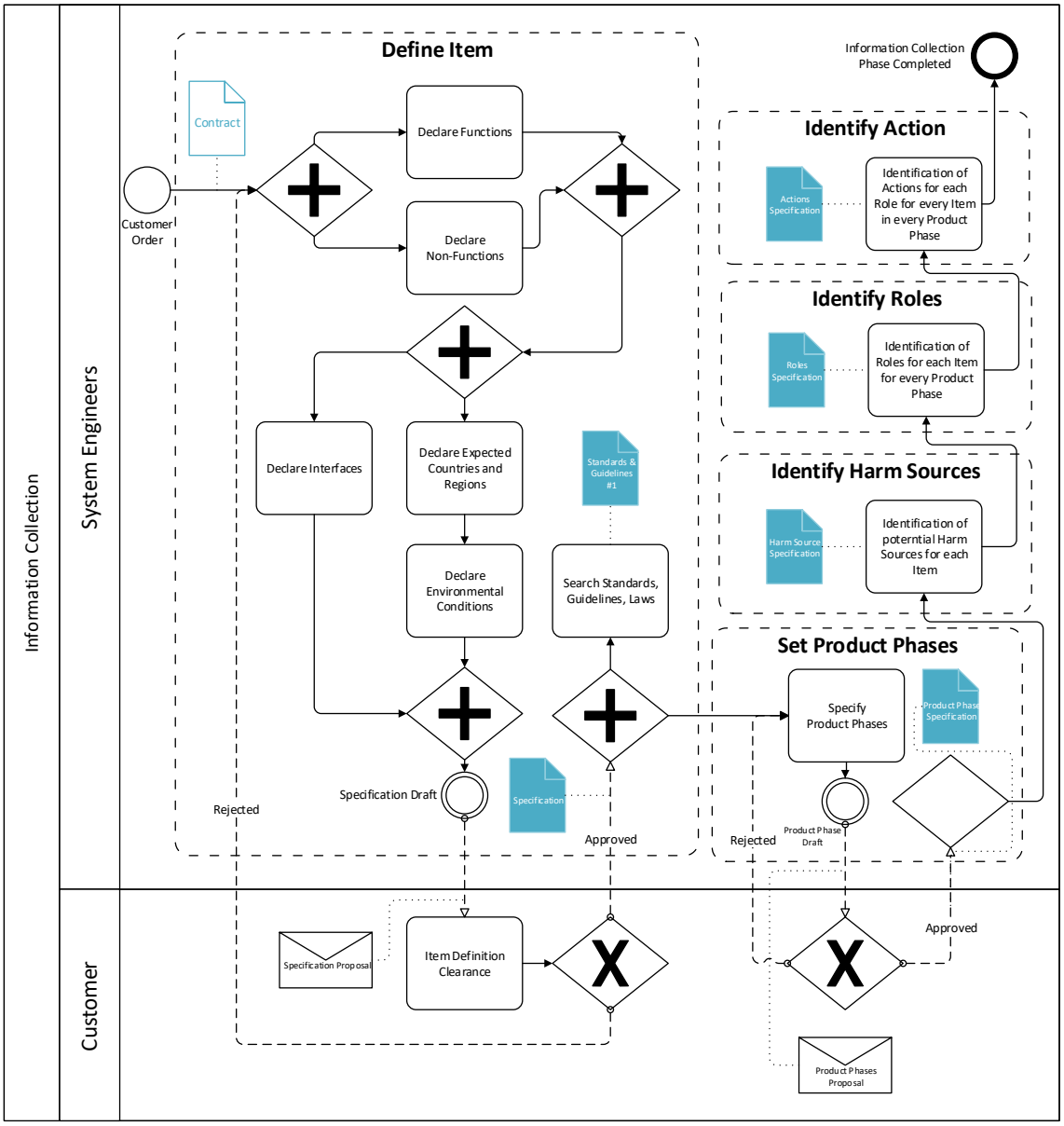


Figure 4.13: *BPMN* Process Procedure Overview of the *Information Collection* phase.

4.3 Information Generation

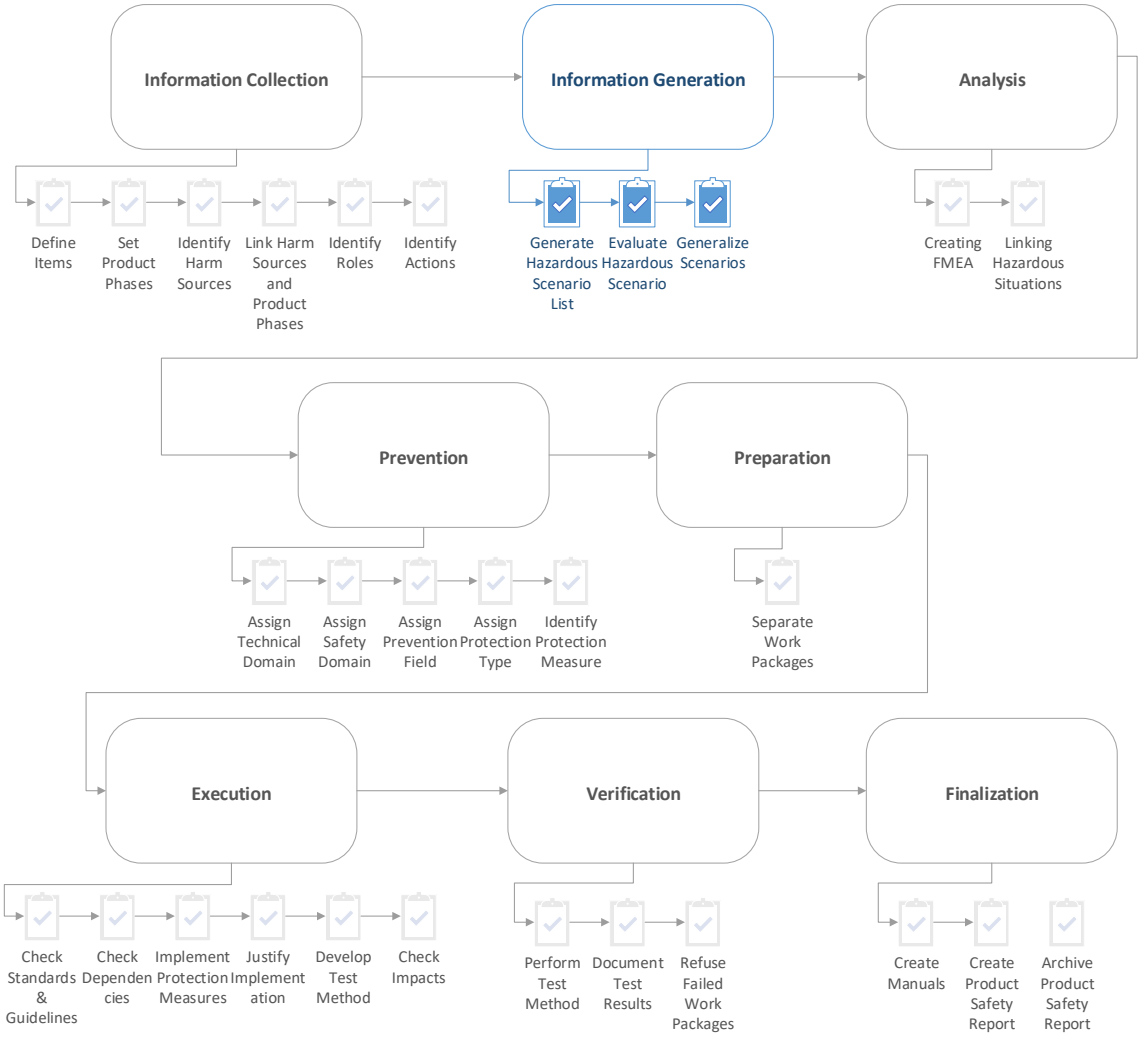


Figure 4.14: General overview of the *Information Generation* phase.

4.3.1 General Overview

The individual factors mentioned in the *Information Collection* have to be connected together to provide the possibility to analyze *Hazardous Situations*. *Hazardous Situations* are situations where a *Role* gets harmed by a specific *Harm Source* during a specific *Action*. This kind of situation needs to be considered in the design phase for establishing a robust product safety concept in the end. The idea is to create a *Hazardous Situation List* automatically to ensure a completeness of the list[GOS+15, LKMP11]. This list can support the engineers during the failure and risk analysis to identify hazards related to the product[Heg11]. This idea has already

been introduced by the Medical Product Domain as mentioned in Section 2.5.3 on Page 15.

4.3.2 Input

To provide the possibility of generating a list automatically, information from the *Information Collection* is needed. The *Information Collection* phase has collected information about the product and these have to be considered:

- *Product Phases*
- *Item* List
- *Harm Sources*
- *Roles*
- *Actions*

4.3.3 Activity

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Generate *Hazardous Situation List*
2. Evaluate the possibility of the *Hazardous Situations*.
3. Summarize and generalize similar *Hazardous Situations*.

Generate *Hazardous Situation List*

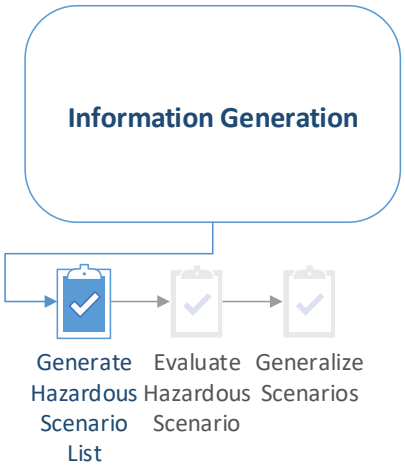


Figure 4.15: Generation of the *Hazardous Situation List* in the *Information Generation* phase.

The first step is about generating the *Hazardous Situation List*[GOS+15, LKMP11]. This table will be the initial point for all future hazard and risk analysis. The automatic generation of the situations support the engineers during the design phase[Heg11]. This idea of supporting the engineers has already been introduced by the Medical Product Domain as mentioned in section 2.5.3 on page 15 as well as the automatic generation of scenarios by Goto *et al.*[GOS+15] and by Li *et al.*[LKMP11]. It is necessary to consider all the terms which where identified in the *Information Collection* phase.

- *Item* List
- *Product Phases*
- *Harm Sources*
- *Roles*
- *Actions*

1. Create all combinations of the given terms

Create all combinations

Item	Product Phase	Role	Harm source	Actions	Hazardous Situation
HV Battery	Crash	Aides	chemical injury	first aiding	[HV Battery] induces chemical injury on Aides during Crash while first aiding

Figure 4.16: Example of a generation of the *Hazardous Situation List* in the *Information Generation* phase.

The *Hazardous Situation* can be automatically generated. For example in Excel it is possible to concatenate the terms with words like:

```
=’’[‘‘\&A2\&’’]’’\&’’ induces ‘‘ \&D2 \& ‘‘ on ‘‘\&C2\& ‘‘ during
‘‘ \&B2\& ‘‘ while ‘‘ \&E2.
```

Item	Product Phase	Role	Harm source	Actions	Questions
HV Battery	Crash	Aides	chemical injury	first aiding	Can [HV Battery] induce a chemical injury on Aides during Crash while first aiding?

Figure 4.17: Example of a generation a question of the *Hazardous Situation List* in the *Information Generation* phase.

Evaluate the possibility of the *Hazardous Situations*

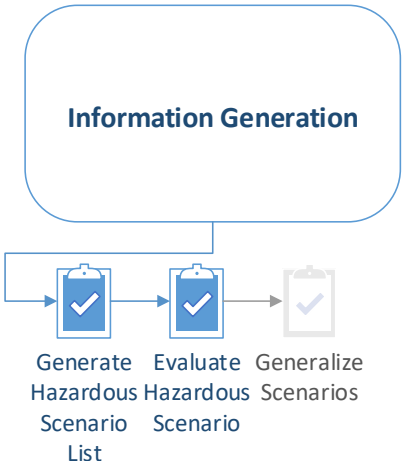


Figure 4.18: Evaluation of the *Hazardous Situation List* in the *Information Generation* phase.

The third step is about reducing the amount of possible *Hazardous Situations*. Automatic generation of all combinations can create a lot of useless or not possible *Hazardous Situations*. To reduce the future work it is useful to purge this kind of situations and justify the decision and record the reason.

1. Eliminate implausible *Hazardous Situations*
2. Record and justify the decision

Summarize similar *Hazardous Situations* together

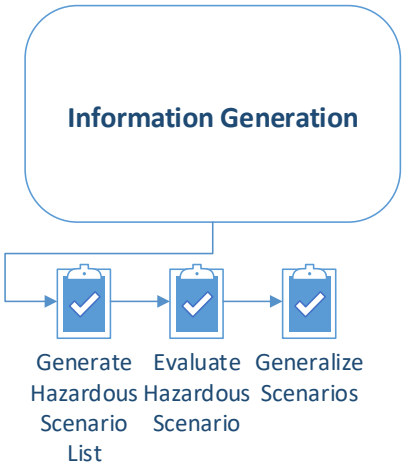


Figure 4.19: Generalizing of the *Hazardous Situation List* in the *Information Generation* phase.

In the fourth and last step it is useful to limit the *Hazardous Situations* again. A car has a lot of different product phases and operators with different actions. This can result in a very long list. It is necessary to reduce it as much as possible to keep this method feasible.

1. Find similar *Hazardous Situations*
2. Derive a generalized situation
3. Apply the new generalized situation and replace the origins

4.3.4 Output

In the end of this phase a list of all possible *Hazardous Situations* is created and can be given to experts. Experts can use this situations to understand how the specific *Item* will be used and what kind of situations they have to consider[Heg11]. The automatic generation supports the engineer to think about every possible situation which can be hazardous and that nothing can be forgotten.

- *Hazardous Situation List*

4.3.5 Process Procedure

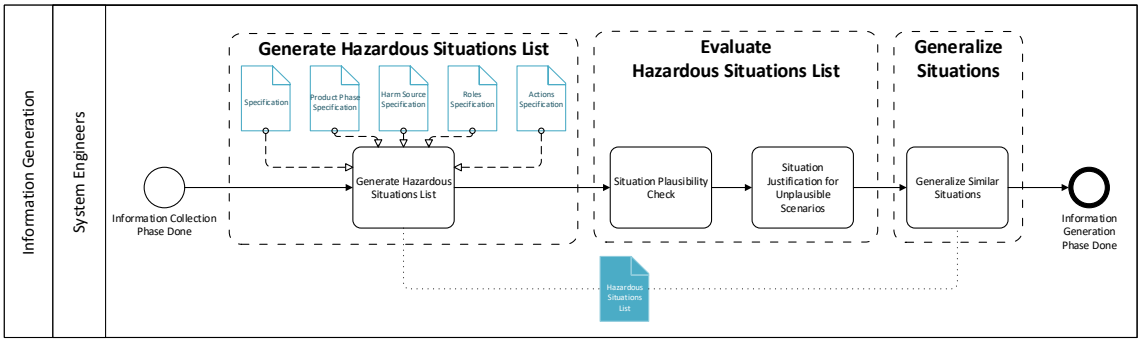


Figure 4.20: *BPMN* Process Procedure Overview of the *Information Generation* phase.

4.4 Analysis

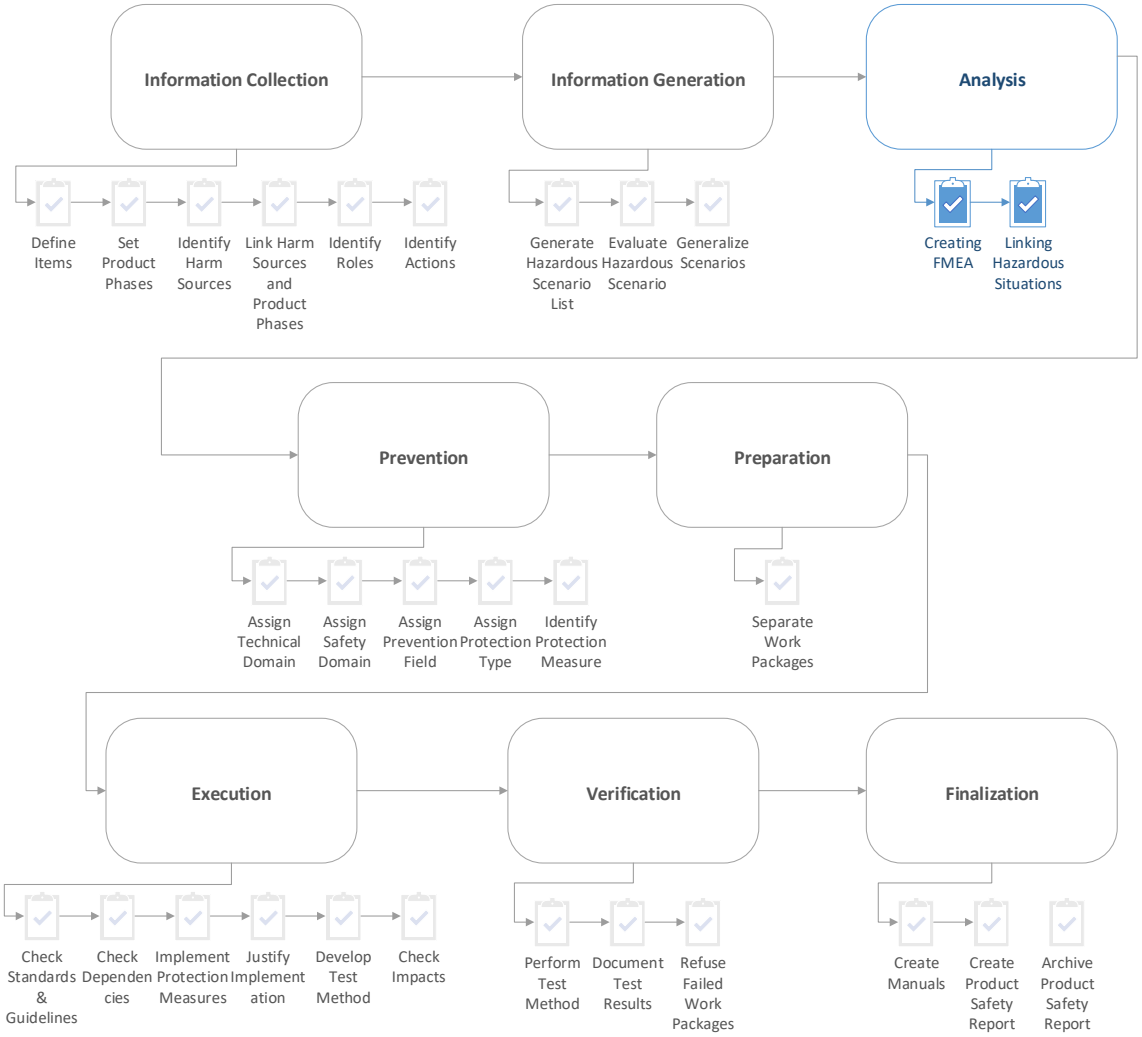


Figure 4.21: General overview of the *Analysis* phase.

4.4.1 General Overview

This phase is about analyzing the system and performing a failure and risk analysis as well as linking to the *Hazardous Situations* from the *Hazardous Situation Lists* of the *Information Generation* phase. This offers a big pool of information which can be used for future phases of this process. This is typically done with the traditional safety engineering methods *FMEA* and *FTA*[PLH16, SSK14]. This idea has already been introduced by many other industries as mentioned in section 2.2 on page 8. This method uses a *FMEA* to find and detect possible failures.

4.4.2 Input

The automatically generated list of *Hazardous Situations* from the *Information Generation* phase will be used to support the finding of safety related failures and causes. Furthermore the linking between the failure and the *Hazardous Situations* helps to understand which failures and therefore causes and effects have an impact on specific *Hazardous Situations*. To support the engineer the following information should be provided:

- *Hazardous Situation List*
- Standards & Guidelines
- Laws
- *Item* Description

4.4.3 Activity

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Creating *FMEA*
2. Linking *Hazardous Situations* to the *FMEA*

Creating *FMEA*

Figure 4.22: Creation of the *FMEA* in the *Analysis* phase.

