Using STPA in an ISO 26262 compliant process

Using STPA in an ISO 26262 compliant process

By

Archana Mallya, B. Eng.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements for the Degree

Master of Applied Science

McMaster University

Master of Applied Science (2015)	McMaster University
(Software Engineering)	Hamilton, Ontario

Title:	Using STPA in an ISO 26262 compliant process
Author:	Archana Mallya, B. Eng. (P. A. College of Engineering, India)
Supervisors:	Dr. Mark Lawford, Dr. Alan Wassyng
Number of Pages:	viii, 109

Abstract

Hazard analysis is an essential activity in the development lifecycle of any safety-critical system. Different industries have their own standards to regulate and standardize their development practices. The introduction of automotive standard ISO 26262 has garnered a lot of interest and the industry is moving towards following ISO 26262 compliant processes. Although the standard suggests using traditional hazard analysis techniques to identify hazards and to perform safety analyses, a literature review shows the limitations of these techniques to handle the increased complexity of modern vehicles, caused by the growing number of features added to them.

Systems-Theoretic Process Analysis (STPA), a relatively novel hazard analysis technique, promises to overcome some of these limitations. However, STPA is not referred to in ISO 26262. In this thesis, we analyze how STPA can help satisfy the requirements of hazard analysis and risk assessment defined in Part 3 of ISO 26262. We also provide an excerpt of our approach of applying STPA as per the concept phase of ISO 26262 on an automotive subsystem, a Battery Management System. One of the main challenges faced by manufacturers is the difference in the terminologies used in the techniques and the standard. To combat this, we provide a detailed comparison of the primary terms used in STPA and ISO 26262, and also compare their founda-

tions. Since most users are familiar with traditional hazard analysis techniques, we also provide a high-level mapping between the outputs of the automotive version of Failure Modes and Effects Analysis (FMEA), Seven Failure Modes FMEA (a variant of FMEA), and STPA.

In conclusion, we determined that STPA can be used in an ISO 26262 compliant manner and also provided guidelines to fulfill any gaps identified. It is important to note that we did not have to modify STPA but only augment it to achieve this.

Acknowledgments

I am extremely grateful to my supervisors, Dr. Mark Lawford and Dr. Alan Wassyng for their strong support and guidance throughout my graduate studies. They have always encouraged me and offered insightful advice. I am equally grateful to Dr. Vera Pantelic for always being there and guiding me all along my thesis work. I would also like to thank Dr. Morayo Adedjouma for encouraging and helping me with my research, specifically our STPA analysis on the battery management system. I am incredibly grateful for the candid suggestions and questions from all four of them, which helped channel my research in the right direction.

I would like to thank my committee members Dr. Spencer Smith and Dr. Ned Nedialkov. Thanks to Dr. Pawel Malysz for his expert advice on the battery management system. I also wish to express my gratitude to all my industrial and academic colleagues. I have been very fortunate to be surrounded by great mentors, colleagues and administrative staff throughout my time with the Department of Computing and Software and Automotive Resource Centre at McMaster University. I would also like to thank my friends, especially, Vasudha, Merhawit, Monika, Alexander, Alex, Linna, Nick, Jason and Manas.

I am grateful for the generous financial support provided by the Ontario Research Fund (ORF) for Research Excellence and McMaster University grad-

uate scholarship.

I would like to especially thank my parents, my parents-in-law, my brother, my sister-in-law and my brother-in-law for their tremendous support and encouragement throughout my life. Last, but not the least, I cannot thank my husband enough for putting up with my random questions and for his continued support and encouragement that helped me complete my thesis.

Contents

List of Figures

List of Tables

List of Acronyms

AIS Abbreviated Injury Scale

ACC Adaptive Cruise Control

AIAG Automotive Industry Action Group

ARP Aerospace Recommended Practice

ASIL Automotive Safety Integrity Level

BCM Battery Control Module

BMM Battery Monitoring Module

BMS Battery Management System

C Controllability

CA Control Action

CoHE Consequences of Hazardous Events

DFMEA Potential Failure Mode and Effects Analysis in Design

E Probability of Exposure

E/E Electrical and/or Electronic

EPS Electric Power Steering

EV Electric Vehicle

FMEA Failure Modes and Effects Analysis

FMECA Failure Modes, Effects and Criticality Analysis

FSC Functional Safety Concept

FSR Functional Safety Requirement

FTA Fault Tree Analysis

HARA Hazard Analysis and Risk Assessment

HAZOP Hazard and Operability Analysis

HPC Hybrid Powertrain Controller

HTV H-IIB Transfer vehicle

ICE Internal Combustion Engine

ISO International Organization for Standardization

JAXA Japan Aerospace Exploration Agency

MAIS Maximum Abbreviated Injury Scale

NHTSA National Highway Traffic Safety Administration

OEM Original Equipment Manufacturer

OS Operating Modes and Operational Situations

PFMEA Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes

PHEV Plugin Hybrid Electric Vehicle

QM Quality Management

RPN Risk Priority Number

S Severity

SAE Society of Automotive Engineers

SOC State of Charge

SOH State of Health

SOP State of Power

7FM Seven Failure Modes FMEA [1]

[1] *7FM* originally stood for seven failure modes, but due to space constraints, we use the term *7FM* to indicate Seven Failure Modes FMEA

STPA Systems-Theoretic Process Analysis

STAMP Systems-Theoretic Accident Model and Processes

TCAS Traffic Collision Avoidance System

UCA Unsafe Control Actions

Chapter 1

Introduction

In this chapter, Section 1.1 discusses the main motivation behind the work done in this thesis and introduces the context of the work. Section 1.2 summarizes the main contributions of this thesis. The organization of the thesis is presented in Section 1.3.

1.1 Motivation

The complexity of modern safety-critical systems is increasing exponentially due to the constant addition of new features and increased automation. While these help in attracting more customers, they also increase the pressure to create a product that is safe and secure, especially if development has to be completed within a short period of time. Moreover, failure[1] of these safety-critical systems could lead to significant loss of property and environmental damage, and in the worst case, could result in harm to humans, or even death. Thus, industries are striving to update their existing safety techniques to keep

[1] "A failure in engineering can be defined as the non-performance or inability of a component (or a system) to perform its intended function." (Leveson 2011)

up with fast paced technology upgrades.

Automotive, one of the safety-critical industries, has seen an increasing number of recalls over the past few years. Born et al. 2010 mention the points recalled by attorneys Thomas Klindt and Andreas Reuter: "the German law on product liability (§ 823 Abs. 1 BGB, § 1 ProdHaftG), which has analogues in other [EU] Member States, states that car manufacturers are generally liable for any damage to the health or death of a person caused by a malfunction of the product, and that liability may be excluded only if the potential malfunction could not have been detected according to the so-called technical state of the art at the time of placing the product on the market." Thus, following the technical state of the art is a great motivation for the automotive companies to reduce their product liability, in addition to ensuring that their products are safe.

ISO 26262, published by the *International Organization for Standardization (ISO)* in late 2011, is an automotive functional safety standard that addresses the safety of automotive systems comprised of electrical, electronic and software components and applies to all activities during the safety lifecycle (ISO26262 2011). ISO 26262 is a comprehensive guide to ensuring functional safety in passenger vehicles. It addresses the possible hazards[2] that are caused by malfunctioning behaviour of electric and electronic safety related systems, including their interactions. Most automotive companies are moving towards an ISO 26262 compliant approach, although it is not mandatory yet. Since ISO 26262 has now been published, Born et al. 2010 noted that to avoid any liability claims in the future, auto industry participants can consider ISO 26262 as current state of the art.

[2]There are multiple definitions of the term *hazard*, such as those listed in Section 3.2

Recent years have seen a significant increase in the amount of software used in modern day vehicles. However, when we build modern vehicles that are so much more software-intensive, the techniques used to ensure safety, such as hazard analysis, also need to deal adequately with the challenges that software introduces with regard to safety. Hazard analysis is an important, if not the most important component of any safety lifecycle. The goal of the hazard analysis is to discover and document how hazards can occur, and to use this information to mitigate (eliminate, reduce or control) these hazards (Leveson 2011). No system can be perfectly safe. Our primary task with respect to safety-critical systems, is to ensure that they are safe from unreasonable risk. We typically talk of "tolerable risk", when assuring the safety of a system. Modern systems encounter more than just traditional component failures. They face both random and systemic failures and hence need a much more robust hazard analysis technique. Accidents could be caused by perfectly functioning components if they do not interact safely. The Mars Polar Lander is a very good example, where the most likely cause of its crash on the surface of Mars was not component failure, but an incorrect interaction between the normally functioning components (Board 2000). The whole notion of "If components and subsystems do not fail, then accidents will not occur" is not completely applicable to modern systems, especially not to complex software-intensive systems. It is important to break out of the traditional approach where it is assumed that proving that components of a system are safe implies that the system is safe.

Many well-established traditional techniques like *Failure Modes and Effects Analysis (FMEA)*, *Fault Tree Analysis (FTA)* and *Hazard and Operability Analysis (HAZOP)* have been in use in various industries for decades. How-

ever, these were designed to deal with older systems where complex human-machine-software interactions might not have played such a major part, and where designs were intellectually manageable (Leveson 2011). Many authors argue that traditional techniques are not effective enough in identifying the hazards and causal factors in modern complex software-intensive systems rich with human interaction (Ishimatsu et al. 2014), (Song 2012), (Leveson 2011), (Breimer 2013). According to Leveson 2011, extending the older techniques to handle the complexity of modern systems is not an efficient strategy. We need a technique built to handle the complexity of modern systems to deal with the limitations of the traditional techniques i.e., we need a state of the art hazard analysis technique. *Systems-Theoretic Process Analysis (STPA)*, based on systems thinking and built on the *Systems-Theoretic Accident Model and Processes (STAMP)* methodology, is a relatively novel technique with the potential to help us achieve a safe system by including the human-software interaction factors in the analysis (Leveson 2011). A systems approach focuses on the system as a whole and not just on proving the safety of the components alone. STPA has been successfully applied across various domains like aerospace, nuclear, medical and automotive to name a few (Stringfellow et al. 2010), (Song 2012), (Antoine 2013), (Breimer 2013). The literature review in Section 2.3 indicates that STPA can effectively handle the added complexity of modern systems. Most notably, GM has been applying STPA on automotive systems (Sundaram and Hartfelder 2013), (D'Ambrosio et al. 2014) and the *National Highway Traffic Safety Administration (NHTSA)* has shown interest in the technique (NHTSA 2014), (Hommes 2015). Given the industry's gradual shift to compliance with ISO 26262, the topic of STPA's application in an ISO 26262 compliant process is very relevant and potentially beneficial from

the standpoint of larger acceptance of STPA in the automotive industry. This is further motivation for the automotive industry to not only consider this relatively novel, promising hazard analysis technique, but also to diligently follow the state of the practice ISO 26262 standard. However, to the best of our knowledge, there is no detailed published work to determine if STPA can be used in an ISO 26262 compliant process. This is precisely what this thesis aims at: to investigate the use of STPA in an ISO 26262 compliant process. Since we are focusing on the hazard analysis technique STPA, we will focus on the *Hazard Analysis and Risk Assessment (HARA)* component of ISO 26262 i.e. Part III, Clause 7 of ISO 26262. The objective of HARA is to identify and categorize the hazards caused by the malfunctioning behaviour of the item and to formulate safety goals to prevent or mitigate against the unreasonable risks caused by the hazardous events (ISO26262-3 2011).

Although STPA is gaining a lot of interest from industries and academics, it is fairly new and not as widely known and applied as some of the traditional hazard analysis techniques. On the other hand, the first FMEA guideline was dated November 9, 1949, (Military procedure MIL-P-1629) titled "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," (Ericson II 2005). Slightly modified versions of FMEA have since been adopted by a variety of industries including nuclear, automotive and medical. Since FMEA is one of the most commonly used traditional hazard analysis techniques, this thesis will also present a high-level comparison between the outputs of STPA with the outputs of FMEA[3] and 7FM (Lindland 2007), which is an extended version of FMEA.