This product safety method supports the integration of all *Product Phases* of the whole lifecycle of the product in development. Therefore it is not useful to create a single *FMEA*. As mentioned in section 2.2.1 on page 8 the *FMEA* can be divided in different types of *FMEA*. This method prefers this possibility and suggests the following different *FMEA*[PLH16]:

- System-*FMEA*
- Production-*FMEA*
- Development-*FMEA*
- Service-*FMEA*

Linking *Hazardous Situations* to the *FMEA*

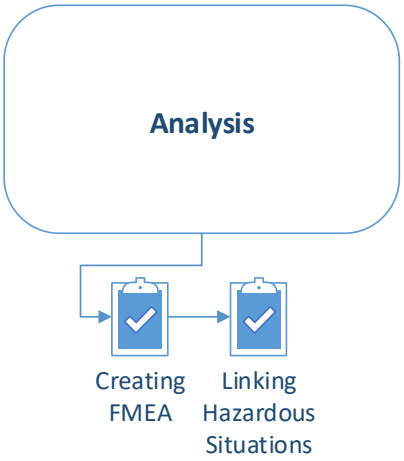


Figure 4.23: Linking between the *Hazardous Situations* and the *FMEA* in the *Analysis* phase.

In this step the *Hazardous Situations* are linked to the specific failures of the different *FMEA*. This step allows for traceability in the future phases and the understanding how the product can harm *Roles*.

4.4.4 Output

The output of this phase is the extended *FMEA* and is called *EFMEA* (extended*FMEA*).

- *EFMEA*

4.4.5 Process Procedure

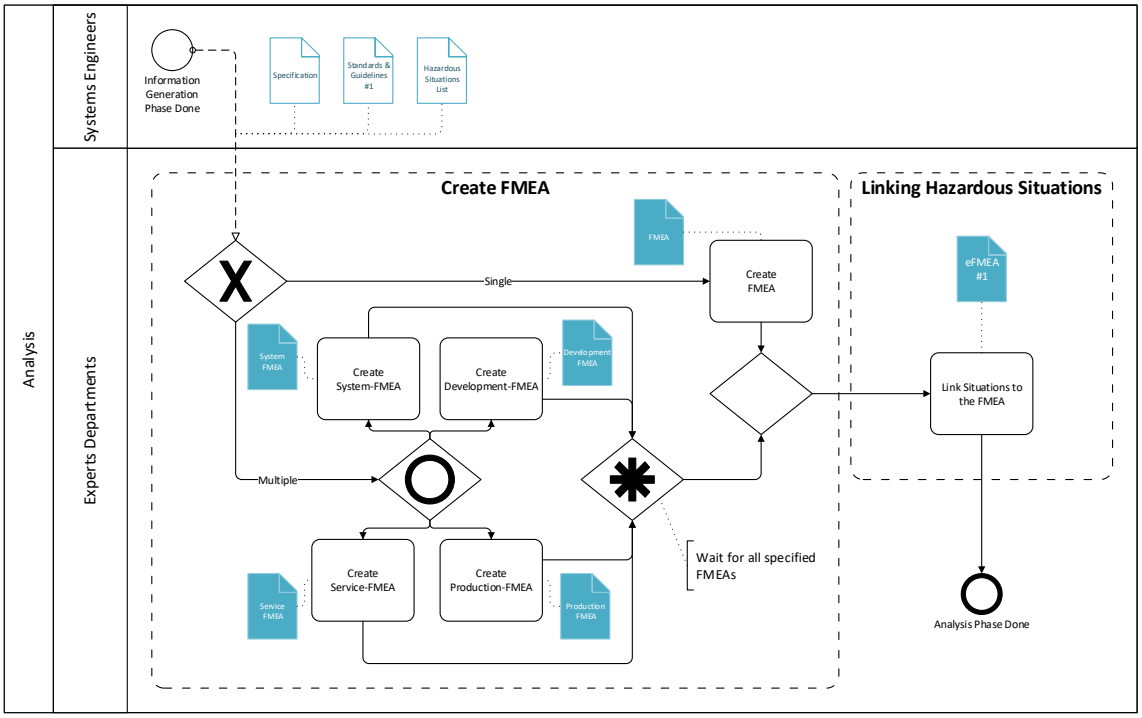


Figure 4.24: *BPMN* Process Procedure Overview of the *Analysis* phase.

4.5 Prevention

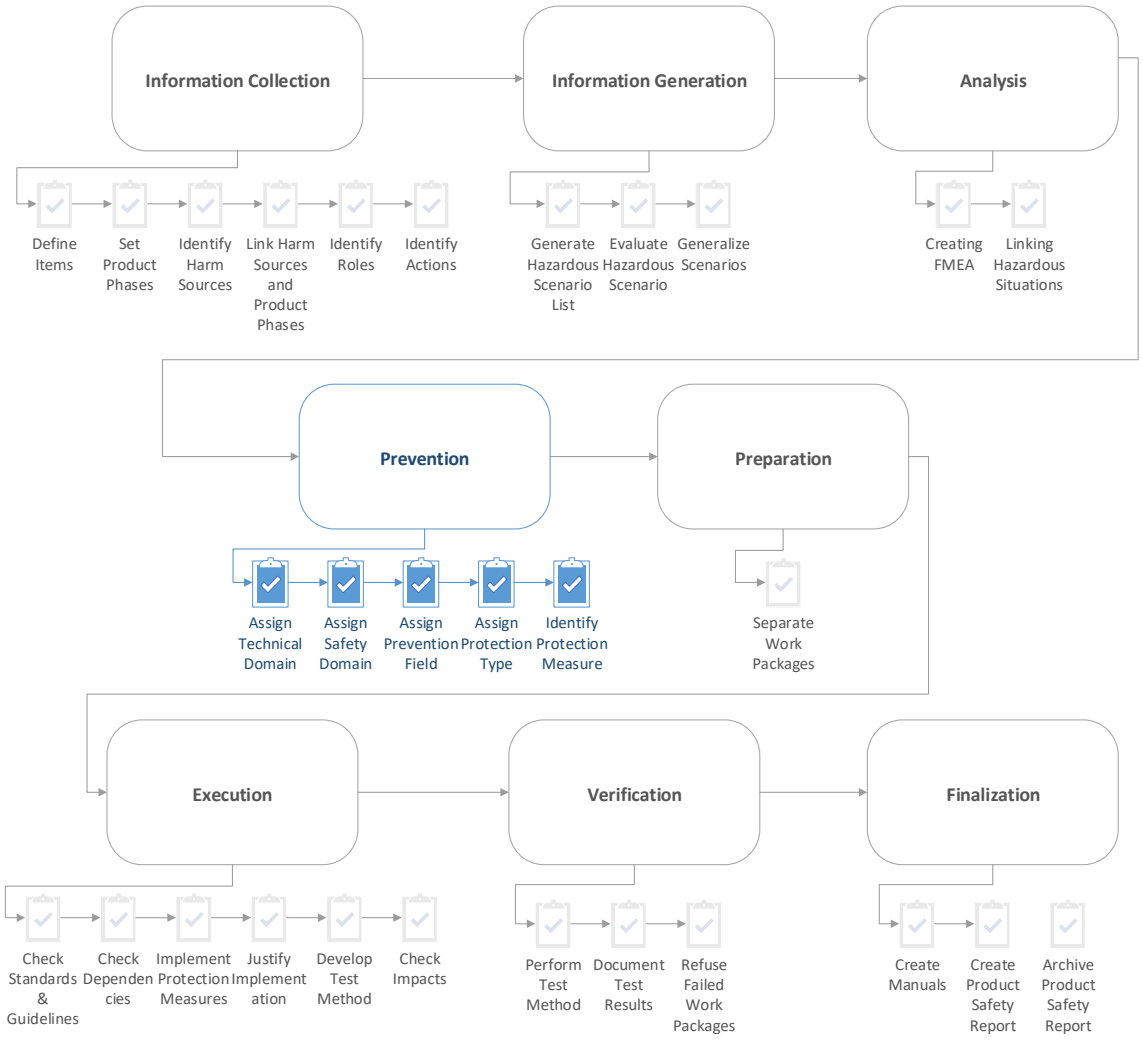


Figure 4.25: General overview of the *Prevention* phase.

4.5.1 General Overview

In this step the *Protection Measures* get classified and assigned. This provides an overview about different technological and safety domains and will help in the future phases to implement the *Protection Measures*.

4.5.2 Input

The previous phases are considered in this phase and therefore the following information is needed:

- *EFMEA*
- Standards & Guidelines
- Laws

4.5.3 Activity

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Assignment of *Technical Domain*
2. Assignment of *Safety Domain*
3. Assignment of *Protection Domain*
4. Assignment of *Protection Type*
5. Identifying *Protection Measure*

Assignment of *Technical Domain*

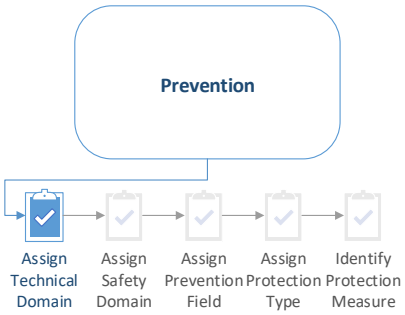


Figure 4.26: Assignment of the *Technical Domain* in the *Prevention* phase.

The different safety domains are linked to a specific engineering domain called *Technical Domain*. In the automotive domain it is possible to reduce them to two basic domains:

- Mechanical
- Electrical

Assignment of *Safety Domain*

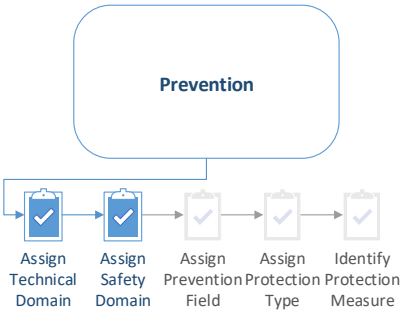


Figure 4.27: Assignment of the *Safety Domain* in the *Prevention* phase.

Safety can be divided in different domains. This separation has been a specification for this thesis and has been provided in the master thesis description[Gri].

- Functional Safety
- Component Safety
- Safety of Use
- High Voltage Safety

Assignment of *Protection Domain*

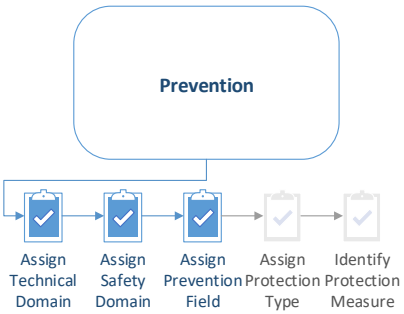


Figure 4.28: Assignment of the *Protection Domain* in the *Prevention* phase.

Safety can be implemented by different domains. This separation is useful to understand at what level the failure can be mitigated. This idea has already been implemented by the Machinery Construction Industry and in the Medical Product Industry as mentioned in section 2.5.4 on page 17 and in section 2.5.3 on page 15. Therefore the following domains were chosen and implemented in this method[DDIfN11, Heg11]:

- Technical
  - Avoid
  - Shield
  - Shut-Off
- Organizational
  - Isolated area
- Personal
  - Protection
  - Training
  - Information

Assignment of *Protection Type*

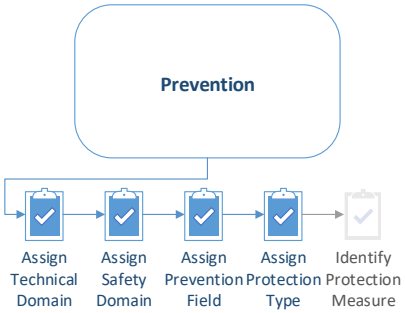


Figure 4.29: Assignment of the *Protection Type* in the *Prevention* phase.

Detecting the right *Protection Type* is the first step to find an appropriate *Protection Measure* for the specific *Harm Sources*. One possibility is to introduce a layer between the *Role* and the *Harm Source*[Sch09]. This idea has already been introduced by IEC 62368 as mentioned in Section 2.5.2 on Page 13. The standard is calling them *Safeguards*. In this method this *Safeguards* are called *Protection Measures*. *Protection Measures* have the same concept like their dependents from the IEC 62368 norm as mentioned in Section 2.5.2 on Page 14[Sch09]. The *Protection Measure* can be separated in the following types as mentioned in Section 2.5.2 on Page 14[Eme15]:

- Equipment *Safeguard*
- Installation *Safeguard*

- Personal *Safeguard*
- Instructional *Safeguard*

Identifying *Protection Measure*

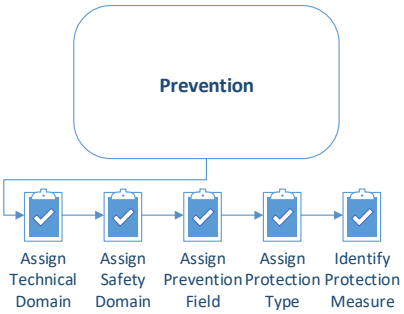


Figure 4.30: Identification of the *Protection Measure* in the *Prevention* phase.

The previous assignments should help to identify the right *Protection Measure*. The identification should consider the *Item* Description, Standards & Guidelines and the Laws from the previous phases. The *Protection Measure* must not be specified in detail in this phase. This will be done in the next phases.

4.5.4 Output

After this step all necessary *Protection Measures* to reduce the risk to an acceptable level has been identified.

- *Protection Measures*

4.5.5 Process Procedure

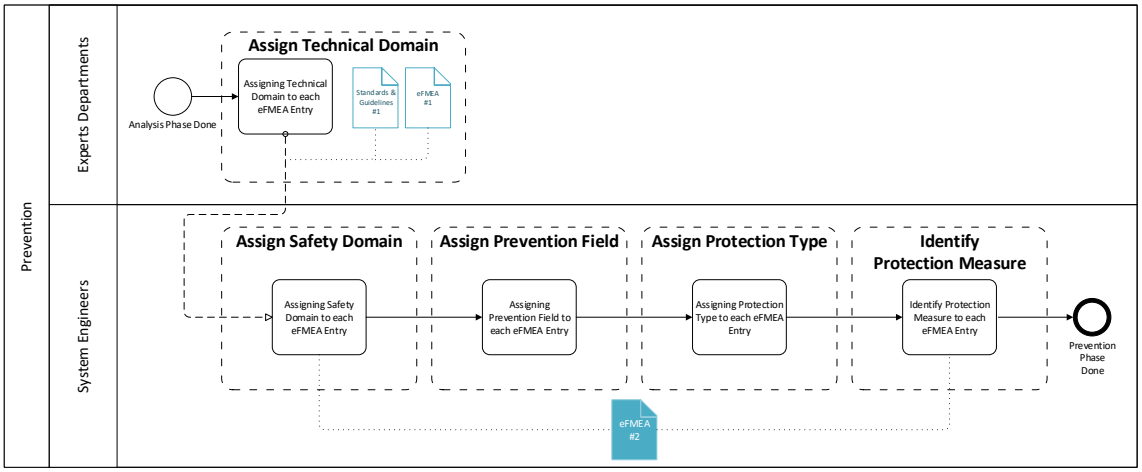


Figure 4.31: *BPMN* Process Procedure Overview of the *Prevention* phase.

4.6 Preparation

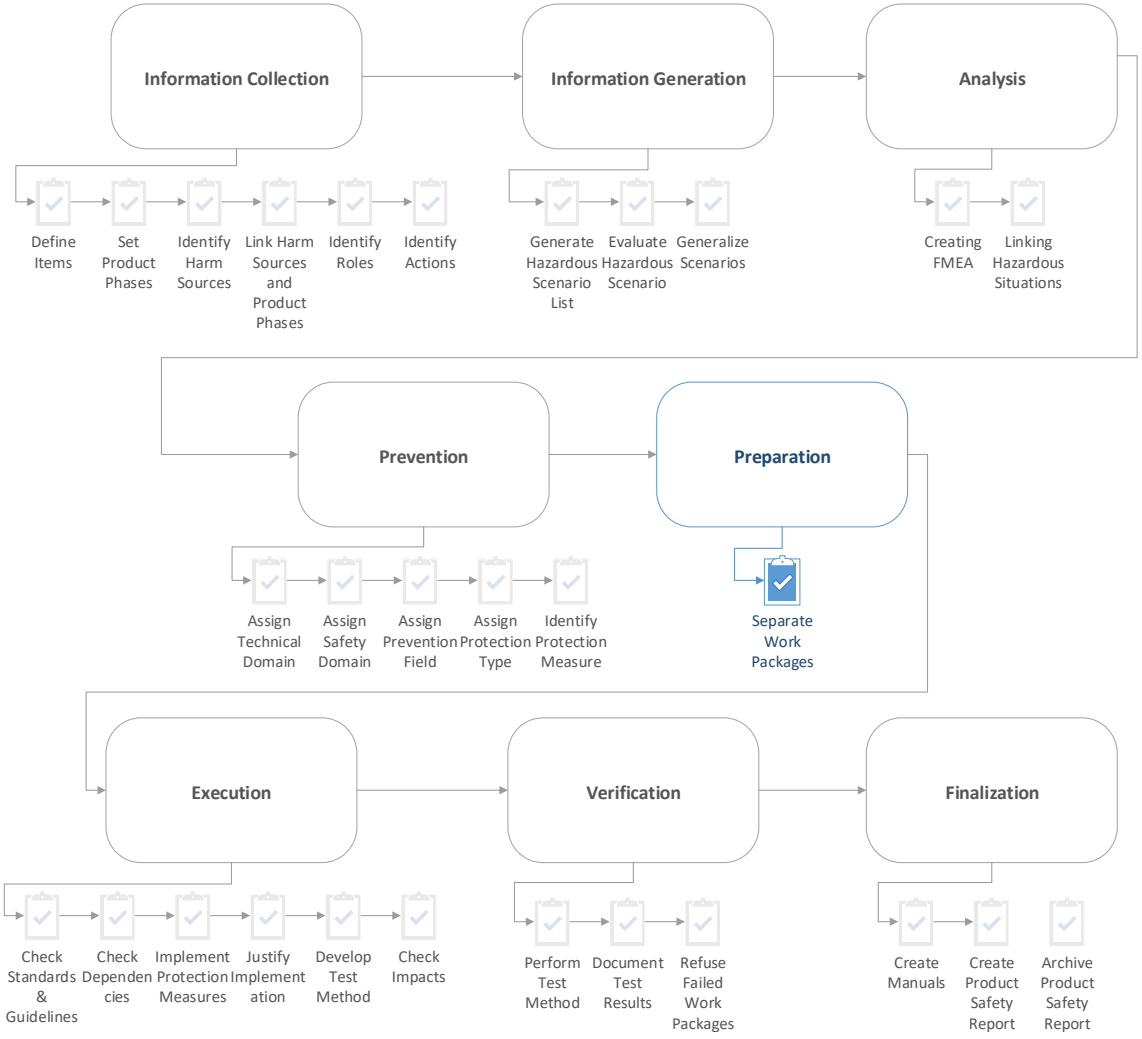


Figure 4.32: General overview of the *Preparation* phase.

4.6.1 General Overview

In this phase the identified *Protection Measures* from the *EFMEA* are separated into individual *Work Packages*. This offers the opportunity to distribute the work into different departments according to the *Technical Domain* as well as a parallelization of the work.

4.6.2 Input

As an input the phase needs the *EFMEA* with the identified *Protection Measures*.

- *Protection Measure*

4.6.3 Activity

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Separation into different *Work Packages*

Separation into different *Work Packages*

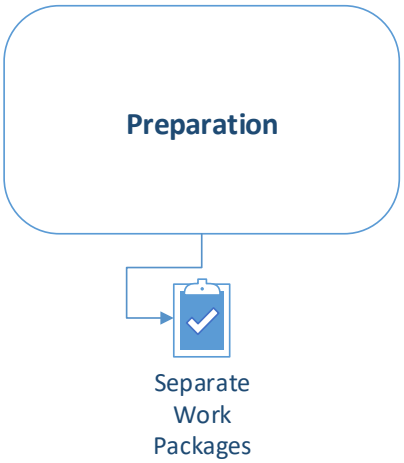


Figure 4.33: Separation of the *Work Packages* in the *Preparation* phase.

In the industry usually experts and engineers are assigned to a specific *Technical Domain*. Therefore the *Work Packages* should be separated by the *Technical Domain* and furthermore separated by the *Safety Domain*. This provides the possibility to deliver the *Work Packages* to different *Technical Domains* and the related experts. To support the engineers it is necessary to provide additional information what can be found in the *EFMEA* from the *Prevention* phase:

- *Item* Description
- *Failures*
- *Hazardous Situations*
- *Protection Measure* Details

4.6.4 Output

In this phase the output is the separation of the whole *EFMEA* list into individual *Work Packages*. This can be forwarded to different departments and different experts and can be implemented in the next phase. This step also provides the possibility to generate a checklist for the project management to support the project controlling.

- *Work Packages*
- Checklists

4.6.5 Process Procedure

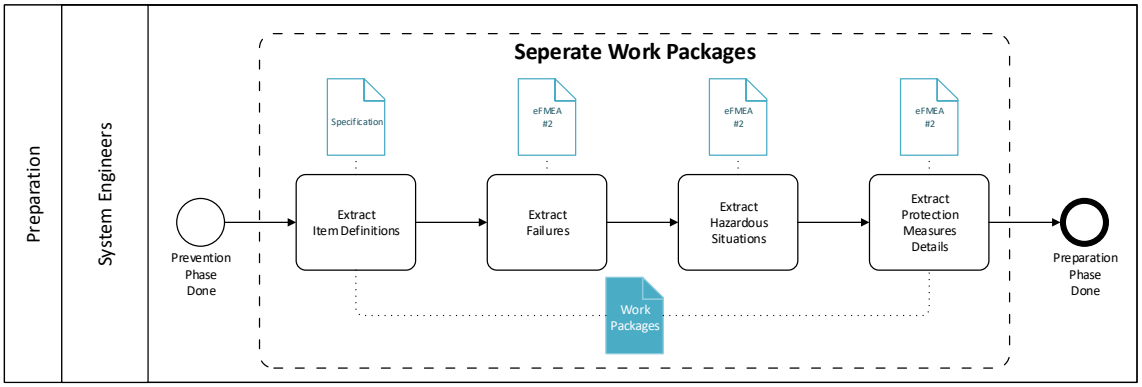


Figure 4.34: *BPMN* Process Procedure Overview of the *Preparation* phase.

4.7 Execution

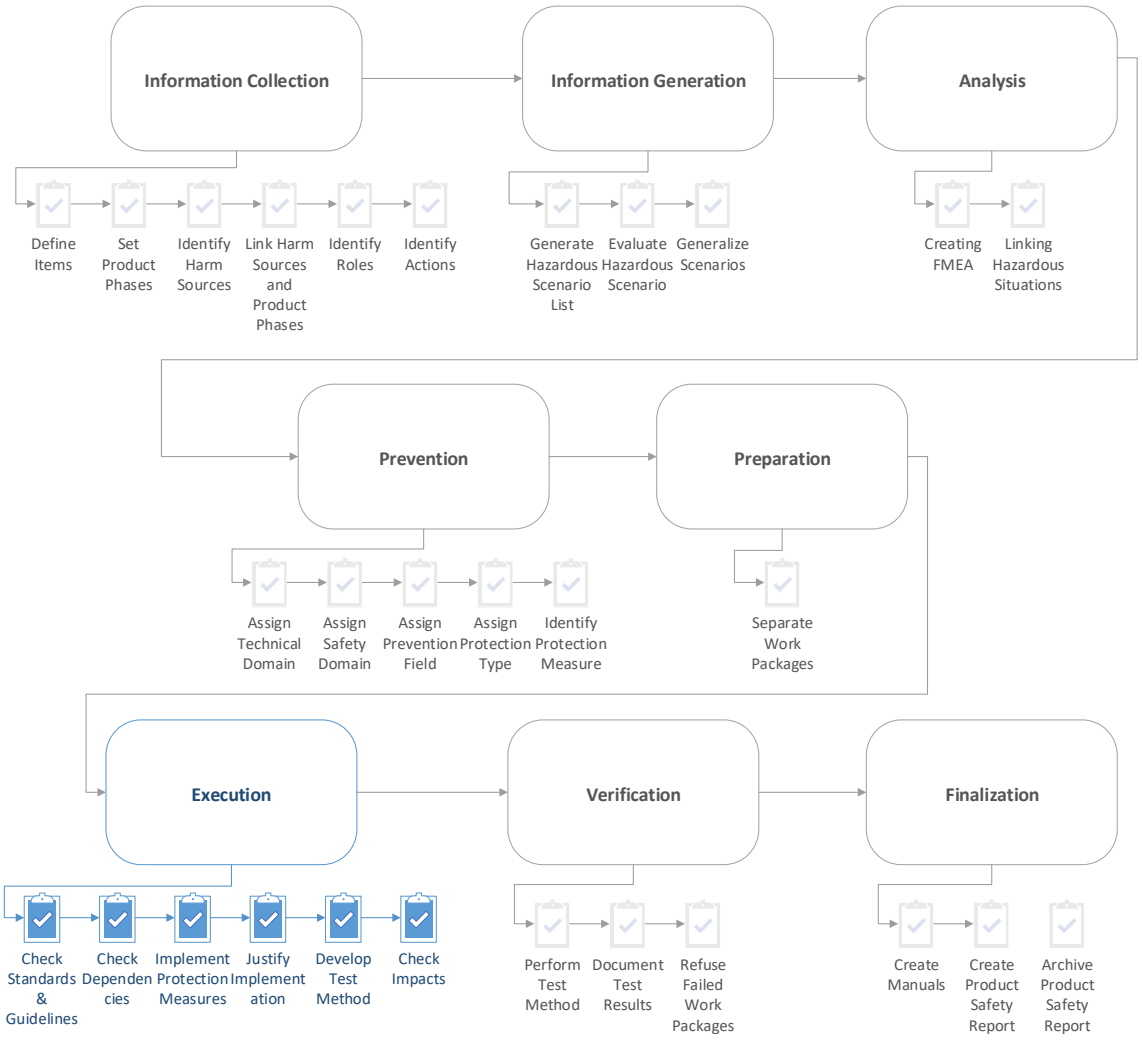


Figure 4.35: General overview of the *Execution* phase.

4.7.1 General Overview

This phase is focusing on the implementation of the determined *Protection Measures* from the previous *Preparation* phase. This is done by engineers in the domain specific departments.

4.7.2 Input

The input comes directly from the previous phases of the process and supports the engineer to understand why and what he has to consider during the implementation. This is in general the following information:

- *Work Package*
- Standards & Guidelines
- Laws

4.7.3 Activity

The implementation of the *Protection Measure* needs to consider all investigated information from the previous phases. Therefore this phase has to consider changes and effects. To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Check Standards & Guidelines
2. Check dependencies to other *Technical Domain*
3. Implementing *Protection Measure*
4. Justify Implementation
5. Develop a *Test Method* for the *Protection Measure*
6. Check impact to other *Work Package*

Check Standards & Guidelines

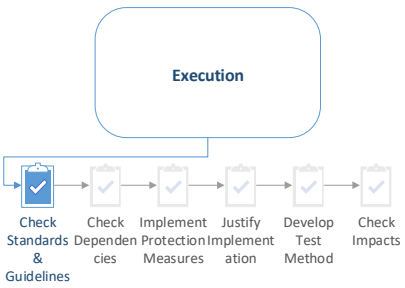


Figure 4.36: Check Standards & Guidelines in the *Execution* phase.

The first step is about checking the selected Standards & Guidelines in the previous phases. This is essential to find out if they are still valid or some are missing.

Check dependencies to other *Technical Domain*

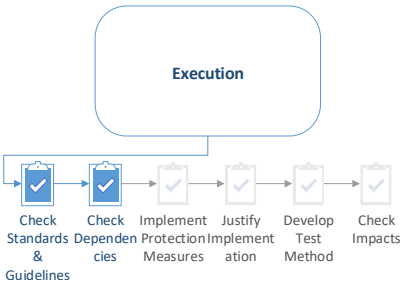


Figure 4.37: Check dependencies to other *Technical Domain* in the *Execution* phase.

Every component has different functions. It is necessary to find out which utilization the specific component and the investigated *Protection Measure* has. Therefore it is necessary to find out, if the *Protection Measure* has interfaces to other *Technical Domain* or other dependencies. If there are some, this *Work Package* must be delayed until the dependency is met or another *Work Package* has to be registered and triggered.

Implementing *Protection Measure*

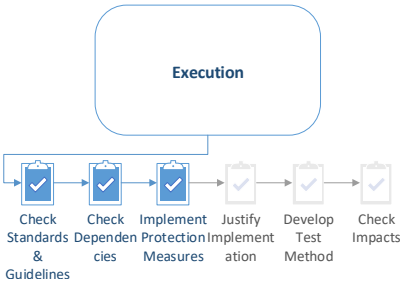


Figure 4.38: Implement *Protection Measure* in the *Execution* phase.

Implementing the *Protection Measure* considers the gathered information provided by the previous phases. This is essential to understand what must be implemented, how it must be implemented and why it must be implemented. The engineer should understand how this *Protection Measure* will be used and what circumstances it must resist. Furthermore this step is an inspection of the previous *Prevention* phase if the *Protection Measure* is usefully selected. Therefore the engineer should consider the following information:

- *Item* definition
  This is necessary to understand where the target market of the product is

and what environmental conditions need to be considered. Furthermore the functional and non-functional requirements from the customer are described.

- *Protection Measure*
  This offers a general information about the chosen *Protection Measure* but no technical implementation details.
- *Failure*
  This provides the engineer with information about the failures the *Protection Measure* has to cope with.
- *Causes*
  Failures are always triggered by causes and therefore they are sticking together to understand how these failures can arise.
- *Hazardous Situations*
  This gives the engineer the opportunity to understand what kind of *Harm Source* can be present.

Justify Implementation

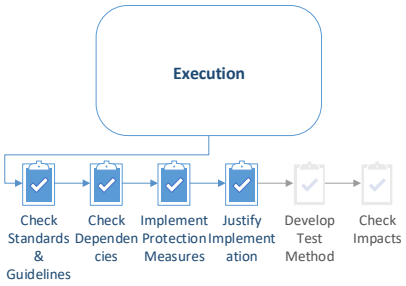


Figure 4.39: Justify the implemented *Protection Measure* in the *Execution* phase.

A product consists of many individual sub-systems and components. Each component is developed and implemented by different *Technical Domain* engineers. In the end of the process and after some years it is necessary to understand and reconstruct how the *Protection Measure* has been developed and what had to be considered. Therefore the engineer must justify his implementation in a *Design Document*. There are different possibilities to show that the implementation of the component fulfills the requirements. This justifications can be:

- Measurement
- Simulation
- Standard & Guideline

Develop a *Test Method* for the *Protection Measure*

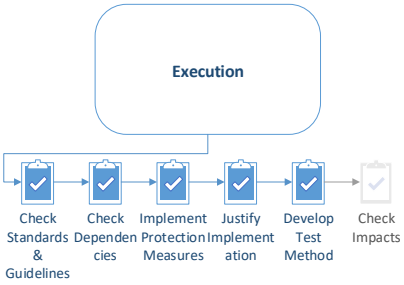


Figure 4.40: Develop a *Test Method* for the implemented *Protection Measure* in the *Execution* phase.

The effectivity of the implemented *Protection Measure* needs to be verified. There is always the possibility that something went wrong during the development, implementation or construction. Therefore the engineer has to develop a method about testing the *Protection Measure*.

Check impact to other *Work Package*

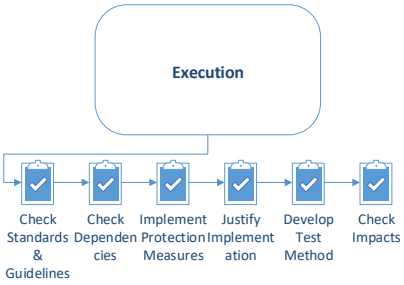


Figure 4.41: Check impacts to other *Work Package* for the implemented *Protection Measure* in the *Execution* phase.

During the implementation requirements sometimes must be changed to ensure the possibility of implementation. This can effect other *Work Packages* and it is necessary to communicate these changes. Any identified impacts need to be transcribed and communicated.

4.7.4 Output

This phase provides the implemented *Protection Measure* and all related documents on that. In general this phase generates:

- Implemented *Protection Measure*
- Created *Design Document*
- Developed *Test Method*
- Additional *Work Packages*

4.7.5 Process Procedure

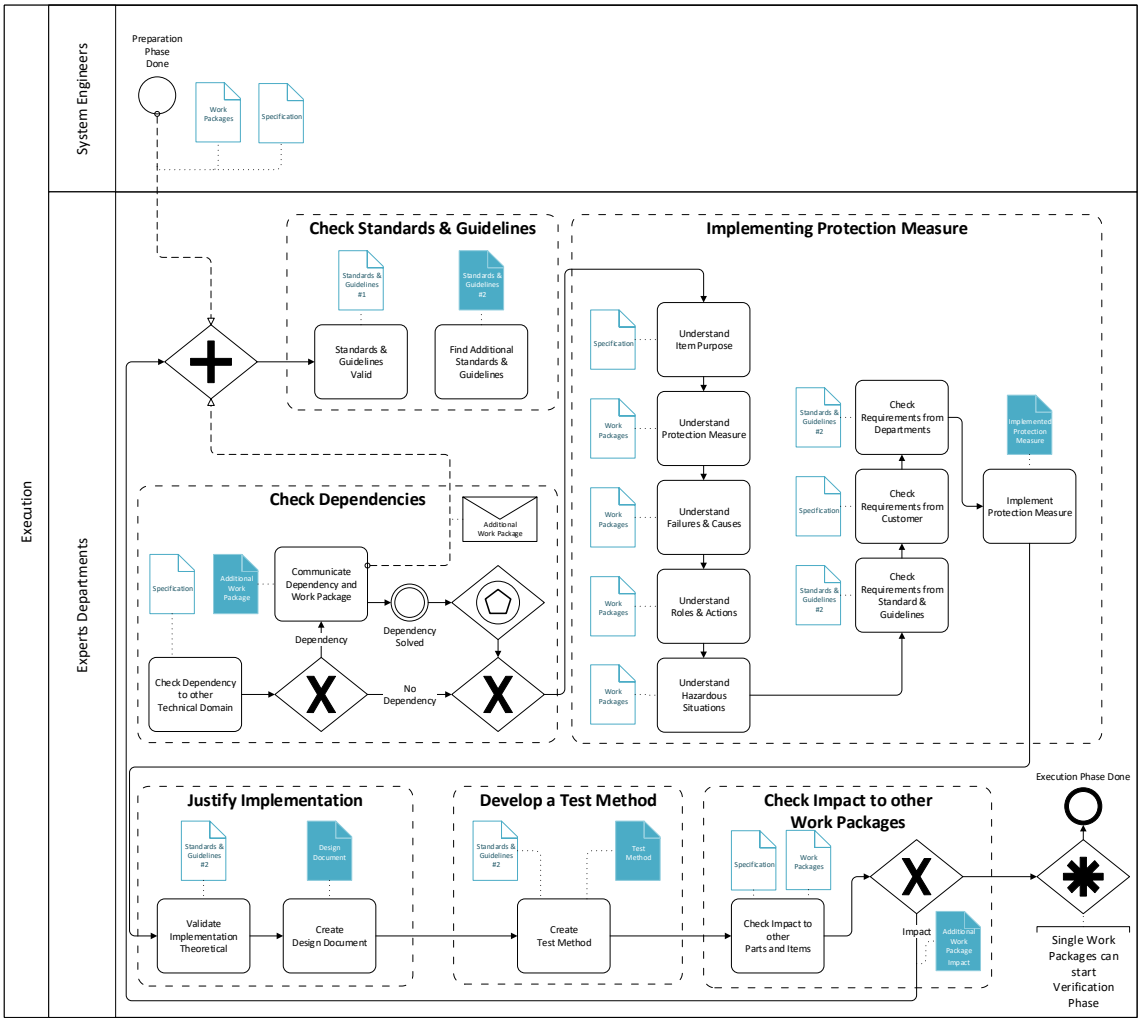


Figure 4.42: *BPMN* Process Procedure Overview of the *Execution* phase.

4.8 Verification

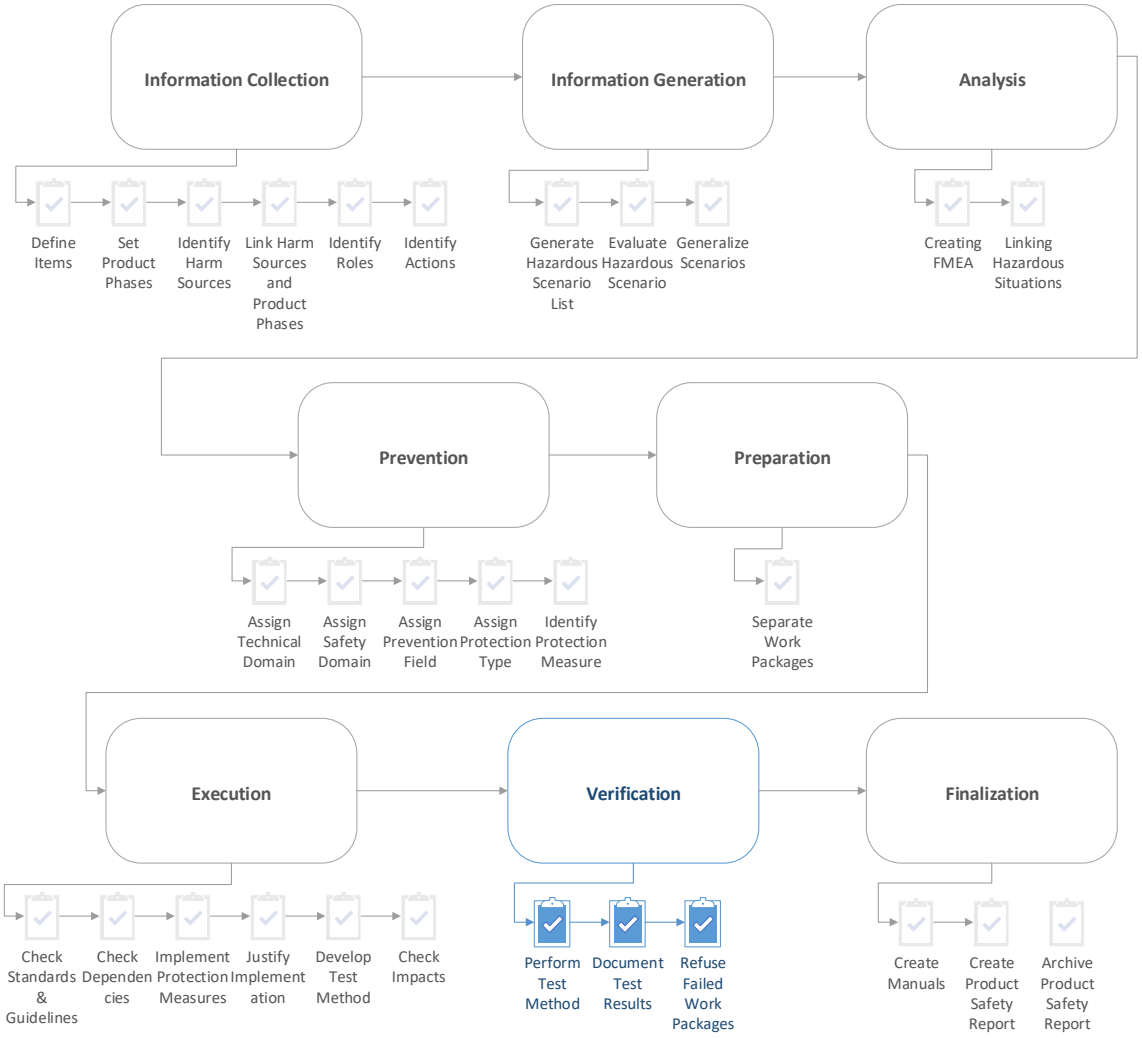


Figure 4.43: General overview of the *Verification* phase.

4.8.1 General Overview

In this phase the *Protection Measures* will be tested that have been implemented in the previous *Execution* phase. This is necessary to prove that the *Protection Measure* fulfills the requirements and that the protection is useful and works.