[3]We will focus on the automotive FMEA as published in SAE 2009

1.2 Main Contributions

Our work contributes to the area of functional safety in the automotive industry. We focus on the relatively novel hazard analysis technique, STPA, and the state of the practice automotive functional safety standard, ISO 26262. This thesis not only answers the question of whether STPA can be used in an ISO 26262 compliant process, but also provides guidelines to use STPA in an ISO 26262 compliant manner. We further illustrate the use of our approach with an example application. The key contributions of this thesis are:

- We provide a detailed comparison of the hazard analysis requirements in ISO 26262 standard and the STPA technique: we present a comparison of the foundations on which these two are based, and then provide a detailed comparison of the central terms. One of the main challenges we encountered was that the same terms in STPA and ISO 26262 did not necessarily have the same meaning. In this thesis, we present the similarities and differences between them.

- We build on our STPA and ISO 26262 comparison to check how every relevant activity and artifact required or recommended by the HARA process of ISO 26262 can be satisfied by applying STPA. Although the topic of using STPA in an ISO 26262 compliant process has been the subject of study (Hommes 2015), or, at least its significance has been recognized (NHTSA 2014), (Hommes 2012b), to the best of the author's knowledge, this thesis represents the first detailed account of the topic.

- We produce guidelines on how to use STPA in an ISO 26262 compliant process. The guidelines can be used by a practitioner when perform-

ing hazard analysis compliant with ISO 26262. Further, we illustrate our approach by applying the guidelines on an excerpt of a real-world automotive subsystem from our industrial partner.

- We provide a mapping between the outputs of STPA, FMEA and 7FM (Lindland 2007) (an extended version of FMEA). This is to ensure that our work helps a wider audience familiar with traditional hazard analysis technique like FMEA to see how it maps to STPA.

1.3 Outline

This thesis is organized as follows: Chapter 2 provides background on hazard analysis techniques like FMEA, 7FM, FTA, HAZOP and STPA. It also introduces the automotive standard ISO 26262, with a focus on the clauses of the concept phase of the standard, which contains the requirements for the hazard analysis and the risk assessment. Related work done to show the potential of STPA as well as work done on ISO 26262 and STPA is presented in Chapter 2. Chapter 3 provides a detailed comparison of concepts and terminologies between ISO 26262 and STPA and also features the main topic of this thesis, *our approach to using STPA in an ISO 26262 compliant process*. The approach is evaluated using an illustrative application on an abstracted real-world automotive subsystem, *Battery Management System (BMS)*, and is presented in Chapter 4. Chapter 5 deals with the high-level mapping between the outputs of the three methods: STPA, automotive FMEA and Seven Failure Modes FMEA. Chapter 6 summarizes the author's conclusions regarding this topic, and provides suggestions for future work.

Chapter 2

Preliminaries

In this chapter, we first explain the different hazard analysis approaches, focusing mainly on the ones used in this thesis (STPA, FMEA, Seven Failure Modes FMEA). We then discuss aspects of the functional safety automotive standard ISO 26262, focusing mainly on the concept phase i.e. Part 3 of ISO 26262. This chapter also includes related work on: comparing STPA with traditional techniques like FMEA and FTA, review of ISO 26262, status of work relating ISO 26262 and STPA and comparing STPA with the *Aerospace Recommended Practice (ARP)* standard. The concepts explained here will lay the groundwork to understanding the approach and comparison explained later.

2.1 Hazard Analysis Techniques

Hazard analysis can be defined in various ways depending on the domain and on what the industry considers to be part of the hazard analysis. Leveson 2011 defines hazard analysis as "the process of identifying hazards and their potential causal factors". Hazard analysis is performed to eliminate, mitigate

and/or control the hazards and their causes (Leveson 2011). Hazard analysis techniques are generally labelled as either deductive or inductive techniques. Deductive techniques are used when the hazard/top event is known, i.e., given a hazard, causes are identified (Ericson II 2005). In deductive techniques, we move from the general to the specific. Inductive techniques are used to identify the hazards when the specific root causes are not known or proven (Ericson II 2005). In inductive techniques, we move from the specific to the general i.e., the system is decomposed into individual components and their failure modes are analyzed. Hazard analysis techniques are also classified as top-down or bottom-up techniques (Ericson II 2005). According to Ericson II 2005, "Some system safety practitioners advocate that a deductive analysis is always a top-down approach and that an inductive analysis is always a bottom-up approach. This may be a good generalization but it is likely not always the case." Examples of top-down techniques include STPA and FTA. FMEA is usually used in a bottom-up manner, although it can also be used as a top-down technique (Song 2012). This section provides a short description of the various hazard analysis techniques cited in ISO 26262 like FMEA, FTA, HAZOP and the relatively new hazard analysis technique, STPA and 7FM, a type of FMEA. This thesis will mainly focus on STPA and variants of FMEA.

2.1.1 Systems-Theoretic Process Analysis

Systems-Theoretic Process Analysis (STPA) is based on the accident causation model called STAMP (Systems-Theoretic Accident Model and Processes), built on systems theory and systems engineering (Leveson 2011). Systems theory is especially useful for complex systems where analyzing the interacting

subsystems as separate entities could give inaccurate results. Such complex systems require a technique which focuses on the system in its entirety and not as a sum of individual subsystems (Leveson 2011). The STPA technique accounts for the interactions between the subsystems, including software interactions and the dynamics between the system and its environment. It also deals with management issues and human factors (Leveson 2011). STPA treats *safety as an emergent property and a dynamic control problem* (Leveson 2011). Safety as an emergent property enforces the assumption that the safety of a system cannot be confirmed by just proving the safety of its individual components, but depends on the interaction of the components involved in the system. System safety thus can be achieved by enforcing a set of safety constraints related to the behaviour of the whole system. Safety as a control problem means that accidents should not be viewed as a result of a failure: the accidents involve dynamic process more than a sequence of events, and occur when inadequate control actions violate the safety constraints of the system.

The general STPA process is explained below. More detailed explanation and an illustrative example with respect to ISO 26262 can be found in Chapter 3 and Chapter 4 respectively. The STPA technique follows 3 steps: Preliminary step (Step 0), Step 1 and Step 2, as shown in Figure 2.1. Step 0 deals with the identification of system level accidents, associated hazards and preliminary safety constraints to mitigate those hazards. The hazard identification step includes drawing the system boundaries as a prerequisite. Drawing the system boundaries helps in determining what constitutes a hazard. The main difference in the scope of accident and hazard is that the latter can only include the aspects of the environment over which the designer or operator has

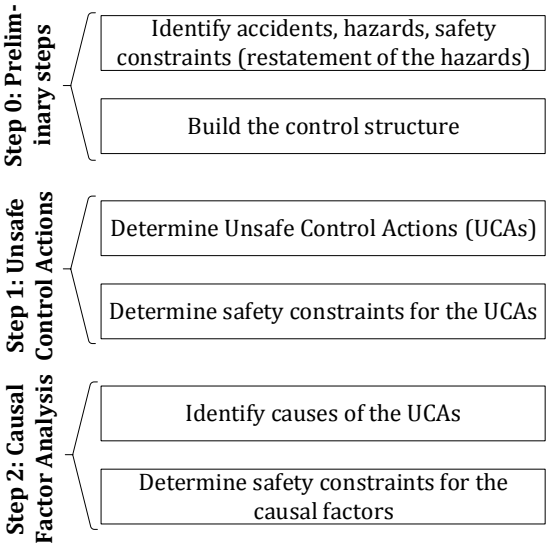

Figure 2.1: Overview of STPA

control (Leveson 2011). Step 0 also involves determining the safety constraints as negations of the hazards identified. A high level safety control structure is then defined, which should incorporate the safety constraints identified earlier in this step. The control structure is a functional model of the system and gives a big picture of the system under consideration.

Based on the output of Step 0, mainly the control structure and the hazards, Step 1 identifies the ways in which the control actions could lead to the system being in a hazardous state, along with the corresponding safety constraints. Leveson 2011 suggests that there are four ways in which a control action can be hazardous:

1. a required control action is not provided or not followed,
2. an unsafe control action is provided,
3. a potentially safe control action is provided too late, too early, or out of

sequence, and

4. a continuous safe control action is stopped too soon or applied too long.

Step 1 can be documented using a tabular format for easy readability as shown in Figure 2.1, but other representations can also be used.

Table 2.1: STPA Step 1 – Unsafe control actions (Leveson 2011)

Control Action	Required control action not provided	Unsafe control action provided	Safe control action provided too late, too early, wrong order	Continuous safe control action provided too long or stopped too soon

Step 2 represents the causal factor analysis and involves identifying the causes of these unsafe control actions along with the corresponding safety constraints. Causal factor analysis involves identifying the scenarios which could lead to unsafe control actions with the help of control loops. The control structure is examined to determine the control loop for each unsafe control action. A process model is added to the controller to determine how it views the system (Leveson 2011). This process model includes the current state of the controlled process and assumptions about how the controlled process operates (*An STPA Primer, V.1* 2013). STPA provides some guide words to help determine the causal factors. Figure 2.2 shows a control loop with guide words as shown in Leveson 2011. Though STPA provides guide words to help analysts in performing the causal factor analysis, it is important not to limit the analysis to only these guide words. The safety constraints identified in this step could lead to the refinement of the control structure. STPA is performed

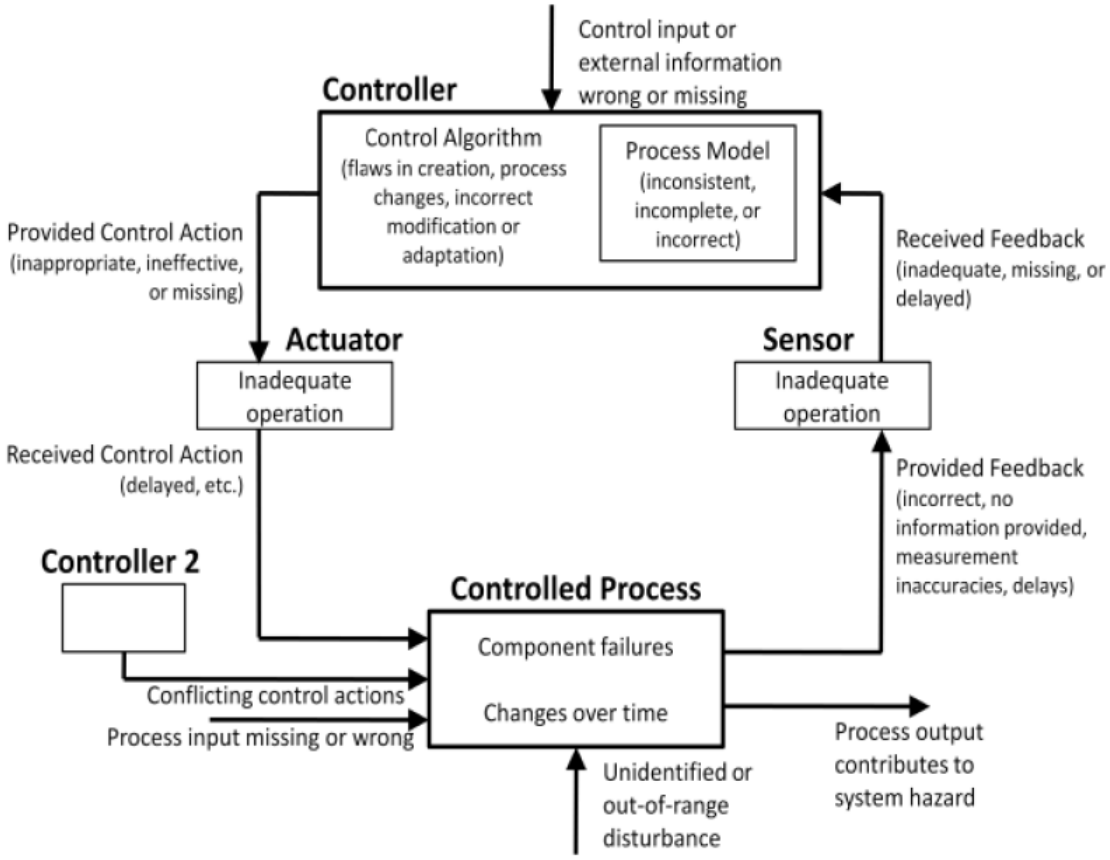

Figure 2.2: STPA Step 2 – Causal factors analysis (Leveson 2011)

iteratively until the system is free of unreasonable risks.

Literature review shows that STPA has been successfully applied in various domains like aerospace, automotive, nuclear and medical, to name a few (Stringfellow et al. 2010), (Breimer 2013), (Song 2012), (Antoine 2013). However, there is a need to demonstrate how STPA can be compliant with relevant safety standards to increase confidence of a successful outcome when it is applied in industrial projects. As of now, the STPA technique does not include a risk-based classification approach of the hazardous events as required by some of the standards, specifically the automotive functional safety standard, ISO 26262. We will look into ISO 26262 in Section 2.2 and then review the work

done on showing how to use STPA in an ISO 26262 compliant process.