4.8.2 Activity

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Perform *Test Method*
2. Document the results in the *Test Document*
3. Refuse failed *Work Packages*

Perform *Test Method*

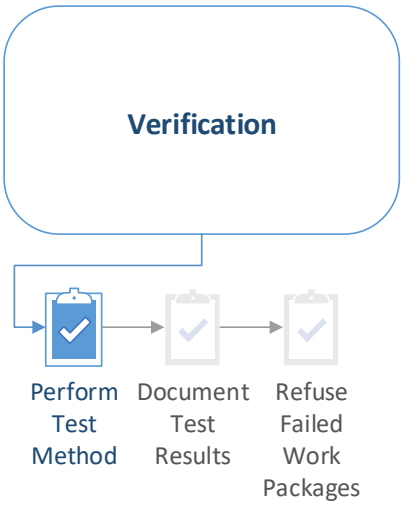


Figure 4.44: Perform the *Test Method* for the implemented *Protection Measure* in the *Verification* phase.

In this step the specified *Test Method* from the *Execution* phase is executed with the specified guideline.

Document the results in the *Test Document*

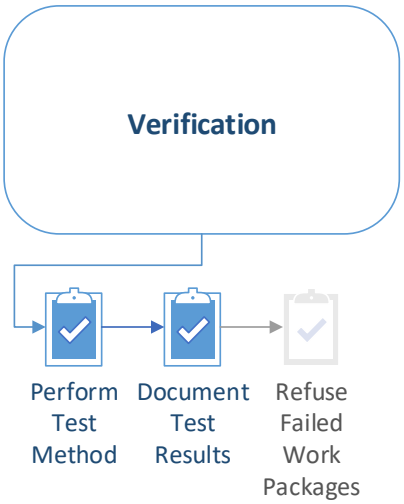


Figure 4.45: Document the results of the *Test Method* for the implemented *Protection Measure* in the *Verification* phase.

The documentation of the results is very important to enable traceability. It is also important to document the used tools and the general setup of the measurement.

Refused failed *Work Package*

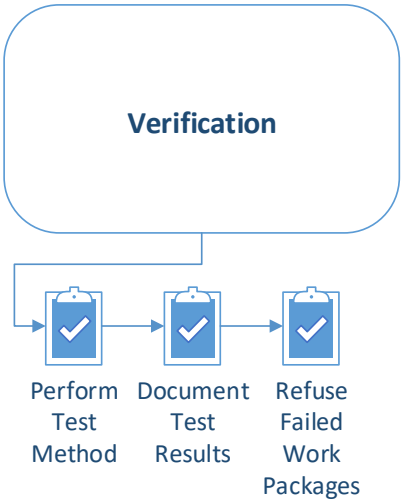


Figure 4.46: Refuse failed *Work Packages* in the *Verification* phase.

If there are any *Protection Measures* that fail the test it is necessary to refuse the *Work Package* and go back to the *Execution* phase and change the implementation.

This step has to be done as long as the *Protection Measure* fails.

4.8.3 Output

In this phase the implemented *Protection Measures* have been tested and the results are the documentation and the results of the test.

- Test Results
- *Test Document*
- Refused *Work Packages*

4.8.4 Process Procedure

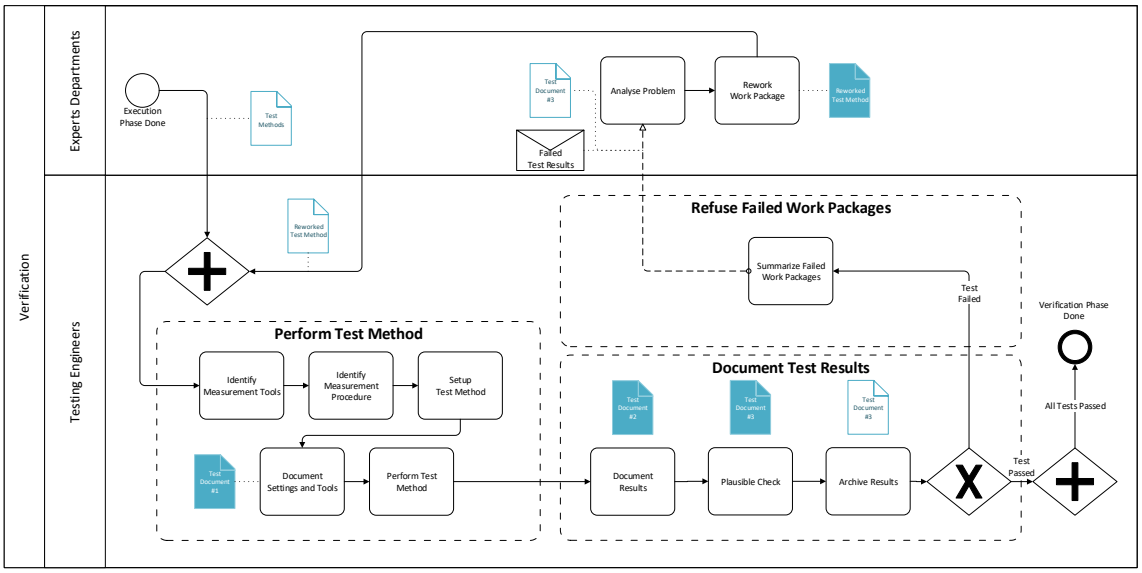


Figure 4.47: *BPMN* Process Procedure Overview of the *Verification* phase.

4.9 Finalization

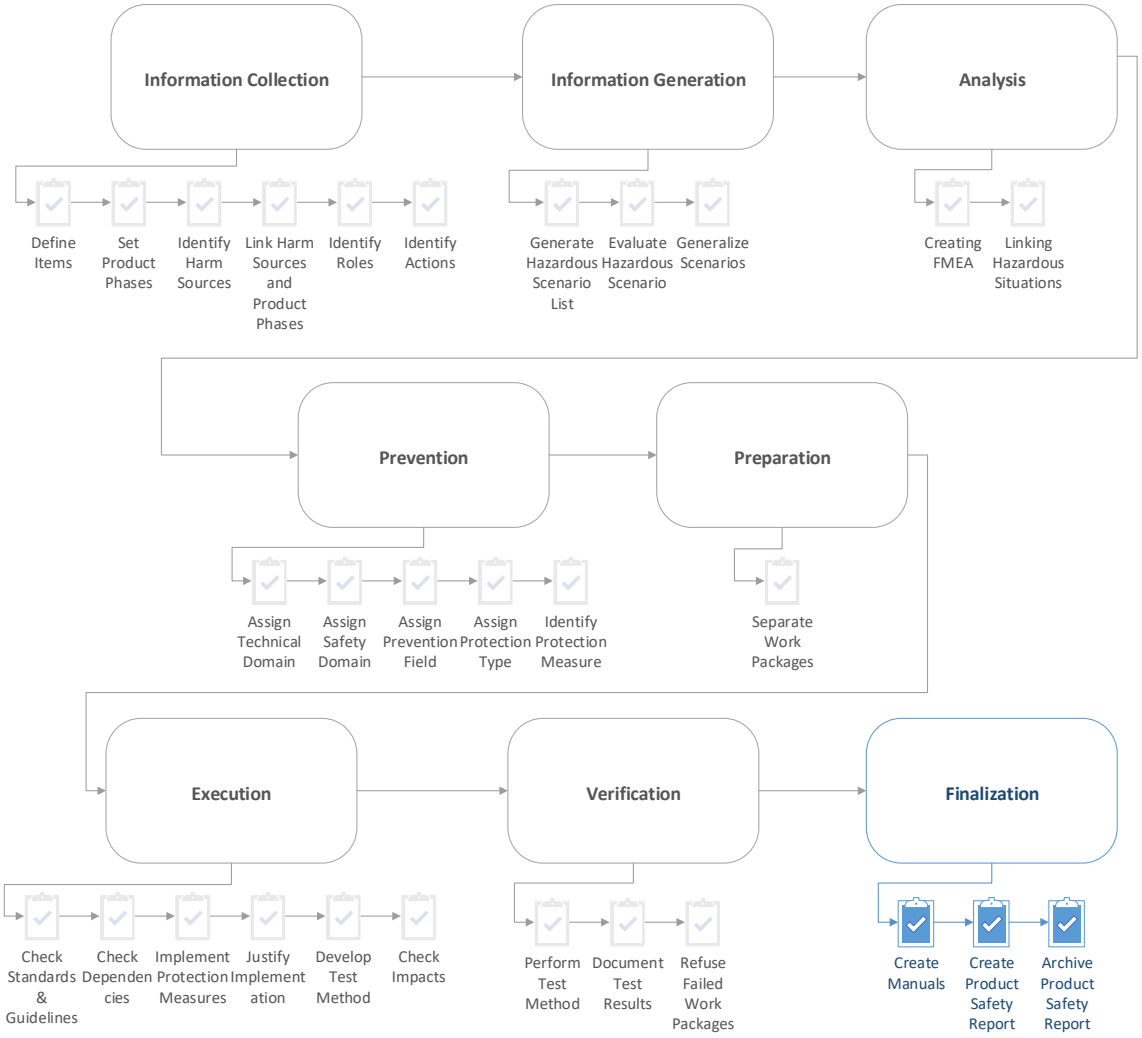


Figure 4.48: General overview of the *Finalization* phase.

4.9.1 General Overview

The last phase of the product safety process is about centralizing the individual files and reports to a single document called *Product Safety Report*. This files the work for future purposes like an inspection. Furthermore this step assists in the writing of the manuals for different product phases. This last step is necessary to complete the safety of the product within all *Product Phases* and all *Safety Domains*.

4.9.2 Input

The input of this phase are the following information from the previous phases:

- *Item* definition
- Guidelines & Standards
- *Hazardous Situation List*
- *EFMEA*
- *Design Document*
- *Test Document*

4.9.3 Activity

To support the engineer the following guideline can be used to understand how this phase has to be performed:

1. Create Manuals
    - Service
    - Manufacturing
    - Operation
    - Decommissioning
    - Crash
2. Create *Product Safety Report*
3. Archive *Product Safety Report*

Create Manuals

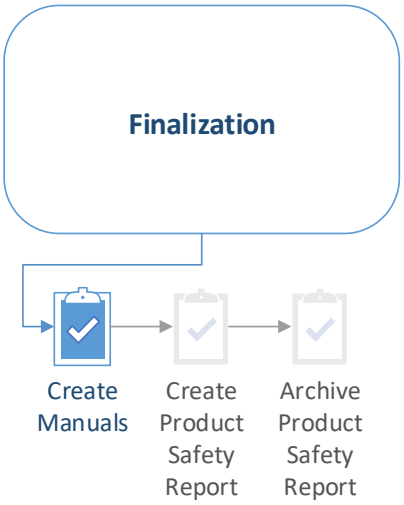


Figure 4.49: Create manuals in the *Finalization* phase.

One of the requested *Safety Domains* is the Safety of Use. This domain considers the *Role* and their *Action*. During the product safety process *Protection Measures* are defined that include instructions about the behavior of the *Roles* to ensure safety. This information needs to be communicated to the different *Roles*. Therefore different manuals are written:

- Service
- Manufacturing
- Operation
- Decommissioning
- Crash

This manuals are very important to ensure product safety and should be written carefully with all relevant information.

Create *Product Safety Report*

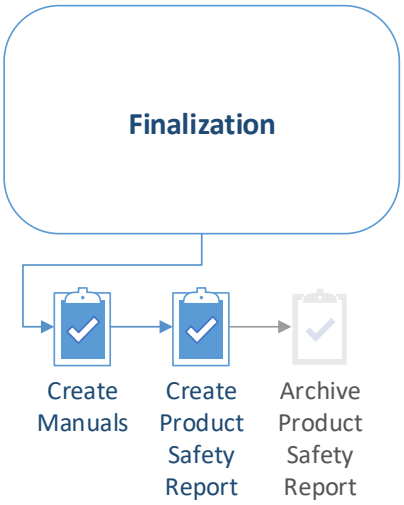


Figure 4.50: Create *Product Safety Report* in the *Finalization* phase.

Traceability is important for the automotive domain. The *Product Safety Report* ensures this quality and collects all information from the whole product safety process[Heg11]. This document summarizes the whole development process in a single file[Heg11]. This idea has already been introduced by the Medical Product Industry as mentioned in the Section 2.5.3 on Page 15.

Archive *Product Safety Report*

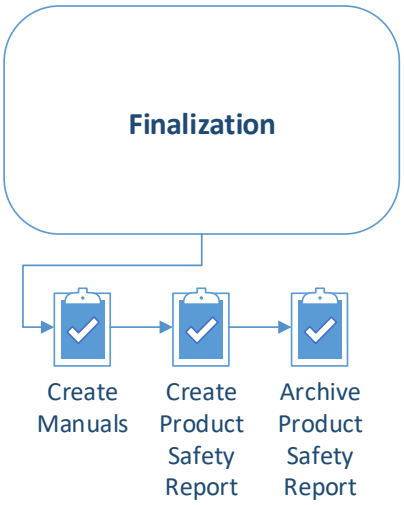


Figure 4.51: Archive the *Product Safety Report* in the *Finalization* phase.

It is necessary to keep this document as long as possible because it will be checked if any investigations arise. It is important to make backups of this report and ensure the availability of this document.

4.9.4 Output

The last phase ensures on the one hand the evidence that the product is safe and on the other hand the *Product Safety Report* with the details about the product safety. Furthermore this last step also creates the *Roles* manuals for different *Product Phases*.

- Safe Product
- *Product Safety Report*
- Manuals for all different *Product Phases*

4.9.5 Process Procedure

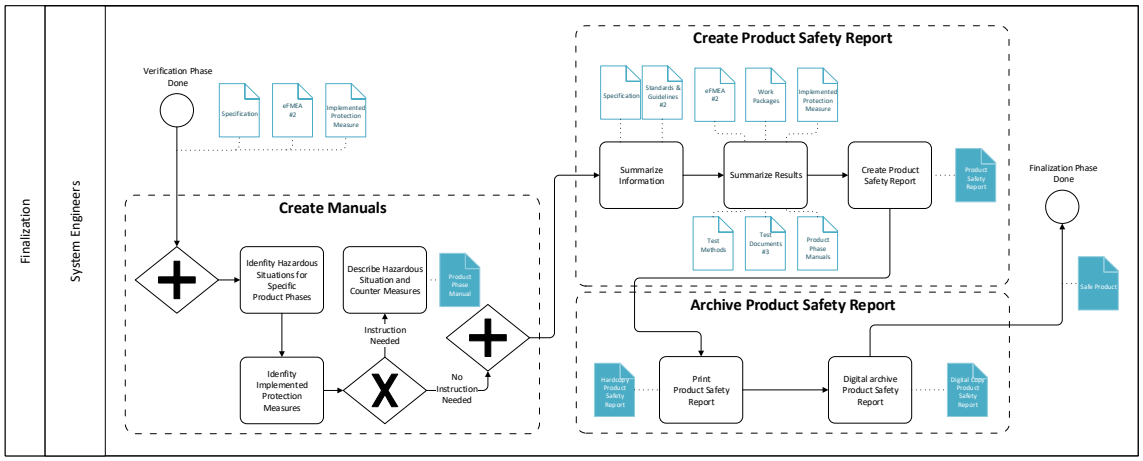


Figure 4.52: *BPMN* Process Procedure Overview of the *Finalization* phase.

Chapter 5

Practical Part & Results

This chapter is about the practical execution of the product safety method described in **Chapter 4** and is about an easy example of a HV Battery System. This system does not provide an exhaustive list of all possible failures and causes. It provides an overview of the method. The detailed *EFMEA* can be seen under section A on page 104. It is important to understand that the *FMEA* does not contain all necessary parts. Non important parts for this thesis have been omitted like detection or preventive action, severity, risk priority number and others. The reason is to give an overview about the method and this parts are not necessary to show the benefits of the new developed product safety method. The introduced method uses ideas from other industries and any cross-references can be found in the theoretical section of the Product Safety Methodology in Section 4 on Page 22.

5.1 Information Collection

The first phase of the product safety method is about the *Information Collection* further information on the execution on this phase can be found in Section 4.2 on Page 26.

5.1.1 Define *Items*

The first step is about the *Item* definition, further theoretical information and cross-references to related work can be consulted in Section 4.2.3 on Page 28. In this example a simple HV Battery System is used because this kind of system is complex and includes different *Technical Domains* as mentioned in Section 2.1.3 on Page 7 and different *Safety Domains* as mentioned in Section 2.1.4 on Page 8.

Overview	Name	Description
Item	HV Battery	The HV Battery system provides energy to drive fully or partially electrical vehicles. The system provides energy to the powertrain. Furthermore the battery system provides energy to all electrical components of the vehicle.

Requirements	Name	Description
Functional	Charging the battery system	The battery system should be chargeable with a common plug-in charger.
	Discharging	Providing energy to the powertrain and other electrical components
Non-Functional	Chemical Safety	No chemical injuries due to leakages
	Electrical Safety	No electrical shock to operators
	Thermal Safety	No thermal injuries like fire or heated surfaces
	Mechanical Safety	No mechanical injuries like sharp edges or crushing body parts

Environmental Conditions	Min	Max
Temperature	-40°C	+80°C
Humidity	0%	100%
Pressure	550hPa	2000hPa

Expected Countries and Regions
European Union

Figure 5.1: *Item* definition of the basic HV battery system example.

A selection of related standards and guidelines for this example can be found in Section 2.6 on Page 18.

5.1.2 Set *Product Phases*

The second step is about the *Product Phase* definition, further theoretical information and cross-references to related work can be consulted in section 4.2.3 on page 29. In this example the most basic *Product Phases* have been selected to keep the example simple and comprehensible.

Identify Product Phases	Consider
Manufacturing	x
Development	
Crash	x
Repair/Maintenance	x
2nd Life Repair/Maintencance	
Installation	
Transport	x
Storage	
Operation	x
2nd Life Operation	
Decomissioning	

Figure 5.2: *Product Phase* definition of the basic HV battery system example.

5.1.3 Identify *Harm Sources* and Link *Harm Sources* with *Product Phases*

The third and fourth steps are about identifying the related *Harm Sources* to the *Items* that are defined in Section 5.1.1 on Page 70. In this example the different *Harm Sources* have been identified and linked to the *Product Phases*, further theoretical information and cross-references to related work can be consulted in Section 4.2.3 on Page 31.

Harm Source	Electrical Shock	Electrical Coursed Fire	Chemical	Thermal	Mechanical
HV Battery					
Product Phases	Manufacturing	Manufacturing	Manufacturing	Manufacturing	Manufacturing
	Crash	Crash	Crash	Crash	Crash
	Repair/Maintenance	Repair/Maintenance	Repair/Maintenance	Repair/Maintenance	Repair/Maintenance
	Transport	Transport	Transport	Transport	Transport
	Operation	Operation	Operation	Operation	Operation

Figure 5.3: *Harm Source* definition of the basic HV battery system example.

5.1.4 Identify *Roles*

The fifth step is about identifying the *Roles* that will operate with the *Items* that are defined in Section 5.1.1 on Page 70. In this example the identified *Roles* have been reduced to ensure a comprehensible overview. Furthermore this example used the provided table with a basic overview about *Roles* in the automotive domain, further theoretical information and cross-references to related work can be consulted in Section 4.2.3 on Page 32.

Roles	Operation	Crash	Repair/Maintenance	Transport	Manufacturing
Driver	X	X			
Road users	X	X			
Aides		X			
Domain variant Worker			X	X	
Fully-Trained Worker			X		X

Figure 5.4: *Role* identification of the basic HV battery system example.

5.1.5 Identify *Actions*

The last step of the *Information Collection* phase is about identifying the *Actions* of the different *Roles*. To keep the example small and comprehensible the identified actions are concise, further theoretical information and cross-references to related work can be consulted in Section 4.2.3 on Page 33.