2.1.2 Fault Tree Analysis

Fault Tree Analysis (FTA) is one of the most commonly used traditional safety analysis technique. FTA is used to determine the root causes and probability of occurrence of undesired events (Ericson II 2005). It starts with a top event which corresponds to an undesirable event and then proceeds to identify the causes that triggered that undesired event. All the possible causes identified can be listed and combinations of causes can also be considered. The results are documented graphically in the form of a tree as shown in Figure 2.3. In

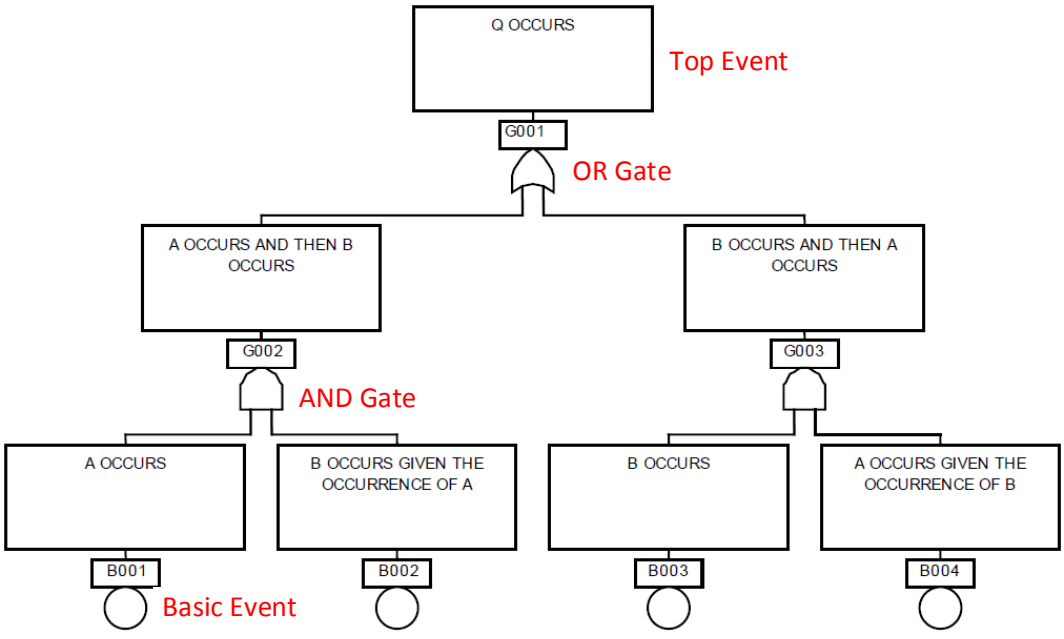

Figure 2.3: Example of Fault Tree Analysis with dependency explicitly shown (Based on Vesely et al. 2002)

short, FTA helps analyze an undesired state of a system using Boolean logic to combine a set of lower level events. It helps us to understand how systems could fail, and identifies ways to mitigate and reduce risk.

FTA is easy to understand and easy to perform as long as the analysts do a good job of determining the causes of the top event. According to Ericson II 2005, modeling multiple phases, sequential timing and repair could be difficult with FTA and could be time consuming. Since FTA is not the focus of this thesis, we do not include additional details about this technique. More details about this technique can be found in Ericson II 2005, Vesely et al. 2002 among various other sources.

2.1.3 Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) is one of the best known traditional hazard analysis techniques used to evaluate potential failure modes. Another version of this technique is called Failure Modes, Effects and Criticality Analysis (FMECA). FMECA is quite similar to FMEA, except, in addition to the normal FMEA process, it also evaluates the criticality[1] of each failure mode.

FMEA can be applied at any level of design detail on a system (Ericson II 2005). FMEA is mostly used in a bottom up fashion, but can also be used in a top down manner. As mentioned in Ericson II 2005, conceptually, there are 3 main approaches to performing a FMEA, each being focused on different aspects. The three types are: 1) the functional approach 2) the structural approach and 3) the hybrid approach. The *functional approach* analyzes the ways in which the functional objectives of the system are unsatisfied or erroneous, and can be utilized in a top-down manner. *Functional FMEA* is more adaptable in considering multiple failures, software functions and human error

[1]Criticality (SO) is the product of Severity (S) and Occurrence (O) ranking and is also known as the criticality number (SAE 2009)

(Ericson II 2005). The *structural approach*, also called the hardware approach, is generally used on hardware when its items can be uniquely identified from the engineering and design data. The *hybrid approach* is a combination of the functional and structural approaches i.e., it "begins with the functional analysis of the system and then transitions to a focus on hardware, especially hardware that directly contributes to functional failures identified as safety critical" (Ericson II 2005). More information regarding these types can be found in (Ericson II 2005) and (Song 2012). FMEAs are used to determine and analyze the potential failure modes and their failure causes and effects.

The initial scope of the analysis can be documented using pictorial tools like functional block diagrams, interface diagrams and process flow diagrams (SAE 2009). In general, the FMEA process is documented and analyzed in the form of a worksheet. Based on the project and the system under study, the amount of detail included in the worksheet can vary. Since we are focusing mainly on the automotive domain, we will focus on the *Society of Automotive Engineers (SAE)* version of FMEA as published in SAE 2009. FMEA presented in SAE 2009 describes FMEA as *Potential Failure Mode and Effects Analysis in Design (DFMEA)* and *Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (PFMEA)*. The format of a DFMEA worksheet as per SAE 2009 is as shown in Figure 2.4. DFMEA is generally started after project initiation and completed before the design release, whereas, PFMEA should be "started before or at the feasibility stage and prior to tooling for production" (SAE 2009). Mainly the difference between DFMEA and PFMEA is product versus process FMEA. In general the results of DFMEA are used as one of the inputs to the PFMEA. In this section, we will focus only on the DFMEA and explain the various columns of Figure 2.4.

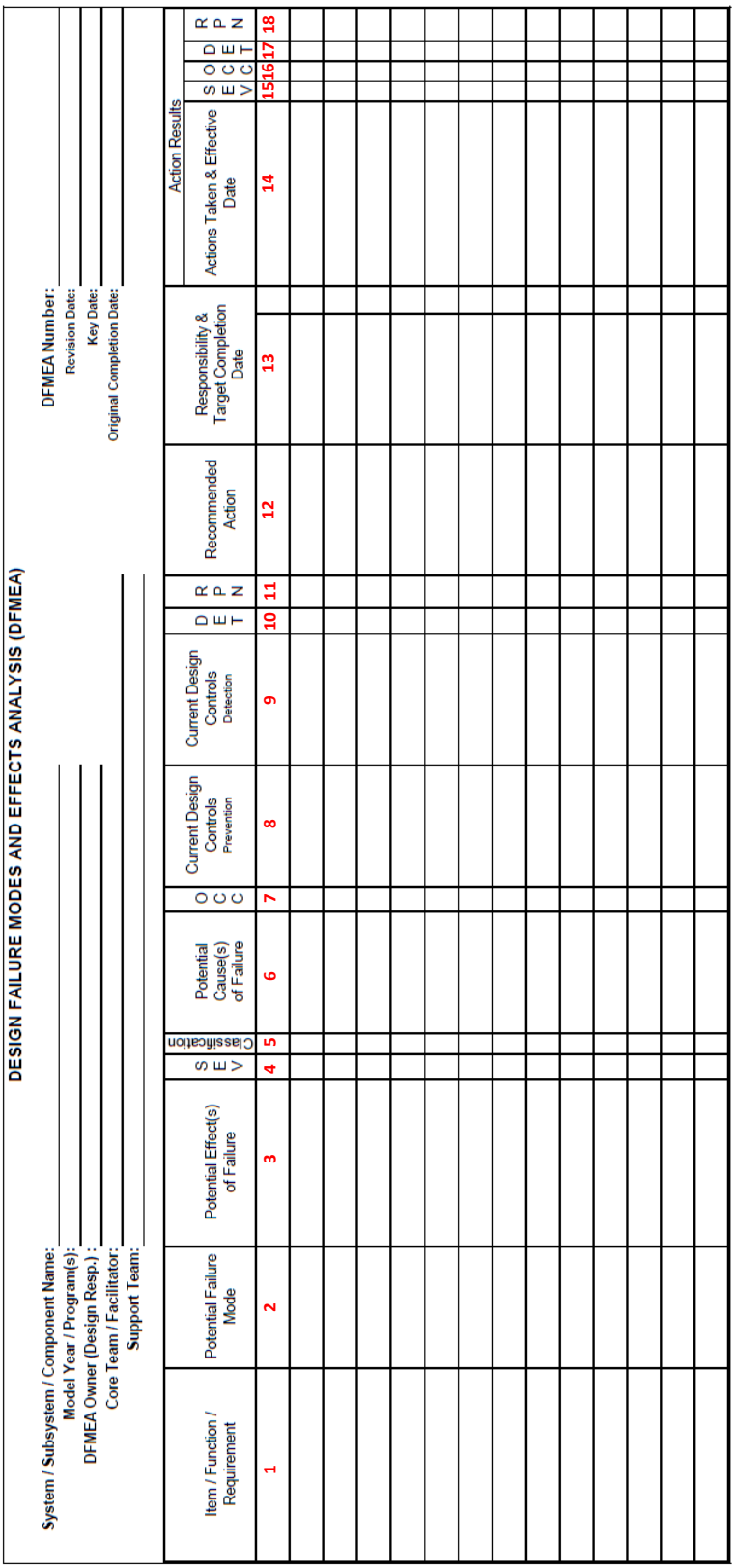

Figure 2.4: Example DFMEA worksheet (SAE 2009)

Column 1 includes information about the item such as the item number or the part class, function(s) of each item being analyzed and a description/requirement of how each item should perform. Column 2 includes information about the potential failure modes i.e., the ways in which the component, subsystem or the system could potentially fail to meet the intended functions and/or its requirements. According to SAE 2009, "there are at least five different types of potential failure modes:

- loss of function (i.e. inoperable, etc.)
- partial function (i.e. performance loss, etc.)
- intermittent function (i.e. operation starts/stops/starts often as a result of moisture, temperature, etc.)
- degradation (i.e. performance loss over time, etc.), and
- unintended function (i.e. operation at the wrong time, unintended direction, etc.)"

Each entry in column 1 can be associated with more than one failure mode. Experience, brainstorming, historical data can help in listing the failure modes.

Column 3 is used to list the potential effects of the failure modes, i.e. the consequences or results of each of the failure modes. According to SAE 2009, the effects are considered against the next level up. Column 4 is used to list the estimated severity ranking of the potential effect of the failure mode and is determined using the criteria suggested in SAE 2009. The team should agree on the evaluation criteria and the resulting ranking. Column 5 (classification) is optional and not discussed here. Column 6 is used to list the potential cause of the failure and should be listed as precisely as possible to get the maximum benefit out of the FMEA. Column 7 is used to list the estimated occurrence

ranking of each cause of the failure mode being evaluated. It is important to note that the occurrence ranking is a relative rating within the scope of the FMEA and considers the likelihood of occurrence during production or during the life of the product (SAE 2009). Column 8 (prevention type design controls) is used to describe how a cause, failure mode or effect is prevented currently. Column 9 (detection type design controls) is used to list the potential type of detection design controls to describe how a cause or failure mode is detected before the item is released to production and is used an input to the detection ranking (column 10). The detection ranking column lists the *the rank associated with the best design control from the list of detection-type design controls* (SAE 2009). Column 11 i.e. *Risk Priority Number (RPN)*, is determined as a product of columns 4, 7 and 10 i.e. severity, occurrence and detection ranking respectively. Column 12 is used to list recommended actions to prevent or mitigate the identified risks. Column 12 can also include the name of the organization or department and column 13 (Responsibility and target completion date) should include the name of the person responsible for completing the recommended action and the due date. Column 14 is to provide a short description of the action taken and the effective date. Columns 15, 16, 17 and 18 are revised ratings as a result of the actions taken.

Although literature review suggests FMEA is an ideal technique to evaluate individual failure modes and provide reliability information, its main shortcoming is that it does not deal well with a combination of items failing (Ericson II 2005). Thus it is suggested that FMEA not be used as a sole technique to identify hazards, but as a complementary technique to other hazard analysis techniques. There are various versions of FMEA developed by various industries and organizations to suit their needs. In the next section we present

7FM, an adaption from the *Automotive Industry Action Group (AIAG)* FMEA manual (third edition) as presented in Lindland 2007. The AIAG FMEA manual is a reference manual which is aligned with SAE 2009 and is a reference manual aimed to guide and assist suppliers.

2.1.4 Seven Failure Modes FMEA

Seven Failure Modes FMEA is essentially an extension of traditional FMEA to classify the failure modes into seven failure modes. The main concept behind the seven failure modes FMEA technique is that "an action or energy transfer can fail in one of seven ways", namely: 1) Omission, 2) Excessive, 3) Incomplete, 4) Erratic, 5) Uneven, 6) Too Slow and 7) Too Fast (Lindland 2007). Seven failure modes FMEA can be applied at the system, design and process level.

Figure 2.5, based on Lindland 2007, provides an idea about how the various FMEAs are related. SFMEA, DFMEA, PFMEA in Figure 2.5 are referring to the System, Design and Process level seven failure modes FMEA respectively. Focusing on the red dashed box, SFMEA helps identify the system functional failures and the specific part failures are identified as special characteristics and studied using DFMEA and PFMEA. DFMEA and EFMEA, further help in identifying the various failures and provide input to PFMEA. PFMEA helps in studying the various process actions and energy transfers required in producing the dimensions and special characteristics of the materials and products. In this thesis, we provide a brief explanation of the system seven failure modes FMEA; details about the other types can be found in Lindland 2007. For brevity, we will refer to the seven failure modes FMEA technique as 7FM in

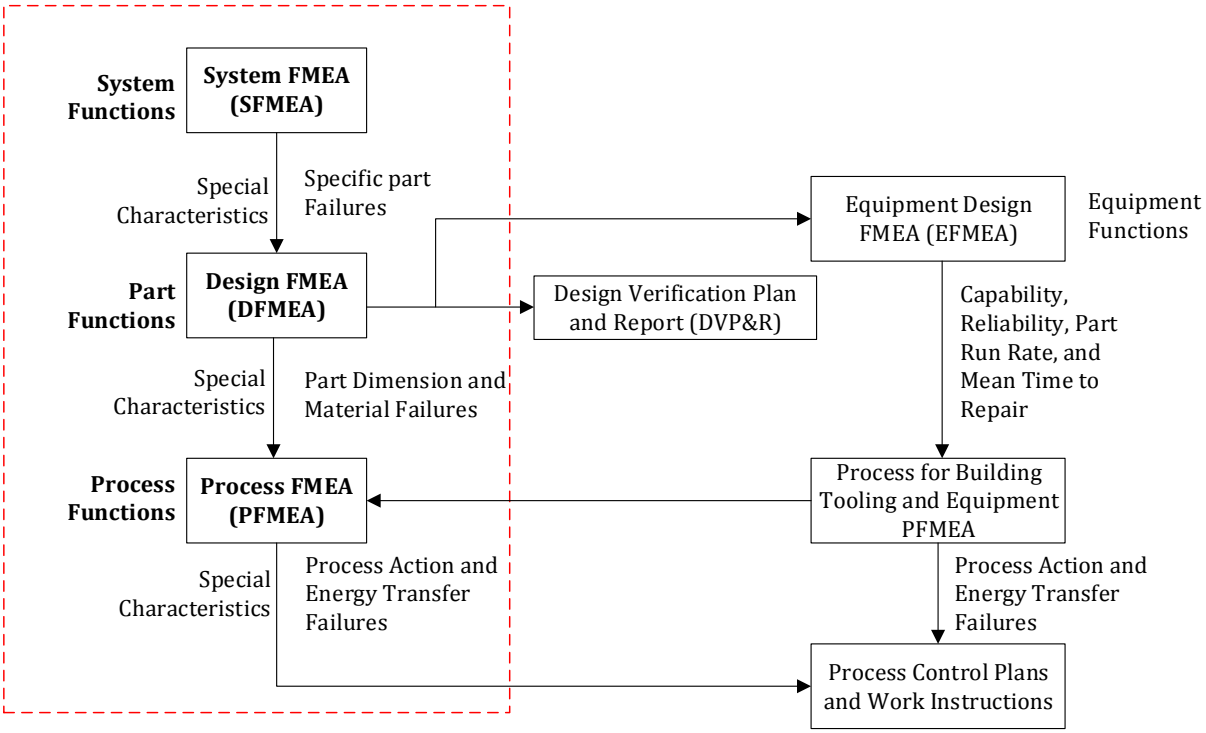

Figure 2.5: Relationship between FMEAs (Based on Lindland 2007)

the following sections.

Figure 2.6 shows the basic steps of setting up a system 7FM. Lindland 2007 documents the initial scope in the form of a functional block diagram. The functional block diagram involves identifying the major building blocks of the system, their physical input/output relationships and the direction of flow of energy and communication. In Lindland 2007, drawing the functional block diagram is an adaptation of MIL-STD-1629A and dotted blocks/lines are used to denote anything that is outside the scope of study. The rest is in the scope of study and inputs to the functional blocks could be the potential causes. This is followed by documenting the building blocks of the system under study and their physical input/output relationships with the use of

arrows to show the direction of communication or energy transfer. The next step involves documenting the outputs and inputs.

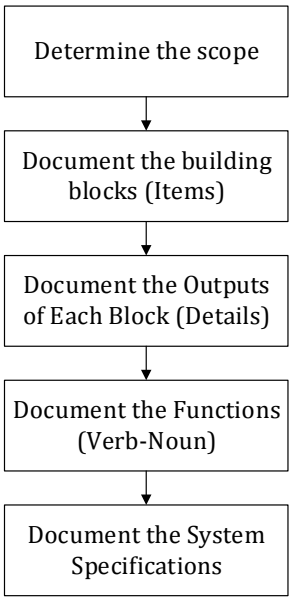

Figure 2.6: Setting-up the system 7FM (Lindland 2007)

Documenting the block output (*function*) is a very important step of this technique. Missing any outputs in this step would mean that the analysis would not identify the risks associated with the missing functions. Worksheets can be used to document this information, as shown in Figure 2.7.

Each of the functions identified can produce seven *failure modes* and each failure mode can produce several *effects*. The technique also mentions failure sequence as *cause, failure mode and then effects*, although causes are identified after the failure modes are listed. Columns 1, 2 and 3 of Figure 2.7 have already been explained and the rest are explained below. Some of the columns are assigned numbers to indicate the sequence in which they need to be filled in and also to help in referring to them in our explanation.

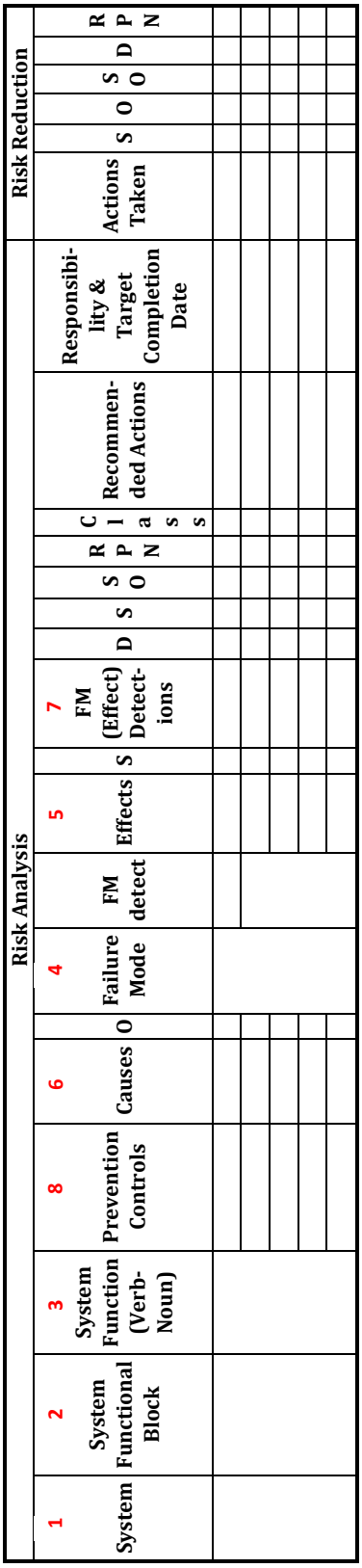

Figure 2.7: System 7FM Worksheet (Based on Lindland 2007)

The 7 failure modes (column 4) as explained in (Lindland 2007) are given below. The exact text from Lindland 2007 is presented below as 7FM is relatively new and to be on the safe side, we did not want to confuse the readers by adding our own interpretation of these failure modes.

1. "[O] Omission (Magnitude): Omissions will occur when there is no energy, no signal to challenge the system to respond, or there is an absolute restriction to energy flow or movement."

2. "[+] Excessive (Magnitude): Excessive relates to the magnitude of response, not the length of time of the response. An excessive function will occur when there is an excess of energy, a resistance/restriction to movement or energy transfer which is too small, or a loss of the feedback signal required to control the level of response."

3. "[−] Incomplete (Magnitude): Incomplete also relates to the magnitude of response and occurs when there is insufficient energy, excessive resistance/restriction to energy transfer, or the control system provides a response that is too small.... Anytime the energy is insufficient to meet the demand, the response will be insufficient."

4. "[V] Erratic (Variation): Erratic requires that energies, resistances, restrictions, or control signals (which control energy/position) are erratic.... Items that are designed to provide restrictions limit movement (both linear and rotational), and when those restrictions become loose the movement becomes erratic."

5. "[U] Uneven (Variation): There are times when a system has a specification for the uniform distribution of energy (force, pressure, heat,

magnetic flux, etc.). Uneven occurs when the system parameters are outside the specified range. There are other circumstances where a system has no specification for the even distribution of energy, it is assumed or expected."

6. "[$+T$] Too Slow (Time): Too slow relates to when the output function is slower than system specifications. As with uneven, both too slowly and too quickly (next topic) will apply even when there are no system specifications. Too slowly relates to the dynamic condition of energy transfer.... Too slowly does not relate to the magnitude of the function; given enough time the magnitude will be achieved. Energy achieved too slowly can relate to heat, force, pressure, torque etc."

7. "[$-T$] Too Fast (Time): Too fast or too quickly relate to when the system responds faster than system specifications.... Too quickly is the opposite of too slowly, however the effects might be very different. In too quickly it is the magnitude of the function that is achieved too quickly."

The three primary considerations with respect to these seven failure modes in system 7FM are failure of: magnitude, variation and time, rate of energy transfer or speed depending on if it is system 7FM, design 7FM or process 7FM. Failure modes like omission, incomplete and excessive belong to the category of failure of magnitude, while erratic and uneven belong to failure of variation and too quickly and too slowly belong to failure of time, rate of energy transfer or speed.

Effects (column 5) lists all the potential effects due to the specific failure mode and *Causes* (column 6) corresponds to the cause of the failure mode. Once again, it uses the 7 failure mode categories and determines their effects

and causes. Causes are identified once the potential failure modes are identified. *Prevention Controls* (column 8) of 7FM relates to the efforts taken to prevent a cause from occurring. *Detection* (column 7) is used to list the methods or tests in place to detect if something is failing before there is a serious consequence. Whenever possible, the specific test description (title/number) should be listed. The columns for which no number is assigned are not explained here as they are similar to SAE 2009 and were explained in Section 2.1.3.

This modified version of FMEA (7FM) although not that widely known to the general public yet, seems to add value to FMEA by forcing the analyst to think about the **seven** failure modes and thus help in the analysis. We were introduced to this technique by our industrial partner and results of our mapping of the outputs of this technique to STPA can be found in Chapter 5.

2.1.5 Hazard and Operability Analysis

Hazard and Operability (HAZOP) analysis is one of the most widely known techniques to identify potential hazards and to determine operational concerns of a system (Ericson II 2005). It is a well-structured and organized qualitative analysis technique. The key component of this technique is using guide words for the parameters of the system under study, and determining their deviation from the design intent. Guide words like *more of, none, higher or lesser* can be combined with system parameters like *flow, speed or pressure*.