Product Phase	Operation	
Role	**Driver**	**Road users**
Action	driving	remaining passive
Action	charging	

Product Phase	Crash		
Role	**Driver**	**Road users**	**Aides**
Action	exiting	first aiding	first aiding
Action	unconscious	rescuing	rescuing
		remaining passive	

Product Phase	Repair/Maintenance	
Role	**Domain variant Worker**	**Fully-Trained Worker**
Action	opening	repairing

Product Phase	Transport
Role	**Domain variant Worker**
Action	transporting
Action	loading

Product Phase	Manufacturing
Role	**Fully-Trained Worker**
Action	assembling
Action	testing

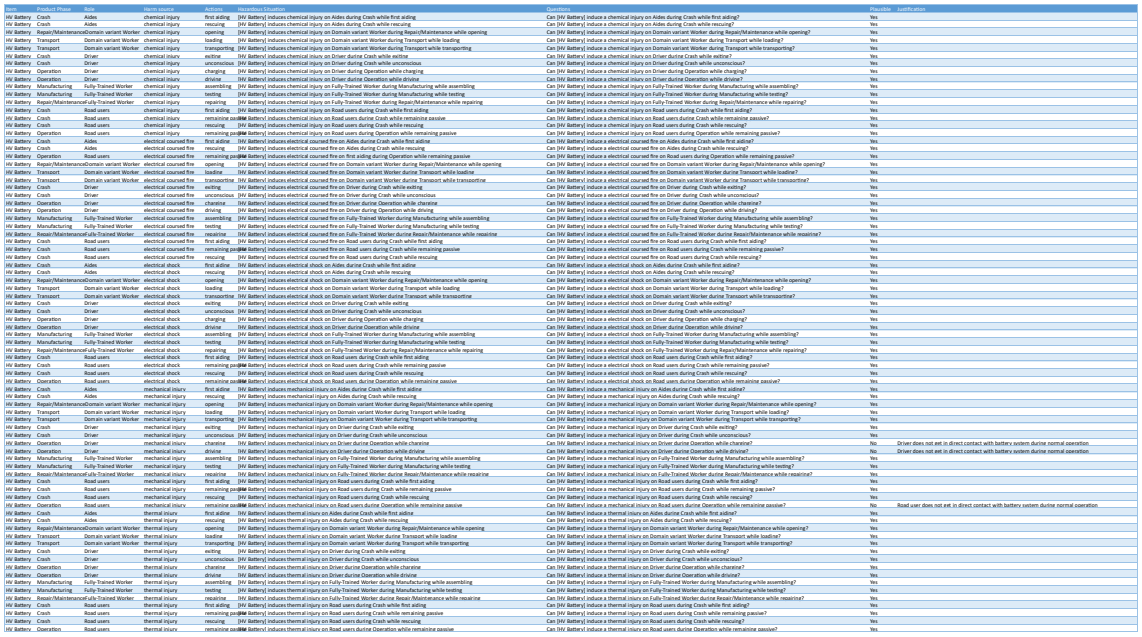
Figure 5.5: *Action* identification of the basic HV battery system example.

5.2 Information Generation

The second phase of the product safety method is about the *Information Generation*, further information can be found in section 4.2 on page 26.

5.2.1 Generate *Hazardous Situation List*

The first step is about the generation of the *Hazardous Situation List*. This method is described theoretical and all cross-references about related work can be found in Section 4.3.3 on Page 38.



Item	Product Phase	Role	Main Hazard	Function	Malfunction	Hazard	Plausible	Justification
HV Battery	Crash	Aides	chemical injury	first aiding	[HV Battery] induces chemical injury on Aides during Crash while first aiding	Can [HV Battery] induce a chemical injury on Aides during Crash while first aiding?	Yes	
HV Battery	Crash	Aides	chemical injury	rescuing	[HV Battery] induces chemical injury on Aides during Crash while rescuing	Can [HV Battery] induce a chemical injury on Aides during Crash while rescuing?	Yes	
HV Battery	Repair/Maintenance	Domain variant Worker	chemical injury	opening	[HV Battery] induces chemical injury on Domain variant Worker during Repair/Maintenance while opening	Can [HV Battery] induce a chemical injury on Domain variant Worker during Repair/Maintenance while opening?	Yes	
HV Battery	Transport	Domain variant Worker	chemical injury	loading	[HV Battery] induces chemical injury on Domain variant Worker during Transport while loading	Can [HV Battery] induce a chemical injury on Domain variant Worker during Transport while loading?	Yes	
HV Battery	Transport	Domain variant Worker	chemical injury	transporting	[HV Battery] induces chemical injury on Domain variant Worker during Transport while transporting	Can [HV Battery] induce a chemical injury on Domain variant Worker during Transport while transporting?	Yes	
HV Battery	Crash	Driver	chemical injury	exiting	[HV Battery] induces chemical injury on Driver during Crash while exiting	Can [HV Battery] induce a chemical injury on Driver during Crash while exiting?	Yes	
HV Battery	Crash	Driver	chemical injury	unconscious	[HV Battery] induces chemical injury on Driver during Crash while unconscious	Can [HV Battery] induce a chemical injury on Driver during Crash while unconscious?	Yes	
HV Battery	Operation	Driver	chemical injury	charging	[HV Battery] induces chemical injury on Driver during Operation while charging	Can [HV Battery] induce a chemical injury on Driver during Operation while charging?	Yes	
HV Battery	Operation	Driver	chemical injury	driving	[HV Battery] induces chemical injury on Driver during Operation while driving	Can [HV Battery] induce a chemical injury on Driver during Operation while driving?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	chemical injury	assembling	[HV Battery] induces chemical injury on Fully-Trained Worker during Manufacturing while assembling	Can [HV Battery] induce a chemical injury on Fully-Trained Worker during Manufacturing while assembling?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	chemical injury	testing	[HV Battery] induces chemical injury on Fully-Trained Worker during Manufacturing while testing	Can [HV Battery] induce a chemical injury on Fully-Trained Worker during Manufacturing while testing?	Yes	
HV Battery	Repair/Maintenance	Fully-Trained Worker	chemical injury	repairing	[HV Battery] induces chemical injury on Fully-Trained Worker during Repair/Maintenance while repairing	Can [HV Battery] induce a chemical injury on Fully-Trained Worker during Repair/Maintenance while repairing?	Yes	
HV Battery	Crash	Road users	chemical injury	first aiding	[HV Battery] induces chemical injury on Road users during Crash while first aiding	Can [HV Battery] induce a chemical injury on Road users during Crash while first aiding?	Yes	
HV Battery	Crash	Road users	chemical injury	remaining passive	[HV Battery] induces chemical injury on Road users during Crash while remaining passive	Can [HV Battery] induce a chemical injury on Road users during Crash while remaining passive?	Yes	
HV Battery	Crash	Road users	chemical injury	rescuing	[HV Battery] induces chemical injury on Road users during Crash while rescuing	Can [HV Battery] induce a chemical injury on Road users during Crash while rescuing?	Yes	
HV Battery	Operation	Road users	chemical injury	remaining passive	[HV Battery] induces chemical injury on Road users during Operation while remaining passive	Can [HV Battery] induce a chemical injury on Road users during Operation while remaining passive?	Yes	
HV Battery	Crash	Aides	electrical coursed fire	first aiding	[HV Battery] induces electrical coursed fire on Aides during Crash while first aidling	Can [HV Battery] induce a electrical coursed fire on Aides during Crash while first aidling?	Yes	
HV Battery	Crash	Aides	electrical coursed fire	rescuing	[HV Battery] induces electrical coursed fire on Aides during Crash while rescuing	Can [HV Battery] induce a electrical coursed fire on Aides during Crash while rescuing?	Yes	
HV Battery	Operation	Road users	electrical coursed fire	remaining passive	[HV Battery] induces electrical coursed fire on Road users during Operation while remaining passive	Can [HV Battery] induce a electrical coursed fire on Road users during Operation while remaining passive?	Yes	
HV Battery	Repair/Maintenance	Domain variant Worker	electrical coursed fire	opening	[HV Battery] induces electrical coursed fire on Domain variant Worker during Repair/Maintenance while opening	Can [HV Battery] induce a electrical coursed fire on Domain variant Worker during Repair/Maintenance while opening?	Yes	
HV Battery	Transport	Domain variant Worker	electrical coursed fire	loading	[HV Battery] induces electrical coursed fire on Domain variant Worker during Transport while loading	Can [HV Battery] induce a electrical coursed fire on Domain variant Worker during Transport while loading?	Yes	
HV Battery	Transport	Domain variant Worker	electrical coursed fire	transporting	[HV Battery] induces electrical coursed fire on Domain variant Worker during Transport while transporting	Can [HV Battery] induce a electrical coursed fire on Domain variant Worker during Transport while transporting?	Yes	
HV Battery	Crash	Driver	electrical coursed fire	exiting	[HV Battery] induces electrical coursed fire on Driver during Crash while exiting	Can [HV Battery] induce a electrical coursed fire on Driver during Crash while exiting?	Yes	
HV Battery	Crash	Driver	electrical coursed fire	unconscious	[HV Battery] induces electrical coursed fire on Driver during Crash while unconscious	Can [HV Battery] induce a electrical coursed fire on Driver during Crash while unconscious?	Yes	
HV Battery	Operation	Driver	electrical coursed fire	charging	[HV Battery] induces electrical coursed fire on Driver during Operation while charging	Can [HV Battery] induce a electrical coursed fire on Driver during Operation while charging?	Yes	
HV Battery	Operation	Driver	electrical coursed fire	driving	[HV Battery] induces electrical coursed fire on Driver during Operation while driving	Can [HV Battery] induce a electrical coursed fire on Driver during Operation while driving?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	electrical coursed fire	assembling	[HV Battery] induces electrical coursed fire on Fully-Trained Worker during Manufacturing while assembling	Can [HV Battery] induce a electrical coursed fire on Fully-Trained Worker during Manufacturing while assembling?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	electrical coursed fire	testing	[HV Battery] induces electrical coursed fire on Fully-Trained Worker during Manufacturing while testing	Can [HV Battery] induce a electrical coursed fire on Fully-Trained Worker during Manufacturing while testing?	Yes	
HV Battery	Repair/Maintenance	Fully-Trained Worker	electrical coursed fire	repairing	[HV Battery] induces electrical coursed fire on Fully-Trained Worker during Repair/Maintenance while repairing	Can [HV Battery] induce a electrical coursed fire on Fully-Trained Worker during Repair/Maintenance while repairing?	Yes	
HV Battery	Crash	Road users	electrical coursed fire	first aiding	[HV Battery] induces electrical coursed fire on Road users during Crash while first aiding	Can [HV Battery] induce a electrical coursed fire on Road users during Crash while first aiding?	Yes	
HV Battery	Crash	Road users	electrical coursed fire	remaining passive	[HV Battery] induces electrical coursed fire on Road users during Crash while remaining passive	Can [HV Battery] induce a electrical coursed fire on Road users during Crash while remaining passive?	Yes	
HV Battery	Crash	Road users	electrical coursed fire	rescuing	[HV Battery] induces electrical coursed fire on Road users during Crash while rescuing	Can [HV Battery] induce a electrical coursed fire on Road users during Crash while rescuing?	Yes	
HV Battery	Crash	Aides	electrical shock	first aiding	[HV Battery] induces electrical shock on Aides during Crash while first aidling	Can [HV Battery] induce a electrical shock on Aides during Crash while first aidling?	Yes	
HV Battery	Crash	Aides	electrical shock	rescuing	[HV Battery] induces electrical shock on Aides during Crash while rescuing	Can [HV Battery] induce a electrical shock on Aides during Crash while rescuing?	Yes	
HV Battery	Repair/Maintenance	Domain variant Worker	electrical shock	opening	[HV Battery] induces electrical shock on Domain variant Worker during Repair/Maintenance while opening	Can [HV Battery] induce a electrical shock on Domain variant Worker during Repair/Maintenance while opening?	Yes	
HV Battery	Transport	Domain variant Worker	electrical shock	loading	[HV Battery] induces electrical shock on Domain variant Worker during Transport while loading	Can [HV Battery] induce a electrical shock on Domain variant Worker during Transport while loading?	Yes	
HV Battery	Transport	Domain variant Worker	electrical shock	transporting	[HV Battery] induces electrical shock on Domain variant Worker during Transport while transporting	Can [HV Battery] induce a electrical shock on Domain variant Worker during Transport while transporting?	Yes	
HV Battery	Crash	Driver	electrical shock	exiting	[HV Battery] induces electrical shock on Driver during Crash while exiting	Can [HV Battery] induce a electrical shock on Driver during Crash while exiting?	Yes	
HV Battery	Crash	Driver	electrical shock	unconscious	[HV Battery] induces electrical shock on Driver during Crash while unconscious	Can [HV Battery] induce a electrical shock on Driver during Crash while unconscious?	Yes	
HV Battery	Operation	Driver	electrical shock	charging	[HV Battery] induces electrical shock on Driver during Operation while charging	Can [HV Battery] induce a electrical shock on Driver during Operation while charging?	Yes	
HV Battery	Operation	Driver	electrical shock	driving	[HV Battery] induces electrical shock on Driver during Operation while driving	Can [HV Battery] induce a electrical shock on Driver during Operation while driving?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	electrical shock	assembling	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while assembling	Can [HV Battery] induce a electrical shock on Fully-Trained Worker during Manufacturing while assembling?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	electrical shock	testing	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while testing	Can [HV Battery] induce a electrical shock on Fully-Trained Worker during Manufacturing while testing?	Yes	
HV Battery	Repair/Maintenance	Fully-Trained Worker	electrical shock	repairing	[HV Battery] induces electrical shock on Fully-Trained Worker during Repair/Maintenance while repairing	Can [HV Battery] induce a electrical shock on Fully-Trained Worker during Repair/Maintenance while repairing?	Yes	
HV Battery	Crash	Road users	electrical shock	first aiding	[HV Battery] induces electrical shock on Road users during Crash while first aiding	Can [HV Battery] induce a electrical shock on Road users during Crash while first aiding?	Yes	
HV Battery	Crash	Road users	electrical shock	remaining passive	[HV Battery] induces electrical shock on Road users during Crash while remaining passive	Can [HV Battery] induce a electrical shock on Road users during Crash while remaining passive?	Yes	
HV Battery	Crash	Road users	electrical shock	rescuing	[HV Battery] induces electrical shock on Road users during Crash while rescuing	Can [HV Battery] induce a electrical shock on Road users during Crash while rescuing?	Yes	
HV Battery	Operation	Road users	electrical shock	remaining passive	[HV Battery] induces electrical shock on Road users during Operation while remaining passive	Can [HV Battery] induce a electrical shock on Road users during Operation while remaining passive?	Yes	
HV Battery	Crash	Aides	mechanical injury	first aiding	[HV Battery] induces mechanical injury on Aides during Crash while first aidling	Can [HV Battery] induce a mechanical injury on Aides during Crash while first aidling?	Yes	
HV Battery	Crash	Aides	mechanical injury	rescuing	[HV Battery] induces mechanical injury on Aides during Crash while rescuing	Can [HV Battery] induce a mechanical injury on Aides during Crash while rescuing?	Yes	
HV Battery	Repair/Maintenance	Domain variant Worker	mechanical injury	opening	[HV Battery] induces mechanical injury on Domain variant Worker during Repair/Maintenance while opening	Can [HV Battery] induce a mechanical injury on Domain variant Worker during Repair/Maintenance while opening?	Yes	
HV Battery	Transport	Domain variant Worker	mechanical injury	loading	[HV Battery] induces mechanical injury on Domain variant Worker during Transport while loading	Can [HV Battery] induce a mechanical injury on Domain variant Worker during Transport while loading?	Yes	
HV Battery	Transport	Domain variant Worker	mechanical injury	transporting	[HV Battery] induces mechanical injury on Domain variant Worker during Transport while transporting	Can [HV Battery] induce a mechanical injury on Domain variant Worker during Transport while transporting?	Yes	
HV Battery	Driver	mechanical injury	exiting	[HV Battery] induces mechanical injury on Driver during Crash while exiting	Can [HV Battery] induce a mechanical injury on Driver during Crash while exiting?	Yes		
HV Battery	Crash	Driver	mechanical injury	unconscious	[HV Battery] induces mechanical injury on Driver during Crash while unconscious	Can [HV Battery] induce a mechanical injury on Driver during Crash while unconscious?	Yes	
HV Battery	Operation	Driver	mechanical injury	charging	[HV Battery] induces mechanical injury on Driver during Operation while charging	Can [HV Battery] induce a mechanical injury on Driver during Operation while charging?	No	Driver does not get in direct contact with battery system durine normal operation
HV Battery	Operation	Driver	mechanical injury	driving	[HV Battery] induces mechanical injury on Driver during Operation while driving	Can [HV Battery] induce a mechanical injury on Driver during Operation while driving?	No	Driver does not get in direct contact with battery system durine normal operation
HV Battery	Manufacturing	Fully-Trained Worker	mechanical injury	assembling	[HV Battery] induces mechanical injury on Fully-Trained Worker during Manufacturing while assembling	Can [HV Battery] induce a mechanical injury on Fully-Trained Worker during Manufacturing while assembling?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	mechanical injury	testing	[HV Battery] induces mechanical injury on Fully-Trained Worker during Manufacturing while testing	Can [HV Battery] induce a mechanical injury on Fully-Trained Worker during Manufacturing while testing?	Yes	
HV Battery	Repair/Maintenance	Fully-Trained Worker	mechanical injury	repairing	[HV Battery] induces mechanical injury on Fully-Trained Worker during Repair/Maintenance while repairing	Can [HV Battery] induce a mechanical injury on Fully-Trained Worker during Repair/Maintenance while repairing?	Yes	
HV Battery	Crash	Road users	mechanical injury	first aiding	[HV Battery] induces mechanical injury on Road users during Crash while first aiding	Can [HV Battery] induce a mechanical injury on Road users during Crash while first aiding?	Yes	
HV Battery	Crash	Road users	mechanical injury	remaining passive	[HV Battery] induces mechanical injury on Road users during Crash while remaining passive	Can [HV Battery] induce a mechanical injury on Road users during Crash while remaining passive?	Yes	
HV Battery	Crash	Road users	mechanical injury	rescuing	[HV Battery] induces mechanical injury on Road users during Crash while rescuing	Can [HV Battery] induce a mechanical injury on Road users during Crash while rescuing?	Yes	
HV Battery	Operation	Road users	mechanical injury	remaining passive	[HV Battery] induces mechanical injury on Road users during Operation while remaining passive	Can [HV Battery] induce a mechanical injury on Road users during Operation while remaining passive?	No	Road user does not eat in direct contact with battery system durine normal operation
HV Battery	Crash	Aides	thermal injury	first aiding	[HV Battery] induces thermal injury on Aides during Crash while first aidling	Can [HV Battery] induce a thermal injury on Aides during Crash while first aidling?	Yes	
HV Battery	Crash	Aides	thermal injury	rescuing	[HV Battery] induces thermal injury on Aides during Crash while rescuing	Can [HV Battery] induce a thermal injury on Aides during Crash while rescuing?	Yes	
HV Battery	Repair/Maintenance	Domain variant Worker	thermal injury	opening	[HV Battery] induces thermal injury on Domain variant Worker during Repair/Maintenance while opening	Can [HV Battery] induce a thermal injury on Domain variant Worker during Repair/Maintenance while opening?	Yes	
HV Battery	Transport	Domain variant Worker	thermal injury	loading	[HV Battery] induces thermal injury on Domain variant Worker during Transport while loading	Can [HV Battery] induce a thermal injury on Domain variant Worker during Transport while loading?	Yes	
HV Battery	Transport	Domain variant Worker	thermal injury	transporting	[HV Battery] induces thermal injury on Domain variant Worker during Transport while transporting	Can [HV Battery] induce a thermal injury on Domain variant Worker during Transport while transporting?	Yes	
HV Battery	Crash	Driver	thermal injury	exiting	[HV Battery] induces thermal injury on Driver during Crash while exiting	Can [HV Battery] induce a thermal injury on Driver during Crash while exiting?	Yes	
HV Battery	Crash	Driver	thermal injury	unconscious	[HV Battery] induces thermal injury on Driver during Crash while unconscious	Can [HV Battery] induce a thermal injury on Driver during Crash while unconscious?	Yes	
HV Battery	Operation	Driver	thermal injury	charging	[HV Battery] induces thermal injury on Driver during Operation while charging	Can [HV Battery] induce a thermal injury on Driver during Operation while charging?	Yes	
HV Battery	Operation	Driver	thermal injury	driving	[HV Battery] induces thermal injury on Driver during Operation while driving	Can [HV Battery] induce a thermal injury on Driver during Operation while driving?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	thermal injury	assembling	[HV Battery] induces thermal injury on Fully-Trained Worker during Manufacturing while assembling	Can [HV Battery] induce a thermal injury on Fully-Trained Worker during Manufacturing while assembling?	Yes	
HV Battery	Manufacturing	Fully-Trained Worker	thermal injury	testing	[HV Battery] induces thermal injury on Fully-Trained Worker during Manufacturing while testing	Can [HV Battery] induce a thermal injury on Fully-Trained Worker during Manufacturing while testing?	Yes	
HV Battery	Repair/Maintenance	Fully-Trained Worker	thermal injury	repairing	[HV Battery] induces thermal injury on Fully-Trained Worker during Repair/Maintenance while repairing	Can [HV Battery] induce a thermal injury on Fully-Trained Worker during Repair/Maintenance while repairing?	Yes	
HV Battery	Crash	Road users	thermal injury	first aiding	[HV Battery] induces thermal injury on Road users during Crash while first aiding	Can [HV Battery] induce a thermal injury on Road users during Crash while first aiding?	Yes	
HV Battery	Crash	Road users	thermal injury	remaining passive	[HV Battery] induces thermal injury on Road users during Crash while remaining passive	Can [HV Battery] induce a thermal injury on Road users during Crash while remaining passive?	Yes	
HV Battery	Crash	Road users	thermal injury	rescuing	[HV Battery] induces thermal injury on Road users during Crash while rescuing	Can [HV Battery] induce a thermal injury on Road users during Crash while rescuing?	Yes	
HV Battery	Operation	Road users	thermal injury	remaining passive	[HV Battery] induces thermal injury on Road users during Operation while remaining passive	Can [HV Battery] induce a thermal injury on Road users during Operation while remaining passive?	Yes	

Figure 5.6: *Hazardous Situation List* generation of the basic HV battery system example.