Table 2.2 shows some example guide words and parameters. Great care should be taken to brainstorm the various parameters and guide words as they are the key elements of HAZOP analysis. Once these are identified, their

deviation from the design intent should help in generating the list of potential hazards. Ericson II 2005 summarizes this as follows:

Guide word + parameter = deviation

Table 2.2: Example of HAZOP guide words and parameters (based on Ericson II 2005)

Guide words	Meaning	Parameters
No	Design intent is not satisfied	Flow
Higher	Quantitative increase of the parameter	Temperature
Reverse	Opposite of the design intent	Pressure

The main steps of the HAZOP process once the parameters and guide words are identified include:

- Combine the parameters and the appropriate guide word
- Determine the hazards from the deviations
- Determine the consequences of each hazard
- List all the possible causal factors for the deviations
- Provide corrective actions or recommendations to mitigate against those hazards
- Provide qualitative measure of the risk if required

All the above steps can be documented using the HAZOP worksheet as shown in Figure 2.8, which is presented in Ericson II 2005. The amount of detail included can vary depending on the project and the specific purpose of performing the analysis.

Although the HAZOP technique is easy to learn and perform, it is time consuming and strongly depends on the skills of the team. The main shortcoming of this technique is its focus on single events and not combinations

HAZOP Analysis										
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments

Figure 2.8: HAZOP worksheet (Ericson II 2005)

of possible events (Ericson II 2005). Moreover, if any important guide words or parameters are missed during the initial stages of analysis, identification of some important hazards could be missed. Since HAZOP is not the main focus of the thesis, more details are not presented here.

2.2 ISO 26262

ISO 26262 (ISO26262 2011), published in late 2011, is an adaptation of the functional safety standard, IEC 61508 (IEC 2010). ISO 26262 addresses functional safety of road vehicles that include *Electrical and/or Electronic (E/E)* systems (ISO26262 2011). The goal of the standard is to provide guidance to avoid unreasonable risks due to systematic failures and random failures (ISO26262-10 2012). ISO 26262 emphasizes the "need to provide evidence that all reasonable system safety objectives are satisfied" (ISO26262 2011). The standard contains requirements and guidelines for the automotive safety lifecycle including management, development, production, operation, service

and decommissioning of the system to ensure that a sufficient and an acceptable level of safety is being achieved (ISO26262-1 2011). ISO 26262 provides a risk based approach using the *Automotive Safety Integrity Level (ASIL)*, to classify the hazardous events according to the risk level i.e. ASIL A, B, C, D, where ASIL A is the lowest safety integrity level and ASIL D the highest one. These four levels specify the stringency of requirements of ISO 26262 and safety measures that should be followed to avoid unreasonable risks (ISO26262-1 2011). Another class, *Quality Management (QM)* exists to denote there is no safety requirement to comply with.

ISO 26262 consists of ten parts and each part is further divided into clauses. The clauses consist of several requirements that need to be fulfilled to produce *work products*. Work products are a "result of one or more associated requirements of ISO 26262" (ISO26262-1 2011). Some of these work products along with other information can be required as a prerequisite for other clauses of the standard. The specific activities related to the product development are described using a V-model in the ISO 26262 standard. Part 1 of the standard defines the various terms and abbreviations used throughout the standard. Part 2 specifies the requirements and recommendations for the management of functional safety during different phases of the safety lifecycle. Part 3 specifies the requirements for the concept phase, while Parts 4, 5 and 6 concern the product development at the system, hardware and software level respectively. Part 7 specifies the requirements for the production, operation, service and decommissioning phase. Part 8 specifies requirements for supporting processes and Part 9 specifies the requirements for ASIL-oriented and safety-oriented analyses. Part 10 provides informative guidelines on ISO 26262 using additional explanations and "enhances the understanding" of the other parts of the

standard. Since our goal is to analyze if STPA can be used in the context of ISO 26262, our work focuses on Part 3 - the concept phase of ISO 26262 which defines the requirements to fulfill when performing hazard analysis. Therefore Part 3 of ISO 26262 will be covered in the following subsection (Section 2.2.1).

2.2.1 Concept Phase of ISO 26262

The concept phase of ISO 26262 includes four main clauses: Item Definition, Initiation of the Safety Lifecycle, Hazard analysis and Risk Assessment, and Functional Safety Concept (ISO26262-3 2011). Figure 2.9 shows the relations between the clauses, along with the input and output work products. The numbers written inside the dotted box are in the form of *m-n*, where *m* corresponds to the particular part of the ISO 26262 standard and *n* corresponds to the clause number within that part. Thus *m-n* points us to the specific part and clause of the standard which contains the requirements to obtain that work product.

If needed, Item Definition, Initiation of the Safety Lifecycle, and Hazard analysis and Risk Assessment clauses can use any relevant further supporting information from other independent items (external source) (ISO26262-3 2011). Similarly, the *Functional Safety Concept (FSC)* clause can make use of further supporting information about the preliminary architectural assumptions from external sources (ISO26262-3 2011). Since they are only optional information, they are not discussed in this thesis.

Before the clauses are presented in more detail, a number of important terms are defined in Table 2.3, taken from the ISO 26262 standard (ISO26262-1 2011).

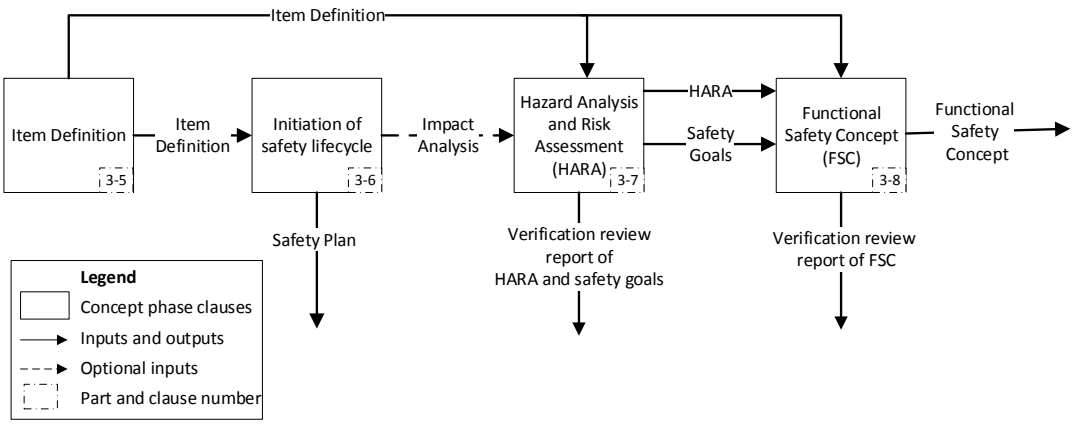

Figure 2.9: Overview of ISO 26262 concept phase (Based on ISO26262-3 2011)

Table 2.3: Definitions of terms in the concept phase of ISO 26262

Term	Definition
Item	system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied
Hazard	potential source of harm caused by malfunctioning behaviour of the item
Operational situation	scenario that can occur during a vehicle's life Example: Driving; parking; maintenance
Operating mode	perceivable functional state of an item or element Example: System off; system active; system passive; degraded operation; emergency operation
Hazardous event	combination of a hazard and an operational situation
Malfunctioning behaviour	failure or unintended behaviour of an item with respect to its design intent

Item Definition clause provides the requirements for defining the item[2] under study, identifying its dependencies and its interactions with the environment and other items (ISO26262-3 2011). According to this clause, potential consequences of known hazards and failure modes as well as the legal requirements, national and international standards which impact the item must be identified

[2]Item is defined as "system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied" (ISO26262-1 2011)

(ISO26262-3 2011). The resulting output of the clause is the *item definition* work product.

Initiation of the Safety Lifecycle clause helps determine if the item under study is a new item or a modification of an existing item. In the case of a modification, the results of an *impact analysis* are used to tailor the safety-related activities and update the safety plan. The analysis is performed based on the *item definition* work product produced by following the requirements of the item definition clause. In the case of a new development, we proceed to the next task i.e., the Hazard Analysis and Risk Assessment.

Hazard Analysis and Risk Assessment Our study focuses mainly on the Hazard Analysis and Risk Assessment clause of the concept phase as STPA is a hazard analysis technique. The *item definition* work product is a necessary prerequisite and the *impact analysis* work product is an optional input to this clause. The HARA clause includes subclauses: Situation Analysis, Hazard Identification, Classification of Hazardous Events, and Determination of ASILs and Safety Goals.

The Situation Analysis determines "the operational situations and operating modes in which an item's malfunctioning behaviour will result in a hazardous event"(ISO26262-3 2011). This subclause deals with listing the operating modes and operational situations that can occur during the vehicles' lifetime like system off, driving, etc. The hazard identification subclause involves identifying the vehicle level hazards, the hazardous events and its consequences. The standard suggests determining the hazards using suitable techniques, e.g., brainstorming, FMEA. Hazardous events are determined by considering the hazards in different operational situations identified during

the situation analysis. The hazardous events are classified using impact factors *Severity (S)*, *Probability of Exposure (E)* and *Controllability (C)*. The severity is estimated based on the extent of potential harm to each person potentially at risk (ISO26262-3 2011). The parameter ranges from S0 to S3 and shall be assigned in accordance with Figure 2.10 (ISO26262-3 2011). The standard suggests using the *Abbreviated Injury Scale (AIS)* to characterize the severity (ISO26262-3 2011). The probability of exposure of each operational situation is "estimated based on a defined rationale for each hazardous event." It is valued from E0 to E4 and shall be assigned in accordance with Figure 2.11 (ISO26262-3 2011). The controllability factor, ranged from C0 to C3, is an estimation of the ability of the driver or other persons potentially at risk to control the hazardous event. Controllability factor shall be assigned in accordance with Figure 2.12 (ISO26262-3 2011).

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Figure 2.10: Classes of severity (ISO26262-3 2011)

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Figure 2.11: Classes of probability of exposure regarding operational situations (ISO26262-3 2011)

	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Figure 2.12: Classes of controllability (ISO26262-3 2011)

The determination of ASILs for each hazardous event is based on the estimated values of the severity, probability of exposure and controllability parameters in accordance with Figure 2.13. In addition to four ASIL levels (A, B, C, D), a class QM exists to denote there is no safety requirement to comply with. Also, if a hazardous event is assigned to the class S0 or E0 or C0, no ASIL assignment is required (ISO26262-3 2011).

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

Figure 2.13: ASIL determination (ISO26262-3 2011)

For each hazardous event with an assigned ASIL, a *Safety Goal* shall be determined as a top-level safety requirement for the item (ISO26262-3 2011). The ASIL identified for a hazardous event shall also be assigned to the associated Safety Goal. Similar safety goals shall be combined into a single one. In the case when there is any difference in their ASILs, the highest ASIL level should be considered for the combined Safety Goal.

Following the HARA clause, three work products are generated: 1) the *HARA* work product which includes a list of the operational situations and

operating modes, the vehicle level hazards and hazardous events with their assigned ASILs, 2) the *Safety Goals* of the item, and 3) a *Verification Review Report of the HARA and Safety Goals*.

The ***Functional Safety Concept (FSC)*** clause helps derive the *Functional Safety Requirement (FSR)* from the item's safety goals. The standard suggests using safety analyses like FMEA, FTA and HAZOP to support the FSR specification. The objectives of the FSC clause also involves allocating the FSRs to the corresponding elements of the preliminary architecture. Item Definition, HARA and Safety goals work products are inputs to the FSC clause. Preliminary architectural assumptions are further supporting information. The resulting work products from the FSC clause are the *Functional Safety Concept* and a *Verification Review Report of the Functional Safety Concepts*.

In our analysis, we will not address the production of the *Verification Review Report of HARA and Safety Goals*, and the *Verification Review Report of FSC*. These work products mainly must include arguments to help ascertain a certain level of confidence on the sufficiency and the correctness of artifacts defined during the product development process. Since we are mainly interested in determining how to obtain the results of following the requirements of HARA,the verification review report work product will not be discussed in this thesis.

2.3 Related Work

This section presents the literature review on the work done related to ISO 26262, STPA and some traditional hazard analysis techniques.

2.3.1 Work Done on Comparing FTA and FMEA with STPA

This section reviews some of the work done to compare STPA with some of the traditional techniques like FTA, FMEA etc.

Stringfellow et al. 2010 and Ishimatsu et al. 2014 have applied STPA in the aerospace domain. Stringfellow et al. 2010 applied STPA on the *Traffic Collision Avoidance System (TCAS)* and compared it with an already existing Fault Tree analysis. According to Stringfellow et al. 2010, "STPA generated all the potential scenarios that are in the fault tree" and "also generated additional scenarios, at least one of which resulted in an aircraft collision and great loss of life." These additional scenarios were a result of unsafe interactions between the components and not due to component failure. Ishimatsu et al. 2014 compared STPA results with existing FTA results of *Japan Aerospace Exploration Agency (JAXA) H-IIB Transfer vehicle (HTV)*. STPA identified all the causal factors identified by FTA, and additional causal factors addressing operator error and process model inconsistency, among others. Thus according to Stringfellow et al. 2010, Ishimatsu et al. 2014, STPA has helped identify hazardous scenarios in the aerospace domain, that were not previously identified when using FTA.

Song applied STPA on the Nuclear Darlington Shutdown system and compared the results with the original FMEA results (Song 2012). The author

found that, when compared to FMEA, STPA identified more hazards, failure modes and causal factors, including inadequate control algorithms, missing feedback and an incorrect logic model (Song 2012).

Abdulkhaleq and Wagner 2015 show the results of quantitative comparison of STPA with FTA and FMEA when applied on three safety-critical systems. The safety-critical systems analyzed were train door control, anti-lock braking and traffic collision and avoidance. The paper concluded with the results that STPA covered more types of software safety requirements (e.g., missing feedback, missing input, wrong output) than FTA and FMEA. According to Abdulkhaleq and Wagner 2015, STPA was more time consuming for novice safety analysts, when compared to FTA and FMEA.

Goerges 2013 presented the results of applying STPA in commercial product development. The author claims that STPA allowed the design team to identify more causal factors for quality losses than FMEA or FTA, e.g., component interactions, software flaws, and omissions and external noises (Goerges 2013).

Sotomayor 2015 presented the results of a comparison of STPA with automotive FMECA on an *Electric Power Steering (EPS)* system. More specifically, Sotomayor 2015 presents the results of the analysis in terms of the types of accident causes identified by both the techniques. Sotomayor's analysis claimed that STPA identified 137 causes in comparison to FMECA which identified 95 causes, although there were overlaps. Breimer 2013 used STPA technique to perform hazard analysis on an *Adaptive Cruise Control (ACC)* for a hybrid electric vehicle. The author found that STPA helps one to better understand the system and identify its vulnerabilities in addition to finding out how to mitigate them. In the automotive industry, GM has shown inter-

est in using STPA in a case study. In Sundaram and Hartfelder 2013, GM compared the safety requirements derived from applying STPA against those derived by following the GM system safety process steps. They found that the overall safety requirements derived from the GM safety analysis activities were compatible with the requirements obtained with STPA. In D'Ambrosio et al. 2014, the experience from applying STPA to an automotive shift-by-wire system was presented. STPA, as an iterative process, was found to work well as effort moves from the concept level to a more detailed design level.

2.3.2 Related Work on STPA and ISO 26262

In this section, we discuss existing work relating ISO 26262 and STPA.

In Hommes 2012b, Hommes discusses strengths and weaknesses of the techniques suggested in the ISO 26262 standard. The author suggests the use of techniques based on system safety engineering principles, especially STPA to guide the analysts in the hazard identification and elimination. The paper also points out the potential subjectivity involved in the assessment of probability of exposure and thus suggests the consideration of the severity level alone for the ASIL assessment. As argued in Hommes 2012b, the hazard analysis techniques mentioned in ISO 26262 are not sufficient to handle the growing complexity of modern software intensive safety-critical systems. The amount of interest and attempts in using STPA in various safety-critical domains show that there is something about STPA that has caught the attention of safety experts and hence is being tried and studied. However, STPA, being mainly a hazard analysis technique does not involve ASIL determination, which is an important component of the HARA of ISO 26262 and hence, "vanilla" STPA

does not follow an ISO 26262 compliant process.

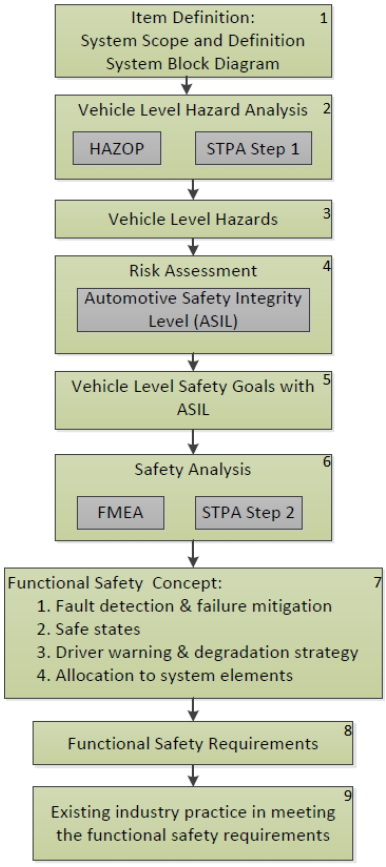

Figure 2.14: Analysis process and approaches based on Hommes 2015

To the best of the author's knowledge, no detailed work exists to show how STPA can be used in an ISO 26262 compliant process. The closest to an investigation of the topic is an analysis of how three hazard analysis techniques, HAZOP, STPA, and FMEA, could be used in the concept phase of development as per ISO 26262 as presented in Figure 2.14 from Hommes 2015. The figure indicates that HAZOP and STPA Step 1 would help in the vehicle level hazard identification (blocks 2, 3). STPA Step 1, in general, does not generate a list of hazards, but mainly identifies the unsafe control actions and links them to the hazards. However, new hazards not identified during Step

0 may be discovered during the determination and analysis of unsafe control actions. According to the figure, FMEA and STPA Step 2 may support the determination of Functional Safety Concept and hence Functional Safety Requirements (blocks 6, 7, 8). This work presents a rough, high-level view of how STPA can be used in the concept phase of a process compliant with ISO 26262. In this thesis however, we perform a detailed analysis of the topic, including detailed terminology mappings, and demonstration of how STPA can help satisfy relevant requirements of the standard based on the detailed analysis of the standard's clauses.

In the aerospace industry, Leveson et al. 2014 compares STPA and the safety assessment process of ARP 4761, an Aerospace Recommended Practice from SAE International. The goal of the report was to demonstrate that "STPA is potentially more powerful than the traditional hazard analysis methods and approach used in ARP 4761" by comparing the approaches and the type of results obtained. The report concludes that the traditional safety assessment processes used in ARP 4761 omits important causes of aircraft accidents when compared to STPA, and thus the traditional methods are not sufficient. Although the report represents a comprehensive comparison, it only explores the causal factors that are identified by STPA but not by ARP 4761 and not the other way around.

Most automotive industries are moving towards following an ISO 26262 compliant process and in this thesis, we provide guidelines on how STPA can help us achieve the work products mandated by the HARA of ISO 26262. We improve on the method suggested in (Hommes 2015) and also include a comparison of STPA and ISO 26262 following a similar structure to Leveson et al. 2014. Thus, this thesis shows how STPA can be augmented to help

generate ISO 26262 compliant outputs obtained as a result of following the requirements of the concept phase of ISO 26262, mainly, the HARA outputs.

Chapter 3

Using STPA in an ISO 26262 Compliant Process

In this chapter, we first compare the basic foundations of ISO 26262 and STPA, explaining why STPA is a good candidate to be used in an ISO 26262 compliant process (Section 3.1). We then compare the central terminologies used in ISO 26262 and STPA (Section 3.2), which further lays the groundwork for the next section. In Section 3.3, we first present our approach of how the results of STPA can help generate the outputs of following the requirements of HARA and its related clauses in the concept phase of ISO 26262 (Section 3.3.1). In Section 3.3.2, we present our analysis of which parts and/or subclauses of the ISO 26262 standard refer to the traditional hazard analysis techniques and also determine if the requirements of those subclauses can be supported using STPA. Finally, in Section 3.3.3, we summarize our approach for using STPA in an ISO 26262 compliant process.

3.1 STPA versus ISO 26262: Comparing Foundations

The key results of comparing the foundations are presented below and shown in Table 3.1.

Both ISO 26262 and STPA are based on a systems engineering framework with the aim of building safety into the system right from the beginning, not as an afterthought. ISO 26262 emphasizes the need for safe system development processes and system safety engineering. STPA is based on Systems-Theoretic Accident Model and Processes (STAMP), which is also built on systems safety and systems theory. Systems theory is especially useful for complex systems where analyzing the interacting subsystems as separate entities could give inaccurate results. Such complex systems require a technique which focuses on the system in its entirety and not as a sum of individual subsystems (Leveson 2011). The main ideas behind systems theory are: 1) Emergence and Hierarchy and, 2) Communication and Control (Leveson 2011). Safety being an emergent system property emphasizes that the safety of the whole system cannot be guaranteed just by proving that the individual components that make up the system are safe. System hierarchy is used to explain the relationships between different levels characterized by emergent properties of the system. Communication and control focus on control theory and imply that accidents may occur when inadequate control actions violate the safety constraints of the system. ISO 26262 follows a hierarchical approach where higher level safety goals are enforced by the lower level safety requirements (ISO26262-3 2011). This is similar to STPA's approach where the safety constraints are refined at each level and the higher level safety constraints are enforced by the lower

Table 3.1: Comparing foundations of ISO 26262 and STPA

	HARA clause of ISO 26262 (ISO26262-3 2011)	STPA (Leveson 2011)	Remarks
Characteristics	Hierarchy of safety constraints Safety requirements are refined as we proceed from the high level (safety goals) to the lower level technical safety requirements	Hierarchy of safety constraints Safety constraints are refined at each step as we proceed from STPA Step 0 to Step 1 and then Step 2	Since both are based on systems development processes and follow a hierarchical approach, STPA is a good candidate for this study
Stage of application	Based on functional behaviour, hence can be applied even in the early stages when design information is not available	STPA does not need detailed design, hence can be applied at any stage, even in the concept phase	Thus both HARA of ISO 26262 and STPA can be applied at any stage of the safety lifecycle Both are iterative in nature
Objectives	Identify the hazards, classify the hazardous events according to ASILs and formulate the safety goals to prevent or mitigate the hazardous events to avoid unreasonable risk	Identify the hazards and accidents associated with the system, determine the scenarios leading to the hazards, identify the causal scenarios and determine safety constraints to eliminate, mitigate or control them	HARA of ISO 26262 is aimed to assess risk in addition to analysing and mitigating the hazards, whereas STPA is geared towards assessing and mitigating the hazards
Results	A set of hazards and classification of the hazardous events according to ASILs A safety goal shall be determined for each hazardous event with an ASIL. This is followed by the verification review	STPA results in identifying a set of accidents, hazards and safety constraints to mitigate/control against the hazards and their causes	HARA of ISO 26262 is aimed to assess risk in addition to analysing and mitigating the hazards, whereas STPA is geared towards assessing and mitigating the hazards

level safety constraints in a top down manner. Thus, the safety constraints and/or requirements derived in STPA and ISO 26262 respectively are hierarchical in nature. Since STPA has the same basic foundation as ISO 26262, i.e., a systems development process, it is reasonable to believe that STPA might be well suited for hazard analysis in a process compliant with the ISO 26262. Moreover, unlike the traditional hazard analysis techniques, STPA considers the entire socio-technical system in the hazard analysis, and an operator is also treated as an integral part of the analysis (Leveson 2011). This is one of the many reasons why STPA is gaining popularity in various safety-critical industries. Based on our discussions with ISO 26262 experts from different parts of the world, we have received varied opinions on the question of "In ISO 26262, do we consider the driver to be a part of the hazard analysis of an item?" Although there does not seem to be a common consensus, for our analysis we have considered the driver to be a part of the hazard analysis of an item.

HARA as per ISO 26262 is based on the functional behavior of the system, thus a detailed design of the system does not necessarily need to be known (ISO26262-3 2011). Similarly, STPA can also be performed before a detailed design is available and can be applied as early as the concept phase (Leveson 2011). Hence, both the HARA and the STPA processes can be applied at a very early stage of development. Furthermore, both the HARA and STPA processes are iterative in nature i.e., after performing the hazard analysis, steps are taken to eliminate/mitigate/control the identified hazards and their causes. Then, the system is analyzed again to see if these elimination/mitigation/control measures introduce any new hazards. Thus, the hazard analysis is performed repetitively until the system is free of unreasonable risks.