5.2.2 Evaluate *Hazardous Situation List*

The second step is about the evaluation of the *Hazardous Situation List*. This method is described theoretical and all cross-references about related work can be found in Section 4.3.3 on Page 39.

Hazardous Situation	Plausible	Justification
[HV Battery] induces mechanical injury on Driver during Operation while charging	No	Driver does not get in direct contact with battery system during normal operation
[HV Battery] induces mechanical injury on Driver during Operation while driving	No	Driver does not get in direct contact with battery system during normal operation

Figure 5.7: *Hazardous Situation List* evaluation of the basic HV battery system example.

The chosen example gives a good point of view why the plausibility check is necessary. In this example it is not possible that the driver gets in contact with the battery system during driving.

5.2.3 Generalize *Hazardous Situation List*

This step has been omitted because the identified *Roles* are already simple and generalized. Further information can be found in section 4.3.3 on page 40.

5.3 Analysis

The third phase of the product safety method is the *Analysis* phase of possible failures and risks, further theoretical information and cross-references to related work can be consulted in Section 4.2 on Page 26. The following tables are an excerpt and can help the experts during the failure and risk analysis in the *FMEA* and can easily be created in Excel using its pivot feature:

Hazardous Situations List (Sorted by Items and Injury Type)
HV Battery
chemical injury
[HV Battery] induces chemical injury on Aides during Crash while first aiding
[HV Battery] induces chemical injury on Aides during Crash while rescuing
[HV Battery] induces chemical injury on Domain variant Worker during Repair/Maintenance while opening
[HV Battery] induces chemical injury on Domain variant Worker during Transport while loading
[HV Battery] induces chemical injury on Domain variant Worker during Transport while transporting
[HV Battery] induces chemical injury on Driver during Crash while exiting
[HV Battery] induces chemical injury on Driver during Crash while unconscious
[HV Battery] induces chemical injury on Fully-Trained Worker during Manufacturing while assembling
[HV Battery] induces chemical injury on Fully-Trained Worker during Manufacturing while testing
[HV Battery] induces chemical injury on Fully-Trained Worker during Repair/Maintenance while repairing
[HV Battery] induces chemical injury on Road users during Crash while first aiding
[HV Battery] induces chemical injury on Road users during Crash while rescuing
[HV Battery] induces chemical injury on Driver during Operation while driving
[HV Battery] induces chemical injury on Driver during Operation while charging
[HV Battery] induces chemical injury on Road users during Operation while remaining passive
[HV Battery] induces chemical injury on Road users during Crash while remaining passive
electrical coursed fire
[HV Battery] induces electrical coursed fire on Aides during Crash while first aiding
[HV Battery] induces electrical coursed fire on Aides during Crash while rescuing
[HV Battery] induces electrical coursed fire on Domain variant Worker during Repair/Maintenance while opening
[HV Battery] induces electrical coursed fire on Domain variant Worker during Transport while loading
[HV Battery] induces electrical coursed fire on Domain variant Worker during Transport while transporting
[HV Battery] induces electrical coursed fire on Driver during Crash while exiting
[HV Battery] induces electrical coursed fire on Driver during Crash while unconscious
[HV Battery] induces electrical coursed fire on Fully-Trained Worker during Manufacturing while assembling
[HV Battery] induces electrical coursed fire on Fully-Trained Worker during Manufacturing while testing
[HV Battery] induces electrical coursed fire on Fully-Trained Worker during Repair/Maintenance while repairing
[HV Battery] induces electrical coursed fire on Road users during Crash while first aiding

Figure 5.8: *Hazardous Situation List* separated by different *Harm Sources* to support the engineers.

Hazardous Situations Questions (Sorted by Items and Injury Type)
HV Battery
chemical injury
Can [HV Battery] induce a chemical injury on Aides during Crash while first aiding?
Can [HV Battery] induce a chemical injury on Aides during Crash while rescuing?
Can [HV Battery] induce a chemical injury on Domain variant Worker during Repair/Maintenance while opening?
Can [HV Battery] induce a chemical injury on Domain variant Worker during Transport while loading?
Can [HV Battery] induce a chemical injury on Domain variant Worker during Transport while transporting?
Can [HV Battery] induce a chemical injury on Driver during Crash while exiting?
Can [HV Battery] induce a chemical injury on Driver during Crash while unconscious?
Can [HV Battery] induce a chemical injury on Driver during Operation while charging?
Can [HV Battery] induce a chemical injury on Driver during Operation while driving?
Can [HV Battery] induce a chemical injury on Fully-Trained Worker during Manufacturing while assembling?
Can [HV Battery] induce a chemical injury on Fully-Trained Worker during Manufacturing while testing?
Can [HV Battery] induce a chemical injury on Fully-Trained Worker during Repair/Maintenance while repairing?
Can [HV Battery] induce a chemical injury on Road users during Crash while first aiding?
Can [HV Battery] induce a chemical injury on Road users during Crash while remaining passive?
Can [HV Battery] induce a chemical injury on Road users during Crash while rescuing?
Can [HV Battery] induce a chemical injury on Road users during Operation while remaining passive?
electrical coursed fire
Can [HV Battery] induce a electrical coursed fire on Aides during Crash while first aiding?
Can [HV Battery] induce a electrical coursed fire on Aides during Crash while rescuing?
Can [HV Battery] induce a electrical coursed fire on Domain variant Worker during Repair/Maintenance while opening?
Can [HV Battery] induce a electrical coursed fire on Domain variant Worker during Transport while loading?
Can [HV Battery] induce a electrical coursed fire on Domain variant Worker during Transport while transporting?
Can [HV Battery] induce a electrical coursed fire on Driver during Crash while exiting?
Can [HV Battery] induce a electrical coursed fire on Driver during Crash while unconscious?
Can [HV Battery] induce a electrical coursed fire on Driver during Operation while charging?
Can [HV Battery] induce a electrical coursed fire on Driver during Operation while driving?
Can [HV Battery] induce a electrical coursed fire on Fully-Trained Worker during Manufacturing while assembling?
Can [HV Battery] induce a electrical coursed fire on Fully-Trained Worker during Manufacturing while testing?
Can [HV Battery] induce a electrical coursed fire on Fully-Trained Worker during Repair/Maintenance while repairing?
Can [HV Battery] induce a electrical coursed fire on Road users during Crash while first aiding?
Can [HV Battery] induce a electrical coursed fire on Road users during Crash while remaining passive?
Can [HV Battery] induce a electrical coursed fire on Road users during Crash while rescuing?

Figure 5.9: *Hazardous Situation List* separated by different *Harm Sources* to support the engineers in question form.

5.3.1 Create FMEA and Link Hazardous Situations

The step is about creating links between the *Hazardous Situation List* and the identified failures in the *FMEA*, further theoretical information and cross-references to related work can be consulted in Section 4.4.3 on Page 43 and in Section 4.4.3 on Page 44.

Failure	Effects	Causes
Battery cells accessible although case is closed	Electrical shock	Battery case damaged
Battery cells accessible although case is closed	Electrical shock	Battery case damaged
Battery cells accessible although case is closed	Electrical shock	Battery case damaged
Battery cells accessible although case is closed	Electrical shock	Battery case damaged
Battery cells accessible although case is closed	Electrical shock	Battery case damaged
Battery cells accessible although case is closed	Electrical shock	Battery case damaged
Battery cells accessible although case is closed	Electrical shock	Battery case damaged

Hazardous Situation
[HV Battery] induces electrical shock on Aides during Crash while rescuing
[HV Battery] induces electrical shock on Domain variant Worker during Transport while loading
[HV Battery] induces electrical shock on Domain variant Worker during Transport while transporting
[HV Battery] induces electrical shock on Driver during Crash while exiting
[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while testing
[HV Battery] induces electrical shock on Fully-Trained Worker during Repair/Maintenance while repairing
[HV Battery] induces electrical shock on Road users during Crash while rescuing

Figure 5.10: Short excerpt of the linking list of *Hazardous Situation List* and *FMEA*.

The full list can be found in section A on page 104.

5.4 Prevention

The fourth phase of the product safety method is the *Prevention* phase, this includes the selection of the domains as well as specifying *Protection Measures*. Further

theoretical information and cross-references to related work can be consulted in Section 4.5 on Page 46.

Failure	Causes	Hazardous Situation	Safety Domain	Technical Domain
Battery cells accessible although case is closed	Battery case damaged	[HV Battery] induces electrical shock on Aides during Crash while rescuing	Component Safety	Mechanical
Protection Domain	**Protection Type**	**Protection Measure**	**Protection Measure Details**	
Technical	Equipment	Stiffness Battery Case	Increase Stiffness of case to ensure sealing after crash	

Failure	Causes	Hazardous Situation	Safety Domain	Technical Domain
Battery cells accessible although case is closed	Battery case damaged	[HV Battery] induces electrical shock on Domain variant Worker during Transport while loading	Component Safety	Mechanical
Protection Domain	**Protection Type**	**Protection Measure**	**Protection Measure Details**	
Technical	Equipment	Stiffness Battery Case	Stiffness good enough to fullfill typical transport conditions	

Failure	Causes	Hazardous Situation	Safety Domain	Technical Domain
Battery cells accessible although case is closed	Battery case damaged	[HV Battery] induces electrical shock on Domain variant Worker during Transport while transporting	Component Safety	Mechanical
Protection Domain	**Protection Type**	**Protection Measure**	**Protection Measure Details**	
Technical	Equipment	Stiffness Battery Case	Stiffness good enough to fullfill typical transport conditions	

Figure 5.11: Short excerpt of the domain assigning of the *EFMEA*.

5.5 Preparation

The fifth phase of the product safety method is the *Preparation* phase, leading up to separated *Work Packages*. Further theoretical information and cross-references to related work can be consulted in Section 4.6 on Page 52.

Technical Domain	Protection Domain	Protection Type	Protection Measure
Safety of Use	Electrical	Personal	Protection

Protection Measure Details	Protection Measure Details
Personal Protection	HV Gloves as additional safety measure

Failure	Effects	Causes	Hazardous Situation
Battery cells accessible although case is closed	Electrical shock	Battery case damaged	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while testing
Battery cells accessible although case is closed	Electrical shock	Battery case damaged	[HV Battery] induces electrical shock on Fully-Trained Worker during Repair/Maintenance while repairing
Connector got loose	Isolation fails	Connection not stable enough	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while testing
Connector got loose	Isolation fails	Connector breaking down	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while testing
Cooling system leakage	Thermal event/Electrical shock	Mechanical connection breaking down	[HV Battery] induces electrical shock on Domain variant Worker during Repair/Maintenance while opening
Cooling system leakage	Thermal event/Electrical shock	Mechanical connection breaking down	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while assembling
Cooling system leakage	Thermal event/Electrical shock	Mechanical stress through thermal expansion	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while assembling
Cooling system leakage	Thermal event/Electrical shock	Mechanical connection breaking down	[HV Battery] induces electrical shock on Fully-Trained Worker during Manufacturing while testing

Figure 5.12: Example for a single *Work Package* as result of the *Preparation* phase.

5.5.1 Pivot Analysis

After the assigning of the different domains it is possible to derive tables from the information to provide checklists for the project manager to control the implementation process or to give an overview which measures are covering what kind of *Hazardous Situations*. Some examples are given in the next sections.

Overview *Failures* and Related Scenarios

Overview Failures and the Related Scenarios	Amount of Scenarios
Battery cells accessible although case is closed	7
Communication between BMS and TMS	26
Condensation on inner components	13
Connector got loose	14
Cooling system leakage	34
Electrical contacts deformed	6
HV unintendely provided	16
Inpropriate Cell Temperature	39
Intrusion of foreign matter	22
Loosening of the mechanical connection to the vehicle	4
Mechanical deformation	13
Not enough power for BMS	13
Opening does not interrupt circuit	5
Overcurrent uninterruptable	13
Overheating	28
Service operation not safe in use	2
Short circuit	13
Unequally distributed cooling temperature	26
Unintended venting	23
Voltage potential difference between vehicle and battery casing	2
Wrong current measurement	26
Wrong temperature measurement	26
Wrong voltage measurement	26
Total Scenarios covered	**397**

Figure 5.13: Example #1 of a pivot table derived from the analysis.

This overview shows the individual *Failures* and how many possible *Hazardous Situations* that *Failure* can trigger. It provides a possibility to find out what *Failures* are more critical than others.

Overview *Protection Measures* and Related Scenarios

Overview Protection Measures and related scenarios
Battery Case Brackets
[HV Battery] induces mechanical injury on Driver during Crash while unconscious
[HV Battery] induces mechanical injury on Road users during Crash while remaining passive
Battery Case Fixation
[HV Battery] induces mechanical injury on Driver during Crash while unconscious
[HV Battery] induces mechanical injury on Road users during Crash while remaining passive
Cell Structure
[HV Battery] induces thermal injury on Aides during Crash while rescuing
[HV Battery] induces thermal injury on Domain variant Worker during Repair/Maintenance while opening
[HV Battery] induces thermal injury on Domain variant Worker during Transport while loading
[HV Battery] induces thermal injury on Domain variant Worker during Transport while transporting
[HV Battery] induces thermal injury on Driver during Crash while exiting
[HV Battery] induces thermal injury on Driver during Crash while unconscious
[HV Battery] induces thermal injury on Driver during Operation while charging
[HV Battery] induces thermal injury on Driver during Operation while driving
[HV Battery] induces thermal injury on Fully-Trained Worker during Manufacturing while testing
[HV Battery] induces thermal injury on Fully-Trained Worker during Repair/Maintenance while repairing
[HV Battery] induces thermal injury on Road users during Crash while remaining passive
[HV Battery] induces thermal injury on Road users during Crash while rescuing
[HV Battery] induces thermal injury on Road users during Operation while remaining passive
Contacts Isolation
[HV Battery] induces electrical shock on Domain variant Worker during Transport while loading
Cooling System
EMC Compatibility
Enclosure Cables
HV Disconnect
HV Fuse
Instruction
Insulation monitoring device
Manual Shut-Off
Organisation
Personal Protection
Position
Sealed
Sealing Case
Shut-Off
Stiffness Battery Case
Stiffness Cooling system
Transport Brackets
Warning

Figure 5.14: Example #2 of a pivot table derived from the analysis.

This overview shows the individual *Protection Measures* and what kind of possible *Hazardous Situations* they can catch and safe.

Overview *Protection Types*, *Product Phases* and *Protection Measure* Details

Overview Protection Type, Product Phases and Protection Measures Details
Equipment
Crash
Manufacturing
Operation
Repair/Maintenance
Battery case is sealed and can not be opened with common tools
Battery case stiff enough and sealed to fullfill the requirements of IP6K7
Battery must be hermetically sealed
Battery shut-off if connection lost
Enclosure must handle all stress of typical repairing conditions
HV Fuse will cut off overcurrent
Increase cooling if possible or shutdown
Place vent that there is no other heated surface next to it
Stiffness good enough to fullfill typical repairing conditions
Use EUCAR Hazard Level 4 Cells
xCU must fullfill all requirements of EMC for automotive domain
Transport
Installation
Manufacturing
Repair/Maintenance
Battery case is sealed and can not be opened with common tools
Transport
Instructional
Crash
Operation
Repair/Maintenance
Describe how to treat the system properly
Protection
Manufacturing
Repair/Maintenance
Chemical resistant gloves as additional safety measure
Fire-Extinguisher as additional safety measure
HV Gloves as additional safety measure
Training
Repair/Maintenance
Battery will be shut-off manually by mechanic

Figure 5.15: Example #3 of a pivot table derived from the analysis.

This overview shows what requirements are needed for the *Protection Measures* to ensure a safe product. This view is divided into different *Product Phases* and *Protection Types*.

Overview *Safety Domains* and *Protection Measures*

Overview Safety Domains and the protection measures
Component Safety
Battery Case Brackets
Battery Case Fixation
Cell Structure
EMC Compatibility
Enclosure Cables
Organisation
Position
Sealed
Sealing Case
Stiffness Battery Case
Stiffness Cooling system
Transport Brackets
Functional Safety
Cooling System
HV Fuse
Insulation monitoring device
Sealed
Safety of Use
Contacts Isolation
HV Disconnect
Instruction
Manual Shut-Off
Personal Protection
Sealed
Shut-Off
Stiffness Battery Case
Warning

Figure 5.16: Example #4 of a pivot table derived from the analysis.

This overview shows what *Safety Domains* are present and what *Protection Measures* have to be implemented to cover the specific *Safety Domain* and ensure product safety.

Overview *Technical Domains*, *Protection Measures* and the Related *Hazardous Situation*

Overview Technical Domains with Measures and Related Scenarios	Amount of Scenarios
Chemical	**112**
Cell Structure	109
Organisation	1
Personal Protection	2
Electrical	**138**
Contacts Isolation	1
EMC Compatibility	13
HV Disconnect	2
HV Fuse	7
Insulation monitoring device	6
Personal Protection	21
Sealed	3
Shut-Off	83
Warning	2
Mechanical	**108**
Battery Case Brackets	2
Battery Case Fixation	2
Cooling System	7
Enclosure Cables	30
Instruction	1
Manual Shut-Off	2
Position	3
Sealed	19
Sealing Case	8
Stiffness Battery Case	25
Stiffness Cooling system	7
Transport Brackets	2
Thermal	**39**
Personal Protection	27
Position	12
Total Scenarios covered	**397**

Figure 5.17: Example #5 of a pivot table derived from the analysis.

This overview shows what *Protection Measures* cover how many *Hazardous Situations* and is sorted by *Technical Domains*.

Overview *Technical Domains* and the *Protection Measures*

Overview Technical Domains and the Protection Measures with Details
Chemical
Cell Structure
Use EUCAR Hazard Level 4 Cells
Organisation
Cleanroom
Personal Protection
Chemical resistant gloves as additional safety measure
Electrical
Contacts Isolation
Isolate contacts during transport
EMC Compatibility
xCU must fullfill all requirements of EMC for automotive domain
HV Disconnect
HV Disconnect warn the driver
HV Fuse
HV Fuse will cut off overcurrent
Insulation monitoring device
Battery shut-off if connection lost
Personal Protection
HV Gloves as additional safety measure
Sealed
Battery case is sealed and can not be opened with common tools
Shut-Off
Battery will shut-off after a crash and this not possible anymore
Warning
Warn driver that HV is unintendely provided
Mechanical
Thermal

Figure 5.18: Example #6 of a pivot table derived from the analysis.

This overview shows what kind of *Protection Measures* have to be implemented by the different *Technical Domains* and can be used as a checklist to check the project progress.

5.6 Execution and Verification

This phases have been skipped because this example is a theoretical approach to provide an overview about the product safety method and what is possible. Further theoretical information can be found in section 4.7 on page 55 and in Section 4.8 on Page 61.

5.7 Finalization

In the last phase of the product safety method the whole process gets documented and archived. The first step is about creating manuals. For this purpose the pivot table 5.5.1 on Page 83 can be used. There is an overview about different *Protection Types* that have to be handled by the different *Roles* in the specific situations. This can be used to understand what kind of information is needed for the manual to ensure a safe product.