The key difference between the STPA and the HARA process of ISO 26262 is the risk assessment process. Risk assessment according to the concept phase of Part 3 of ISO 26262 involves determining the impact factors, i.e., Severity (S), Controllability (C) and Probability of Exposure (E), and using those to assign an Automotive Safety Integrity Level (ASIL) to each of the hazardous events. Tables shown in Figures 2.10, 2.12 and 2.11 are used to determine the S, C and E respectively. These impact factors can then be used in the table shown in Figure 2.13 to determine the ASIL. ASIL levels help determine the stringency of the requirements and the safety measures needed to avoid what the standard considers to be unreasonable risks. But STPA, mainly focuses on the ways in which the hazards could occur and the causes behind them. STPA very specifically considers *severity of consequence* alone. It does not recommend the use of likelihood factors like controllability and probability of exposure (Hommes 2012c). Leveson 2011 discusses the difficulty and inaccuracy in assigning values to these parameters where there are cases of non-random failures and in the case of newer systems with most of the software being new, there is a lack of historical information. In fact, Hommes 2012b discusses how assigning values to the likelihood factors could result in inappropriate lowering of the stringency of requirements. Due to the possible subjectivity involved in determining the E and C factors as mentioned in Leveson 2011 and Hommes 2012b (Section 2.3.2), they suggest that only the S factor be used to categorize the hazards. Our own opinion is that consideration of S alone is safer. However, to use STPA in an ISO 26262 compliant process, we have to determine, and use, the C and E factors as well. Since we believe that STPA has the potential to improve on traditional hazard analysis techniques in the automotive domain, and we have already seen a gap between

what STPA considers and what ISO 26262 requires for compliance, we need to further analyze differences and commonalities between the two. This is the motivation for the remaining sections in this chapter.

3.2 Comparison of Terminologies of ISO 26262 and STPA

In this section, we compare the main terminologies of ISO 26262 and STPA. One of the major challenges we encountered during the course of our work was the inconsistency between the terms used in various hazard analysis techniques and standards. Although ISO 26262 tries to overcome this by having a dedicated vocabulary section (Part 1 of the standard - ISO26262-1 2011), the definitions of some of the terms are still ambiguous as we will see in this section (e.g. ISO 26262's definition of failure). This thesis presents an explicit comparison between the terms used in HARA as per ISO 26262 and in STPA. Table 3.2 presents definitions of central terms used by ISO 26262 and STPA as defined in ISO26262-1 2011 and Leveson 2011 respectively.

Both ISO 26262 and STPA use similar definitions for the term *hazard*. According to our interpretation, ISO 26262's definition of *hazard* means something that has the potential to cause *harm* or lead to an *accident*, due to *malfunctioning behaviour* of an item. According to Ladkin 2005, STPA's definition of *hazard* is interpreted as "a system state, which in combination with the most unfortunate environment state, results inevitably in (is a sufficient causal factor of) an accident". STPA's definition points out the need for the right combination of environmental conditions to be present for a *hazard* to

Table 3.2: Definitions of terms in ISO 26262 and STPA

Term	ISO 26262 (ISO26262-1 2011)	STPA (Leveson 2011)
Hazard	Potential source of harm caused by malfunctioning behaviour of the item	A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss) Peter Ladkin's interpretation of STPA's Hazard definition "a system state, which in combination with the most unfortunate environment state, results inevitably in (is a sufficient causal factor of) an accident" (Ladkin 2005)
Malfunctioning behaviour	Failure or unintended behaviour of an item with respect to its design intent	
Failure	Termination of the ability of an element, to perform a function as required Note: Incorrect specification is a source of failure	No explicit definition A failure in engineering can be defined as the non-performance or inability of a component (or a system) to perform its intended function
Accident	No explicit definition	An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
Harm	Physical injury or damage to the health of persons	
Hazardous event	Combination of a hazard and an operational situation	

lead to an *accident*. The words *potential source of harm* from ISO 26262's *hazard* definition, as well as from the Figure 3.1 extracted from ISO 26262 Part 10 indicate that a *hazard* does not necessarily lead to an *accident*. The occurrence of an *accident* depends on "whether the persons at risk are actually exposed

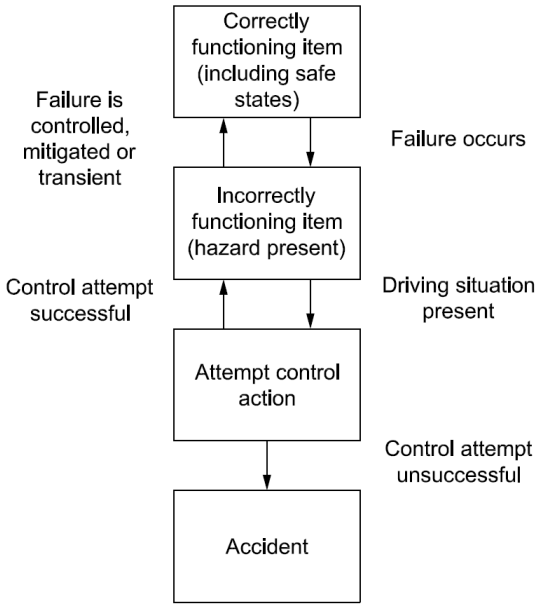

Figure 3.1: Example showing hazard, failure, accident (ISO26262-10 2012)

to the hazard in the situation in which it occurs, and whether they are able to take steps to control the outcome of the hazard" (ISO26262-10 2012). Thus, both ISO 26262 and STPA emphasize the need for appropriate environmental conditions to be present for the *hazard* to lead to an *accident*. The notable difference we infer from the definition of *hazard* is that STPA does not limit the *hazards* to those caused by *malfunctioning behaviour*, unlike ISO 26262. To be certain, we need to check what exactly is covered by *malfunctioning behaviour* of the item.

Malfunctioning behaviour is defined as "Failure or unintended behaviour of an item with respect to its design intent", where *failure* is defined as "Termination of the ability of an element, to perform a function as required" (ISO26262-1 2011), and, there is no explicit definition for *unintended behaviour*. Thus, according to the available definitions, the standard seems to consider an item as malfunctioning only if it does not adhere to the design intent. Based on

the definitions alone, flawed requirements, incorrect specification, etc., do not seem to be considered as *malfunctioning behaviour*. However, there is a 'Note'[1] under the definition of *failure* as, "Incorrect specification is a source of failure" (ISO26262-1 2011). But based on our understanding, 'incorrect specification' could lead to *malfunctioning behaviour* and not really a source of *failure*. This is one of the instances where the standard is ambiguous and confuses the reader. The next revision of the standard should aim to clarify the definition of *failure* and *malfunctioning behaviour*.

The 'Note' under the definition of *hazards* mentions that *hazards* are identified in terms of conditions or behavior at the vehicle level (ISO26262-3 2011), whereas STPA considers *hazards* at the system level, with system being the largest unit being considered, (Leveson et al. 2014). In STPA, once the hazards are identified at the system level, they (system level hazards) can be mapped into hazardous behaviours at the component or subsystem level (Leveson 2011). More specifically, if the hazards cannot be "eliminated or adequately controlled" at the system level, they are then refined into hazards to be "handled by the system components" (Leveson 2011).

ISO 26262 does not have an explicit definition of *accident*. However, both *hazardous event* of ISO 26262 and *hazard* in presence of worst-case environmental conditions of STPA could lead to some level of loss including loss of human life, i.e. *harm* of ISO 26262. Thus, the term *harm* of ISO 26262 can potentially be mapped to the results of an *accident* of STPA. STPA's loss can include human injury or loss of human life, property damage, environmental pollution, mission loss, etc. (Leveson 2011). It is important to note

[1] According to ISO26262 2011, "Information marked as a 'NOTE' or 'EXAMPLE' is only for guidance in understanding, or for clarification of the associated requirement, and shall not be interpreted as a requirement itself or as complete or exhaustive."

that STPA's concept of loss is more general as it is meant for different stakeholders to adapt as it suits them, whereas ISO 26262 only mentions injury to people and not property damage. However, deciding on what is considered an *accident* and/or a *hazard* depends on the stakeholders. *Consequences of Hazardous Events (CoHE)* of ISO 26262 are identified by considering the consequences of the *hazard* in various *operational situations* and could potentially be mapped to the *accident* of STPA. However, *accidents* in terms of STPA are more general in nature, while the consequences determined in ISO 26262 tend be more fine-grained, since they are determined for different *operational situations* of the *hazard*. Hence, care should be taken to ensure STPA's *accidents* are refined to a correct level of detail as required in ISO 26262 process.

Although *operational situations* of the standard seem to be related to the environment conditions of STPA, we need to look into it in more detail to see how STPA could help in deriving the *operational situations*. The fact remains that even though STPA states that a *hazard* along with worst case situations (environmental conditions) will lead to an *accident*, there is no explicit step in STPA to determine the *operational situations* and STPA does not have a specific term for this. Since ISO 26262 strongly requires the determination of *ASILs*, which in turn require the *operational situations*, we need to augment STPA so that *operational situations* are explicitly listed. More details will be provided in Section 3.3.1.

3.3 An Approach to Using STPA in an ISO 26262 Compliant Process

We examined all ten parts of the ISO 26262 standard to check where hazard analysis is performed. Although various parts of the standard mention hazard analysis, the requirements to perform it are found only in the concept phase of ISO 26262. Thus, whenever hazard analysis is mentioned in any part of the standard, it refers back to the concept phase of ISO 26262. The terminology analysis (Section 3.2) and the background information provided in Section 2.2.1 (Concept phase of ISO 26262) from Chapter 2 (Preliminaries), lay the groundwork for this section. We first check how the results of applying STPA can help generate the work products of HARA and its related clauses in the concept phase of ISO 26262 (Section 3.3.1). This helps identify the gaps and additional steps that need to be followed to use STPA in an ISO 26262 compliant manner. In Section 3.3.2, we examine the standard to determine the instances where traditional hazard analysis techniques are referenced. We provide an overview of the specific subclauses where hazard analysis techniques are suggested and determine if and how STPA can support the requirements of those subclauses.

3.3.1 Mapping ISO 26262 Concept Phase and STPA Outputs

Our goal is to demonstrate how STPA could help in performing Hazard Analysis and Risk Assessment (HARA) defined in the concept phase of ISO 26262. If we want to use STPA in an ISO 26262 compliant process, STPA should help

satisfy all the requirements mentioned in the HARA clause of the ISO 26262 concept phase (ISO26262-3 2011).

Figure 3.2 shows the STPA results (as shown on the right hand side of the figure) that can help generate the outputs required by the concept phase of ISO 26262 (as shown on the left hand side of the figure). In particular, the red dashed box includes blocks numbered i2 to i10 corresponding to all the subclauses of the HARA. In cases where there is a rectangle inside another rectangle, the contents of the inner rectangle are a subset of the contents of the outer rectangle. In cases where there are ovals inside the rectangles, the ovals are the outputs of HARA that are required to determine the contents of the outer rectangle. The solid arrows from STPA blocks to ISO 26262 blocks denote that the specific STPA output can completely support the corresponding ISO 26262 block output, while the dashed arrows denote that the specific STPA output can partially support the corresponding ISO 26262 block output. The dotted arrows are used to represent cases where the results of STPA can help provide additional support in generating the output of ISO 26262. The numbers in the form of *w-x-y-z* point to the specific subclause of the standard where the requirements are specified. *w* corresponds to the specific part of the ISO 26262 standard, *x* corresponds to the specific clause and y-z corresponds to the subclauses where the requirements of the clauses and subclauses are mentioned.