For example in this case the following information needs to be part of the Service Manual:

- Protection Equipment
  - HV Gloves (Chemical Resistant)
  - Fire-Extinguisher
- Instruction
  - Manual Shut-Off of Battery System

This information is needed for the specific *Role* and the specific *Product Phase* to ensure safety. The manufacturer must write this kind of information into the manual to ensure product safety as mentioned in Section 2.5.1 on Page 12. Furthermore it is advisable for the manufacturer to summarize all identified and investigated information into a single file. Therefore the next step is about the creation of the *Product Safety Report*. This step is described theoretically in Section 4.9 on Page 65. After this step the whole traceability is provided in a single file and can be used to prove that the developed product is safe in general. Furthermore it is reproducible how the product is designed to provide system safety and it is possible to understand how and why the implemented *Protection Measures* have been identified.

5.8 Testing Parts of the Method

The developed product safety process contains a framework for a whole project. For the first tryouts it is necessary to understand the different parts and their difficulties and possibilities. The described process is too vast in the current workflow for a safety project. Therefore the process should be separated into different methods and be partly applied in a project. The chosen project is an ongoing project about a special transport vehicle in the logistics industry. The project is focusing on an independent electrical battery system for driving.

In the beginning of the cooperation there have been several meetings with the system

engineer of this specific project from the battery department. The project has already been started and an A-Sample of the battery system has been already released to the customer. Therefore it was not possible to use the product safety process to support the development process from the beginning, neither has the item definition been finished. The specific independent electrical battery system is different to other systems and therefore totally new to the customer as well as the development department. Therefore the definition of the item proves challenging and to support this process on the customer side a special method has been developed.

5.8.1 Support the Item Definition

This project is new and different for the customer and therefore it is hard for him to specify all relevant requirements and information for the developer. Investigating the current challenges the following issues have been recognized:

- Customer has difficulties recognizing necessary safety aspects.
- Customer wants to test the system by himself but has no experience in implementation.
- Customer wants to specify what kind of regulations and standards are necessary.

These issues are problems in the specification process of the requirements for the customer, but there are also issues on the side of the developer:

- Developer does not know how this product will be treated or abused during operation.
- Developer does not know how about specific industry processes and their common work flows.

Considering the issues on both sides it seems that the weaknesses from the one party are the strengths from the other party. Therefore it is beneficial if both parties are working together to understand the environment and in specifying the requirements. Because the customer knows how this industry is working and the usual practices, on the other side is the developer an expert in developing safe electrical battery systems. Therefore the solution is a methodology where both parties can participate together in finding the requirements. The safety experts should guide the customer through all possible situations during the lifecycle of the product.

Exploring the Product Lifecycle

To support the customer in finding the requirements it is necessary to step through all different phases of the product lifecycle with all possible tasks and misuses. In

the ISO 12100 standard a list can be found with a description of exactly these circumstances. This list has been used as a starting point and a listing has been created with the following additional columns:

- **Relevant**
  This column is used because the standard is describing a general machine and there could be phases that are not relevant for this specific project.
- **Operator**
  Description of the operator that is active in this specific phase.
- **Level of Education**
  The assumed education level of the operator.
- **Activity Description**
  Detailed Description how the specific Task will be executed by the described operator.
- **Frequency**
  How often this activity will be executed (daily, monthly, yearly, ...)

This list can be used to support the customer in finding and defining the requirements that are necessary for this project to achieve a safe product.

Extract Safety Information

The next step would be that the filled list from the previous section can be used to extract all relevant information and fill them in the newly developed product safety methodology from this thesis. This information was not available at the time this thesis has been finished, therefore the information has been extracted from the existing Item definition of the B-Sample. The following basic data has been extracted:

Information	#
Product Phases	5
Harm Sources	5
Roles	4
Actions	28
Generated Hazardous Situations	155

Figure 5.19: General overview of the extracted basic data of the item definition.

5.8.2 Analysis

The analysis focuses on the thermal events and the caused thermal injuries. Thermal events are the most critical hazards in a battery system. The following analysis data has been extracted from the current Design-FMEA from the ongoing project. The allocation of *Hazardous Situations* and all other information has been made by myself. The intention is to find out how good the newly developed product safety methodology performs in a real project and how much the methodology covers.

Plausibility of generated *Hazardous Situations*

The first analysis focuses on the plausibility of the generated *Hazardous Situations*. This part is covered in section 4.3.3 on page 39 of the newly developed product safety process of this thesis.

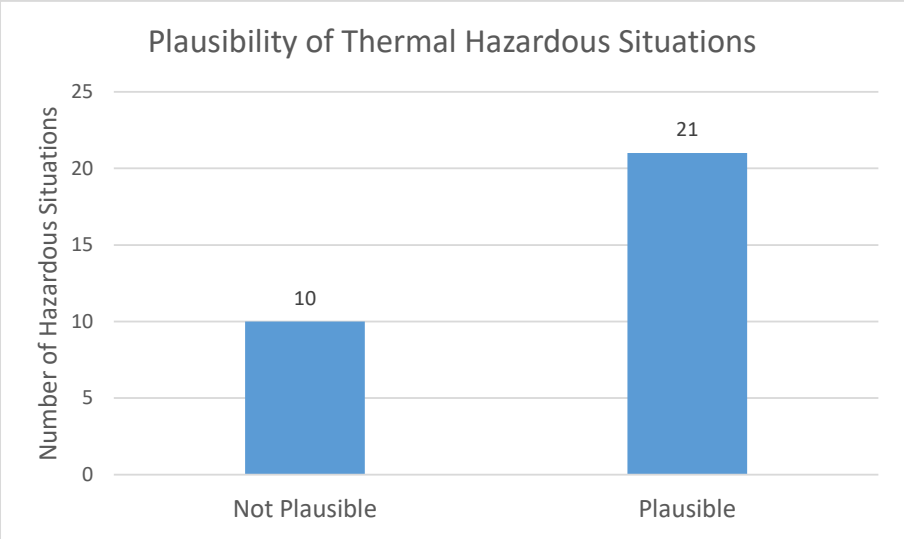


Figure 5.20: Plausibility of Thermal *Hazardous Situations*.

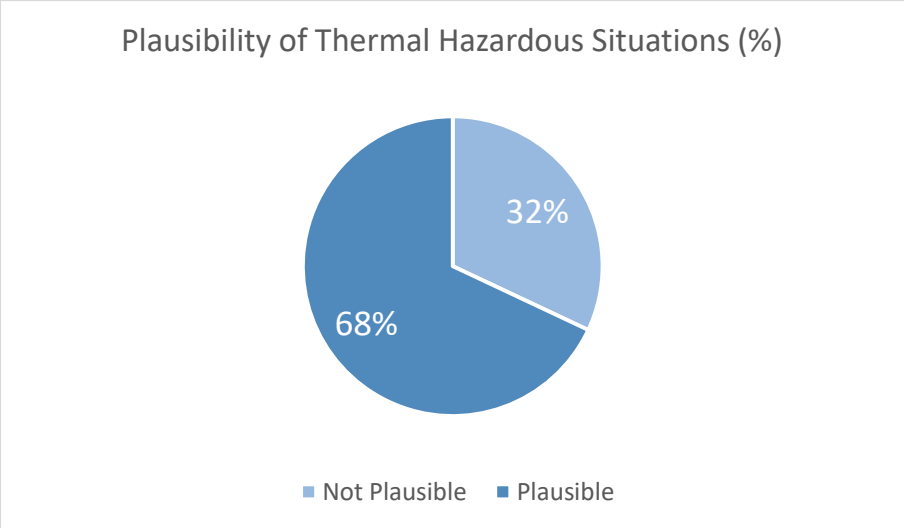


Figure 5.21: Plausibility of Thermal *Hazardous Situations* in percent.

Figure 5.21 shows that about 32% of all generated *Hazardous Situations* are not plausible. An example for an unplausible generated *Hazardous Situation* is that the operator can induce a thermal event while deforming the battery case. This situation is not plausible because the battery case is protected inside the vehicle and can not directly touched.

Linking Failure and *Hazardous Situations*

The *Hazardous Situations* are generated to support the Failure and Risk Analysis of a project. Therefore this analysis investigates how many *Failures* can be detected with the provided *Hazardous Situation List*.

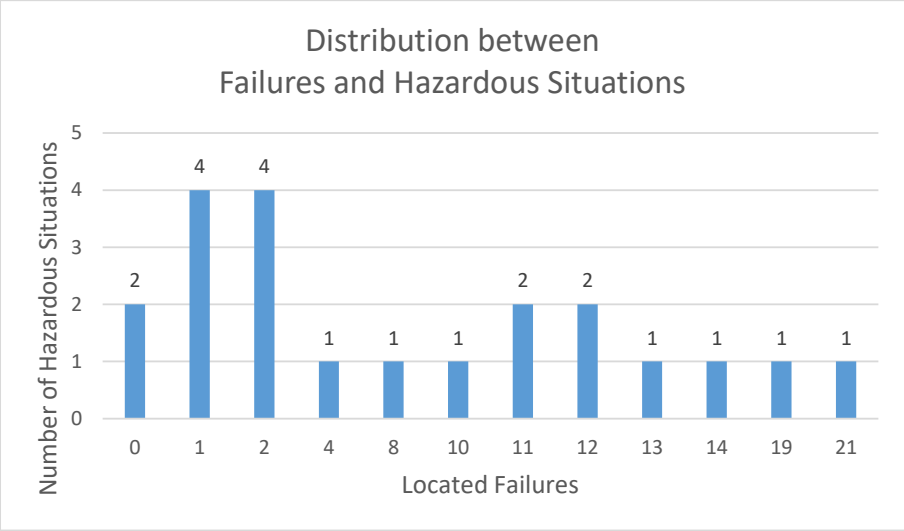


Figure 5.22: Distribution between *Failures* and *Hazardous Situations*.

Figure 5.22 shows that there are two *Hazardous Situations* that are not covered in the Design-FMEA. One of this *Hazardous Situation* is about a thermal event that is induced by a diagnosis tool during maintenance. On the other side there are several *Hazardous Situations* that are linked with more than ten different possible failures. One of these *Hazardous Situation* is the assembly of the battery system.

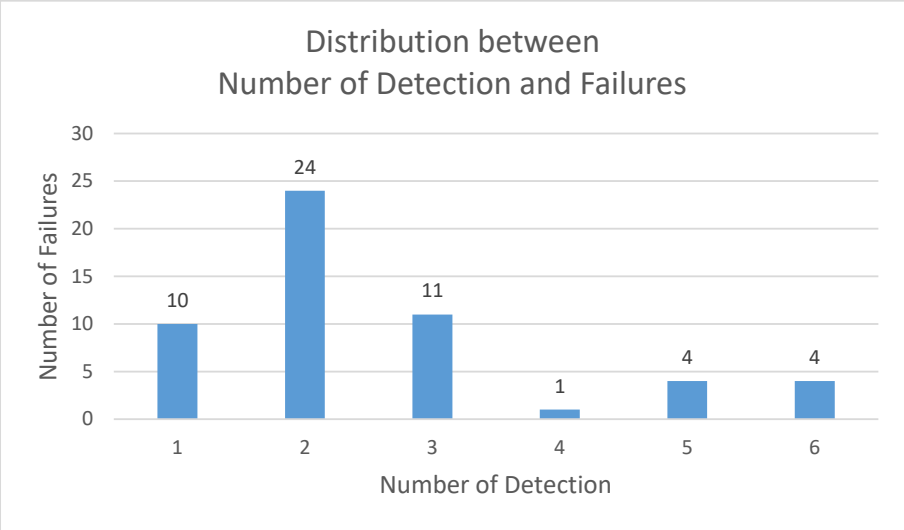


Figure 5.23: Distribution between number of detection and *Failures*.

Figure 5.23 shows how often the individual *Failures* have been identified. There are ten failures that has only been recognized once.

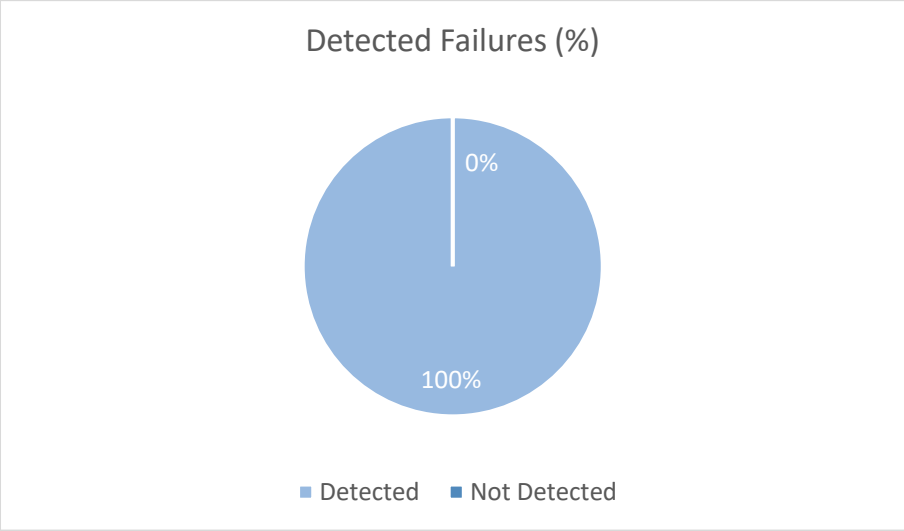


Figure 5.24: Distribution between number of detection and *Failures* in percent.

Figure 5.24 shows that 100% of all failures have been recognized at least once with the generated *Hazardous Situation List*.

Hazardous *Product Phases*

This subsection covers the analysis of the individual *Product Phases* and the distribution of the hazardousness between them.

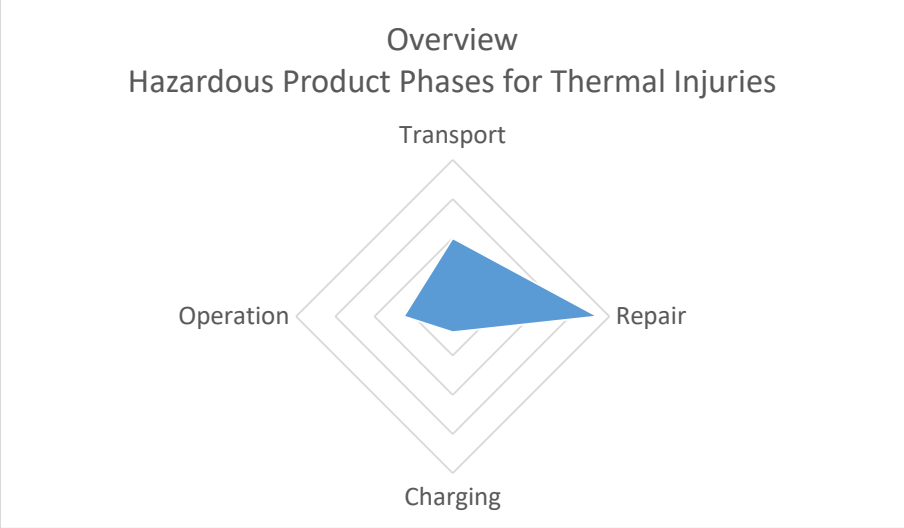


Figure 5.25: Overview Hazardous *Product Phases* as radar chart.

Figure 5.25 shows that the most critical *Product Phase* is the repair phase.

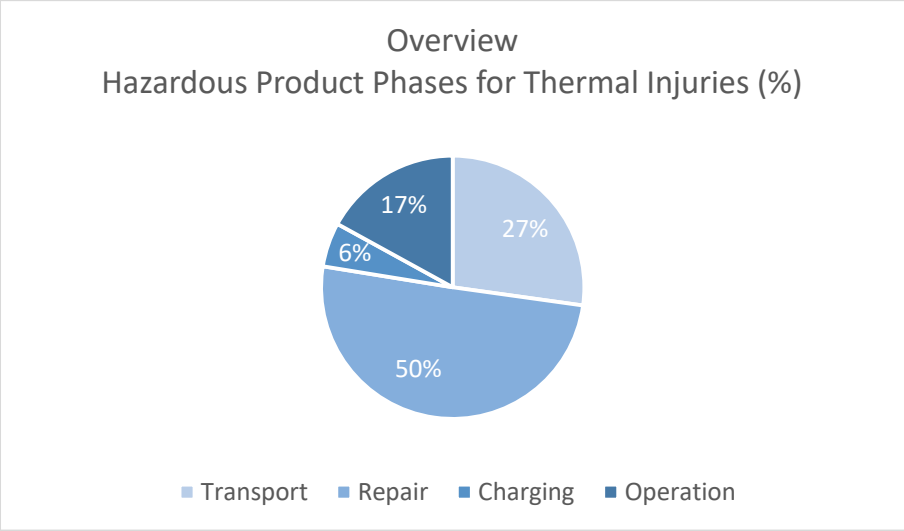


Figure 5.26: Overview Hazardous *Product Phases* in percent.

Figure 5.26 shows that the repair *Product Phase* includes 50% of all identified *Failures*.

Exposed *Roles*

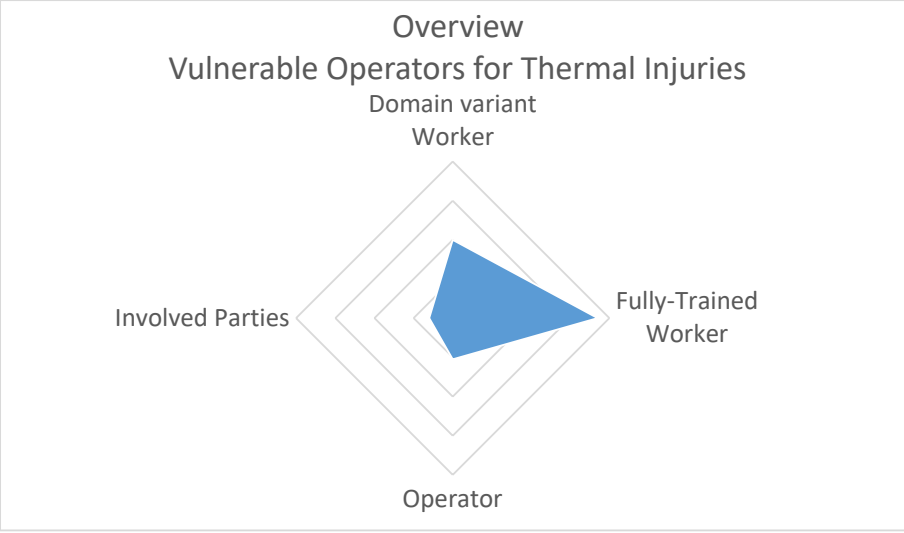


Figure 5.27: Overview Exposed *Roles* as radar chart.

Figure 5.27 shows that the most exposed *Role* is the Fully-Trained Worker.

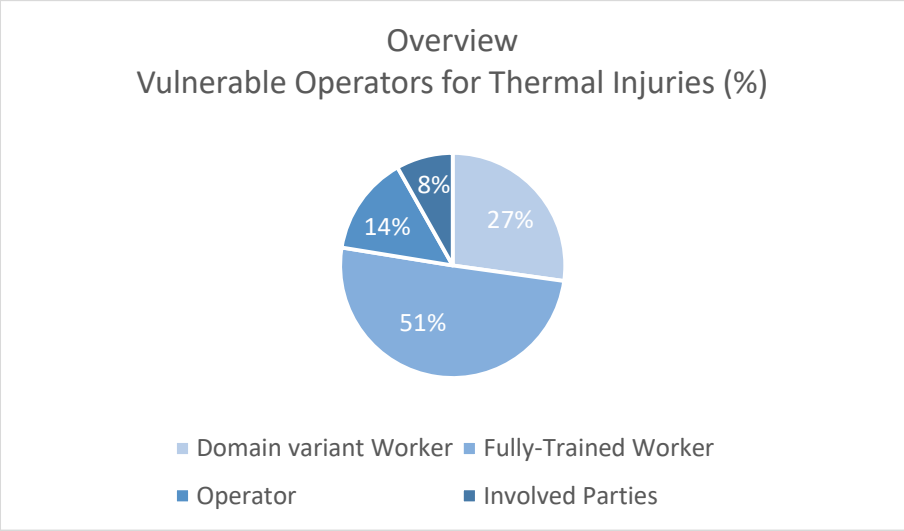


Figure 5.28: Overview Exposed *Roles* in percent.

Figure 5.28 shows that the Fully-Trained Worker *Role* includes 51% of all identified *Failures*.

Chapter 6

Limitations and Future Work

The developed product safety methodology of this thesis is totally independent of other processes in the automotive industry like the ISO 26262. This thesis does not cover the implementation in the current ISO 26262 process.

Furthermore this methodology is not ready for use in the day-to-day business. The reason is that this thesis has not been sufficiently field-tested. Because new *Items* for the automotive industry need months during the development phase. This time was not available during the writing of this thesis. Instead this method has been tested with an abstract example of a HV Battery System.

One of the most time intensive parts of the newly developed product safety methodology is the analysis of the *Hazardous Situation List*. The level of detail of the *Roles* and *Actions* determine the length of the generated *Hazardous Situation List*. It is necessary to keep this list practical and therefore it is necessary to understand how big this list can become. The combination of the list contains five different parameters and can be found in section 4.3 on page 36:

- *Product Phases*
- *Item* List
- *Harm Sources*
- *Roles*
- *Actions*

This parameters are the inputs for the combination equation:

$$Y_{max} = X_{ProductPhase} \cdot X_{Item} \cdot X_{HarmSources} \cdot X_{Roles} \cdot X_{Actions} \tag{6.1}$$

To find out the maximum amount of generated *Hazardous Situations* it is necessary to determine the maximum of all different parameters. The *Product Phases* is all-

ready fixed and can be up to eleven different phases. The *Item* List can be fixed with a single *Item* that is in development. The *Harm Sources* is also allready fixed and can be up to six different sources. The last two parameter the *Roles* and the *Actions* are the most difficult parameters. They are depending on the project and the application. At least the *Roles* can be fixed by generalization then there can be up to four different *Roles*. The *Actions* can be expected with a maximum of eight different *Action* per *Role*.

$$Y_{max} = 11 \cdot 1 \cdot 6 \cdot 4 \cdot (8 \cdot 4) = 8448 \tag{6.2}$$

The number of 8448 different *Hazardous Situations* in the *Hazardous Situation List* seems to be a high number and limits the usefullness of the methodology but this number can be divided in handy parts that can support the FMEA. The data can be separated by different *Product Phases* and *Harm Sources*. Therefore the list can be reduced:

$$Y_{part} = \frac{8448}{11 \cdot 6} = 128 \tag{6.3}$$

This separation can reduce the amount of *Hazardous Situations* to 128 different situations for a particular *Harm Source* during a *Product Phase*.

Usually Excel is widely used for system safety related work. During the work on the example it has been identified that the use of Excel for system safety processes is not sufficient for this methodology. The reason for the impracticability is on the one hand the generation of the *Hazardous Situation List* and on the other hand the linking between the *Hazardous Situations* and the *Failures*. This needs a lot of effort and time and furthermore it is often unclear for engineers. This problem can be mitigated by developing a software tool that implements this product safety methodology and supports the engineers in creating the *Hazardous Situation List* and the linking between the list and the *Failures*. This will decrease the likelihood of mistakes because of the complex methodology scope.

Regarding future work the following topics could be covered:

- Developing a Tool that implements the Product Safety Method
  - Automatically generate *Hazardous Situation List*
  - Support *EFMEA* linking between *Hazardous Situations* and the *Failures*
  - Automatically generate draft versions of different manuals
  - Automatically generate draft version of the *Product Safety Report*
- Test the method in practice
- Integrate this methodology in the ISO 26262 process

Chapter 7

Conclusion

This thesis was about developing a product safety methodology for the automotive industry that supports the engineers during the development phase. This methodology has been developed in this thesis considering the whole product lifecycle of a product with all different operators and uses. Furthermore the method considers different safety, technical and protection domains.

First of all this thesis described what is necessary to fulfill the legal aspects about product safety in Austria and in the European Union. Additionally it gives an overview about the product safety methodologies and processes of other industries as well as an overview about the scientific system safety view.

The introduced and developed methodology shows that the requested tasks can be fulfilled. The consideration of the product lifecycle is achieved by the *Product Phase* identification in the *Information Collection* phase. The related operators and foreseeable use cases are also considered in the *Information Collection* phase. The engineers get supported by automatically generated lists to simplify the failure and risk analysis part that is done in the *Information Generation* phase. The separation and classification of different measures to different *Safety Domains* is done in the *Prevention* phase and can be used for further investigations or the generation of checklists for management purposes.

The whole process is totally independent of the ISO 26262 process, can be implemented in the existing processes and extends the current safety processes. Furthermore it is possible to integrate this method in the current safety process of the different departments. Because it only needs the execution of the failure and risk analysis method *FMEA*. This is typically done in every department and industry, therefore this method could be used in other industries as well.

In conclusion this thesis shows that the currently used safety methods of the automotive industry (ISO 26262) do not fulfill the legal requirements of the European Union concerning product safety. The newly introduced Product Safety Methodology of this thesis is an approach at fulfilling the requirements and supports the engineers during this process. The methodology shows that it is possible to consider the whole product lifecycle with all related operators and foreseeable uses during the system safety development phase. Furthermore it shows that this method can be used to derive checklists for the project management and lists to support engineers during the risk analysis. This methodology also shows that it is possible to consider more than one system safety domain.

This newly introduced methodology is a fundamental step in the right direction to prove and support overall product safety in the automotive industry over the next years and achieve a higher level of product safety as well as making automotive vehicles safer to decrease the number of accidents and the subsequent damages to individuals.

Bibliography

[Age17] International Energy Agency. Global EV Outlook 2017. Two million and counting, [online]. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf, 2017. [25.10.2017]].

[BS13] Hans-Hermann Braess and Ulrich Seiffert. *Vieweg Handbuch Kraftfahrzeugtechnik*. Springer-Verlag, 7th edition, 2013.

[Bun17] Statistisches Bundesamt. Verkehrsunfälle. Zeitreihen 2016. https://www.destatis.de/DE/Publikationen/Thematisch/TransportVerkehr/Verkehrsunfaelle/VerkehrsunfaelleZeitreihenPDF_5462403.pdf__blob=publicationFile, July 2017. [27.12.2017].

[DDIfN11] International Organization for Standardization/Technical Committee (ISO/TC 199) DIN Deutsches Institut für Normung. DIN EN ISO 12100. Safety of machinery. General principles for design. Risk assessment and risk reduction (ISO 12100:2010). March 2011.

[Eme15] Matthew Emery. IEC 62368-1. A new 'hazard-based' standard approach, [online]. https://www.tuv-sud.co.uk/uploads/images/1437489758609448320302/iec62368-1.pdf, 2015. [31.08.2017].

[Eri99] Clif Ericson. Fault Tree Analysis. A History. In *Proceedings of the 17th International Systems Safety Conference*, 1999.

[fSCI11] International Organization for Standardization/Technical Committee (ISO/TC 22). *ISO 26262. Road vehicles-Functional safety. Part 1-10.*, 2011.

[GOS+15] Kenta Goto, Shinpei Ogata, Junko Shirogane, Takako Nakatani, and Yoshiaki Fukazawa. Support of scenario creation by generating event lists from conceptual models. In *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, pages 376–383, Feb 2015.

[Gri] Gerhard Griessnig. Diplomarbeit Fahrzeugsicherheit - Aufgabenstellung Fahrzeug Sicherheit, [Internal Document].

[Heg11] Vaishali Hegde. Case study. Risk management for medical devices (based on ISO 14971). In *2011 Proceedings - Annual Reliability and Maintainability Symposium*, pages 1–6, Jan 2011.

[Kor13] Reiner Korthauer. *Handbuch Lithium-Ionen-Batterien*. Springer-Verlag, 2013.

[Lev11] Nancy Leveson. *Engineering a safer world. Systems thinking applied to safety*. MIT press, 2011.

[LKMP11] Jinghui Li, Rui Kang, Ali Mosleh, and Xing Pan. Simulation and uniform design-based automatic generation of risk scenarios. *Journal of Systems Engineering and Electronics*, 22(6):1015–1022, Dec 2011.

[LP15] Sebastian Lach and Sebastian Polly. *Produktsicherheitsgesetz: Leitfaden für Hersteller und Händler*. Springer-Verlag, 2nd edition, 2015.

[Mal15] Archana Mallya. Using STPA in an ISO 26262 compliant process. Master's thesis, McMaster University, 2015.

[MLW14] Helmut Martin, Andrea Leitner, and Bernhard Winkler. Holistic Safety Considerations for Automotive Battery Systems. In *Automotive Battery Technology*, pages 1–17. Springer-Verlag, 2014.

[otEC01] Official Journal of the European Communities. DIRECTIVE 2001/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 December 2001 on general product safety, [online]. `http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001L0095`, December 2001. [27.12.2017].

[PLH16] Georgi Popov, Bruce K Lyon, and Bruce Hollcroft. *Risk Assessment. A Practical Guide to Assessing Operational Risks*. John Wiley & Sons, 2016.

[pro04] Bundesgesetz zum Schutz vor gefährlichen Produkten (Produktsicherheitsgesetz 2004 – PSG 2004), [online]. `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004009`, 2004. [27.12.2017].

[Sch09] Wilfried Schulz. The New Product Safety Standard for Communication Technology Equipment. In *4th International Telecommunication - Energy special conference*, pages 1–7, May 2009.

[SSK14] Adam Scharl, Kevin Stottlar, and Rani Kady. Functional Hazard Analysis (FHA) Methodology Tutorial, [online]. `http:`

//issc2014.system-safety.org/83_Functional_Hazard_Analysis_Common%20Process.pdf, 2014. [27.12.2017].

Appendix A

eFMEA Abstract

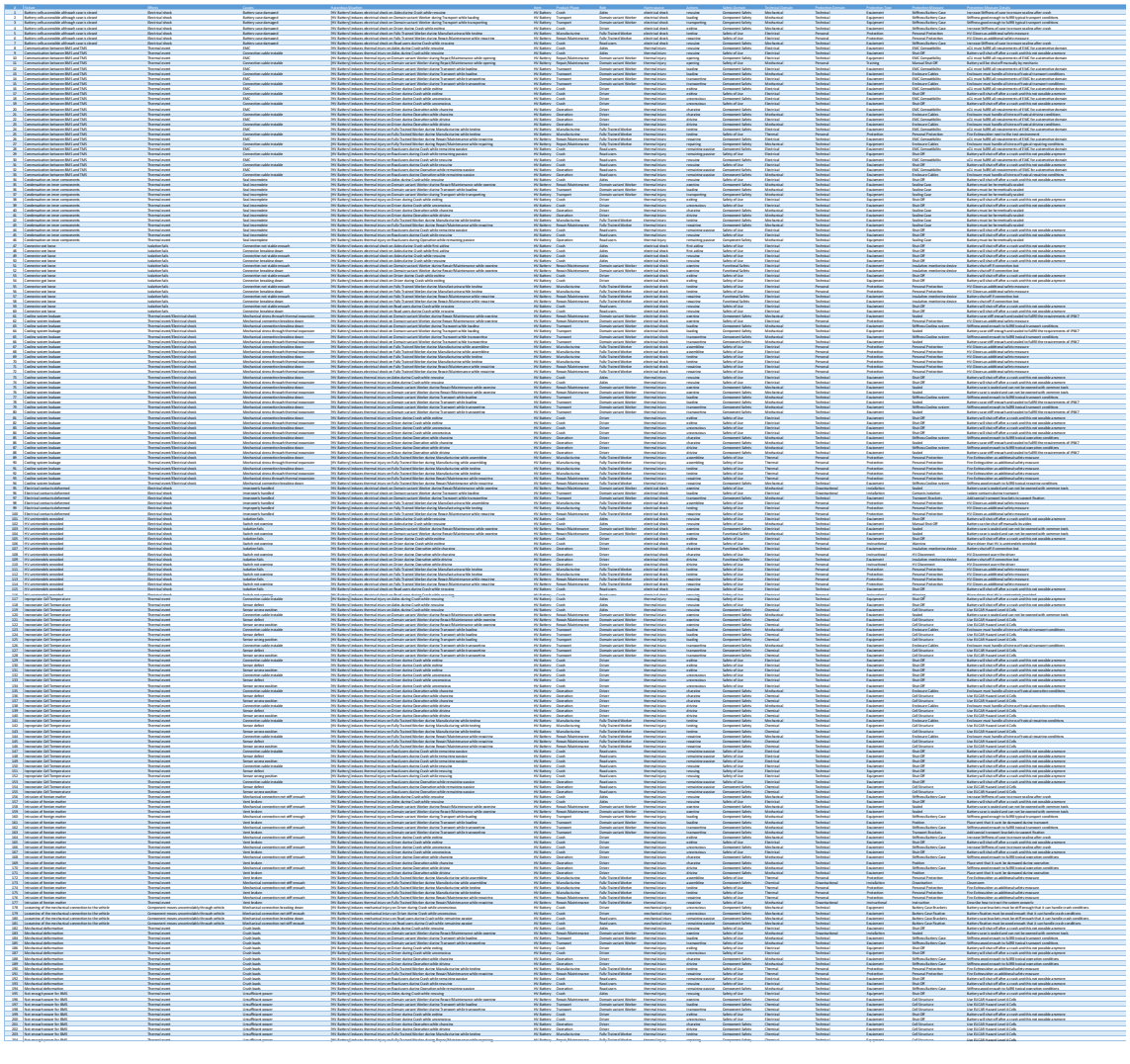


Figure A.1: Abstract of the eFMEA, this does not cover all typical *FMEA* elements and are reduced to the most important that are necessary for this thesis. (Part 1)

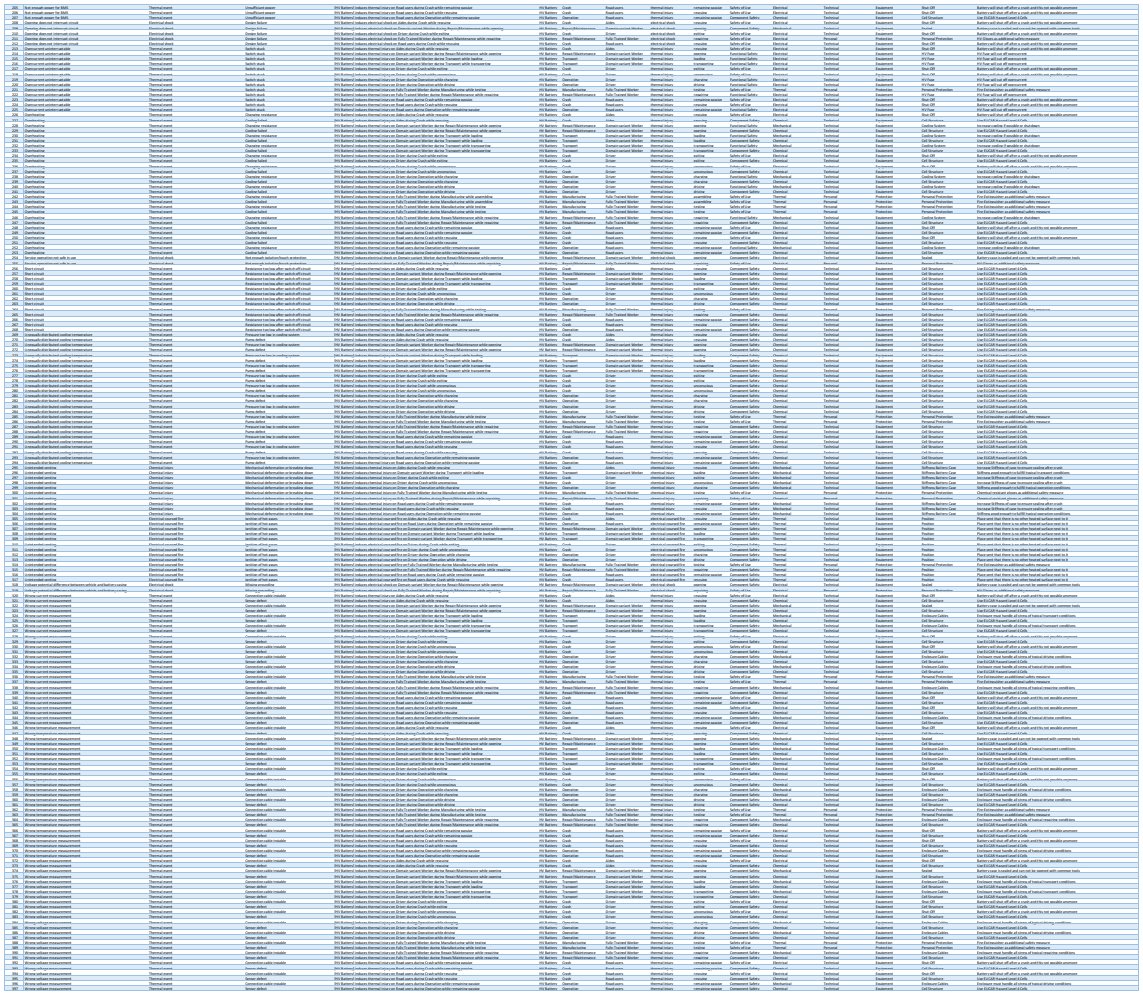


Figure A.2: Abstract of the eFMEA, this does not cover all typical *FMEA* elements and are reduced to the most important that are necessary for this thesis. (Part 2)

Hint: It is important to understand that the *EFMEA* does not contain all necessary parts of a typical *FMEA* . Non important parts for this thesis have been omitted like preventive action, detection action, severity, risk priority number and others. The reason is to give an overview about the method and this parts are not necessary to show the benefits of the method.

Glossary

Action

Describes the possible uses of the product by specific *Roles*.

Analysis

Third phase of the newly introduced Product Safety Method of this thesis and is about the failure and risk analysis.

Cause

Definition of the ISO 26262.

Design Document

Document of the Product Safety Method with detailed information about the implementation of the *Protection Measure*.

eFMEA

Typical *FMEA* with extended information on the developed Product Safety Method.

Execution

Sixth phase of the newly introduced Product Safety Method of this thesis and is about the implementation of the *Protection Measures*.

Failure

Definition of the ISO 26262.

Finalization

Eighth and last phase of the newly introduced Product Safety Method of this thesis and is about the documentation of the whole process results.

Harm Source

Physical energy sources that can harm humans.

Hazardous Scenario

Definition of the ISO 26262.

Hazardous Situation

Detailed information about an accident that can occur while handling the product.

Hazardous Situation List

List with possible situations of accidents that is generated by the Product Safety Method.

Information Collection

First phase of the newly introduced Product Safety Method of this thesis and is about the collection of information about the *Item* in development.

Information Generation

Second phase of the newly introduced Product Safety Method of this thesis and is about the generation of the *Hazardous Situation Lists*.

Item

Definition of the ISO 26262.

Measure

Definition of the ßafety measureïn ISO 26262.

Preparation

Fifth phase of the newly introduced Product Safety Method of this thesis and is about the separation into *Work Packages*.

Prevention

Fourth phase of the newly introduced Product Safety Method of this thesis and is about the failure assignment and classification to different domains.

Product Phase

Different time periods of a product from the manufacture to the decommissioning.

Product Safety Report

Document of the Product Safety Method with detailed information about the product safety process and the results of the individual phases.

Protection Domain

Separation of system safety level on management level.

Protection Measure

Measure that mitigates or eliminates possible risks of harm.

Protection Type

Separation of system safety level on execution level.

Risk Management File

Definition of the ISO 14971.

Risk Management Report

Definition of the ISO 14971.

Role

Operators in the different *Product Phases* that are handling the product.

Safeguard

Definition of the ISO 62368.

Safety Domain

Separation of system safety scopes for a higher level of detail.

Technical Domain

Separation of engineering domains like mechanical or electrical.

Test Document

Document of the Product Safety Method with detailed information about the test results of the defined *Test Method*

Test Method

Document of the Product Safety Method with detailed information about the test process of the implemented *Protection Measure*.

Verification

Seventh phase of the newly introduced Product Safety Method of this thesis and is about the verification of the implemented *Protection Measures*.

Work Package

Information about individual *Protection Measure* that has to be implemented by particular engineers.

Acronyms

BEV

Battery-electric Vehicles

BMS

Battery Management System

BPMN

Business Process Model and Notation

FMEA

Failure Modes and Effects Analysis

FTA

Fault Tree Analysis

HEV

Hybrid electric Vehicles

HSBE

Hazard Based Safety Engineering

HV

High Voltage

SSSM

Specific System Safety Methods

TSSM

Traditional System Safety Methods