As we see in Figure 3.2, outputs of blocks i1, i2, i3, i5, i10 and i11 have been mapped to STPA, and outputs of blocks i4, i6, i7, i8 and i9 have not been mapped to the outputs of STPA. To use STPA in an ISO 26262 compliant process, all the blocks of HARA need to be obtained using STPA or some additional processes. This is similar to work published by Dardar 2013, in

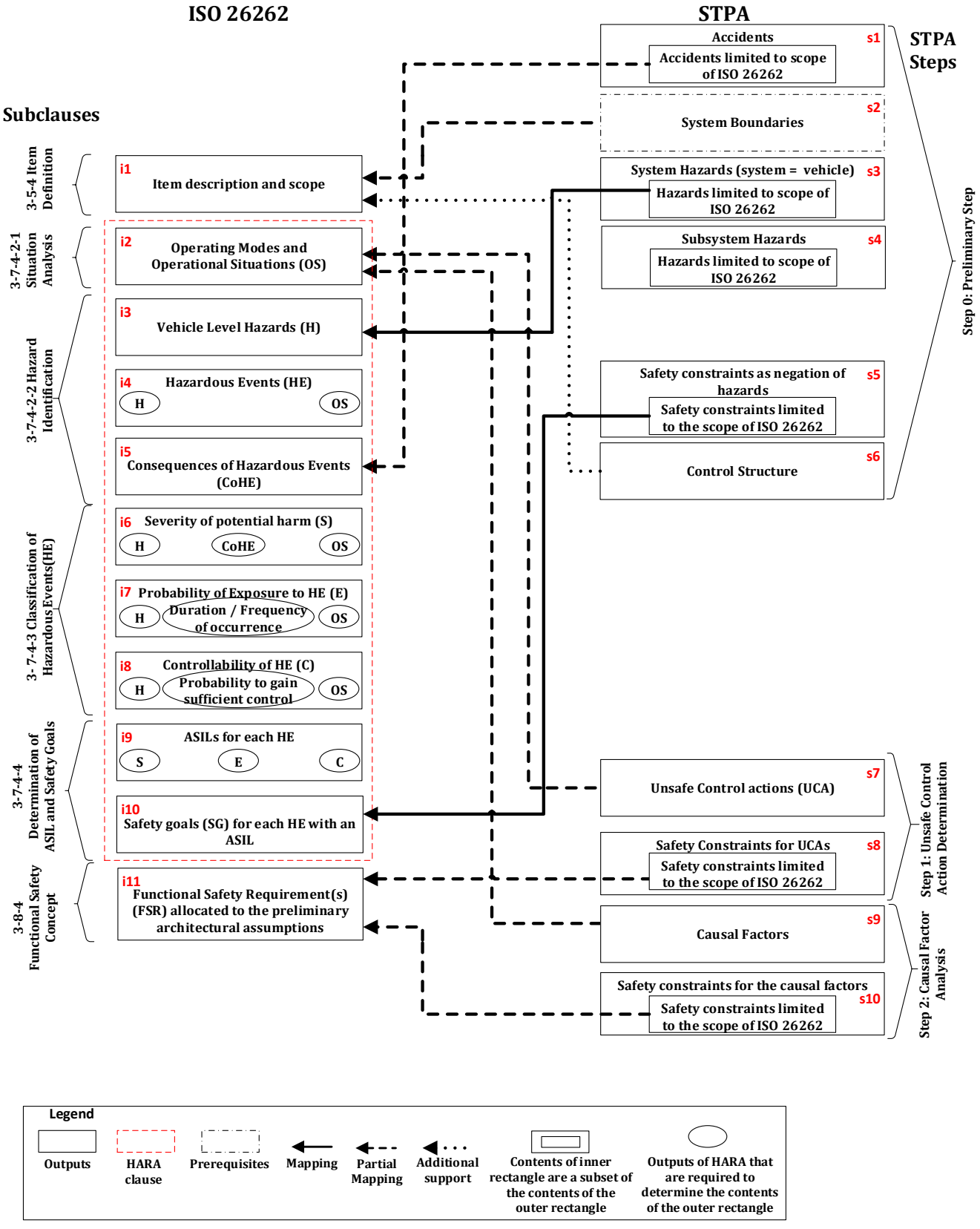

Figure 3.2: Mapping between ISO 26262 and as-is STPA

which HAZOP was to be used in compliance with ISO 26262. In Dardar 2013, the HAZOP worksheet was adapted to include more fields to "make it in compliance with ISO 26262" (Dardar 2013). We compared the adapted HAZOP worksheet shown in Dardar 2013 to the traditional HAZOP worksheet (Figure 2.8) shown in Ericson II 2005. The additional columns in Dardar 2013 were *deviation*, *hazardous event*, *operational situation*, impact factors *S, C, E* and *ASIL*. We observe that the additional columns used in Dardar 2013 for making HAZOP compliant with ISO 26262 are very similar to the unmapped blocks of ISO 26262 from Figure 3.2, i.e., the blocks i4, i6, i7, i8 and i9, corresponding to *hazardous events, severity of potential harm, probability of exposure to hazardous events, controllability of hazardous event* and *ASIL* respectively. In this section, we provide guidelines to help obtain those unmapped outputs, which results in Figure 3.3. We start with the blocks inside the red dashed box.

The **Situation Analysis** subclause 3-7-4-2-1 (block i2), generates a list of *operational situations and operating modes*, which are mainly used to determine *hazardous events* and support the estimation of their *severity, probability of exposure and controllability* parameters during *ASIL* assessment. STPA does not include an explicit step that lists the *operational situations and operating modes*. However, in STPA Step 0, when identifying *hazards* using the definition of *accident* or loss, the analyst has to consider worst-case conditions in the environment that could combine with the *hazard* to lead to an *accident*. Although the STPA process does not require one to list the worst-case conditions, there is an undocumented list of the circumstances under which a *hazard* could lead to an *accident*. If STPA is to be used in a process compliant with ISO 26262, we recommend that these various situations or circumstances be

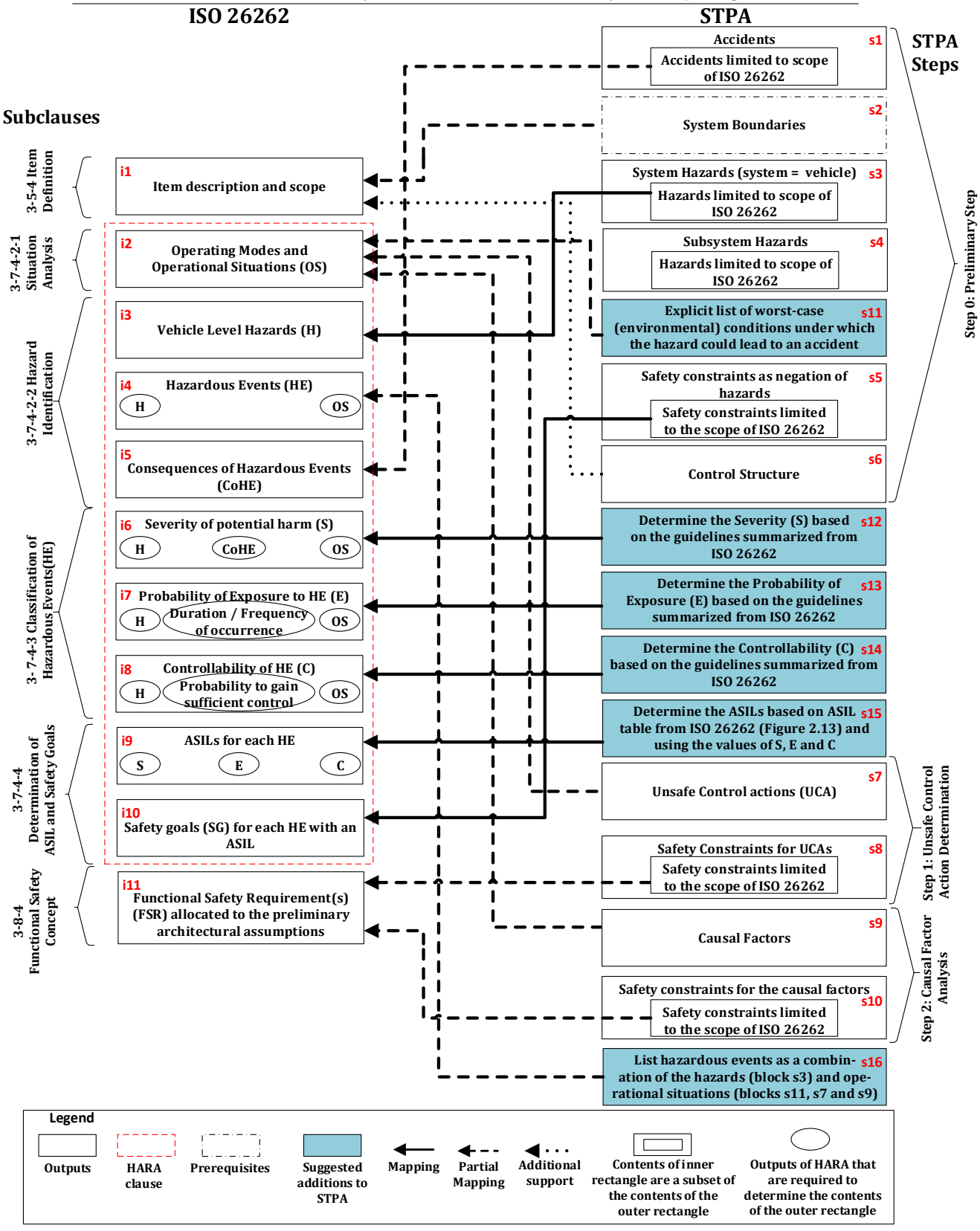

Figure 3.3: STPA in compliance to ISO 26262

listed explicitly, as shown in Figure 3.3. STPA Step 1 and Step 2 can also partially help in generating *operational situations*. The goal of *Unsafe Control Actions (UCA)* determination in Step 1 is to identify the context or conditions in which the control actions will be unsafe (*An STPA Primer, V.1* 2013). In Step 2, when analyzing the *causal factors* in STPA, we use a control loop and the guide words along with some assumptions about the system. These assumptions can help generate some of the operating modes and operational situations. We suggest that these context, conditions and assumptions along with the implicit environmental conditions from Step 0 could support the generation of the *Operating Modes and Operational Situations (OS)* (block i2). The guidelines from ISO 26262 are summarized below.

A summary of the various types of vehicle *operational situation* scenarios from ISO26262 2011 are as follows: 1) type of road, e.g., highway, intersection 2) vehicle state, e.g., high-speed driving, lane change, executing a turn, 3) road surface, including due to weather conditions, e.g., bumpy, slippery, nails present, 4) nearby elements, e.g., trailer attached, traffic congestion, 5) visibility, e.g., snow, unlit road, 6) driver distractions, e.g., unexpected radio volume increase, warning messages, unavailability or faulty components/software that affect the comfort level of the driver (faulty seat adjustment, headlight failure at night, faulty driver airbag while driving etc.). The above list is intended to help analysts think of different possible *operational situations*, and is neither exhaustive nor should it be treated as a substitute for an analyst's brainstorming activity. Moreover, depending on who is performing the hazard analysis i.e., supplier or *Original Equipment Manufacturer (OEM)* and on which system, the list of *operational situations* to be considered could vary. For example, a supplier might not have information about the different *operational situa-*

tions the system/vehicle might encounter and may only focus on the specific item level situations. It is important to not get caught up in the detailed list of *operational situations* as this might lead to too fine-grained a classification of the *hazardous events*. An overly detailed list of *operational situations* might result in "a very granular classification of *hazardous events*" and could eventually lead to "an inappropriate lowering" of an *ASIL*, which would decrease the efficiency of risk assessment using *ASILs* (ISO26262-3 2011).

As mentioned in mentioned in Section 3.3.2, the **Hazard Identification** subclause of ISO 26262 suggests using traditional hazard analysis techniques. The specific requirement of *7.4.2.2 Hazard identification* is:

"*7.4.2.2.1 The hazards shall be determined systematically by using adequate techniques.*

NOTE Techniques such as brainstorming, checklists, quality history, FMEA and field studies can be used for the extraction of hazards at the item level."

We looked into the standard FMEA technique (SAE 2009) to see how *hazards* are identified. As explained in Section 2, FMEA results are documented in the form of a worksheet and based on the SAE 2009 version of FMEA, there is no column called *hazard*. However, as we will see in Chapter 5, the *effect*[2] of FMEA could be mapped to *hazard* of STPA. Determining the *effects* in FMEA is mainly a brainstorming activity and some of the main limitations of FMEA are: it considers "only single item failures and does not consider mishaps resulting from failure combinations" (Ericson II 2005). Thus Lindland 2007 and Ericson II 2005 suggest that one should not solely rely on FMEA for *hazard* identification.

The identification of *vehicle level hazards* (block i3) as required by ISO

[2]effects can be considered as consequences or results of each of the failure modes

26262 can be supported when using STPA since Step 0 of STPA involves identifying *system level hazards*. As discussed in Section 3.2, in ISO 26262, *hazards* should be identified at the vehicle level (ISO26262-3 2011). In STPA, the *hazards* are identified at the system level, with system being the largest unit under consideration (Leveson et al. 2014). It is important to recall that in STPA, if the system level hazards cannot be "eliminated or adequately controlled" at the system level, they are then refined into hazards to be "handled by the system components" (Leveson 2011). Based on our discussion with safety experts from our industrial partner, the ISO 26262 hazard level depends on who is identifying the *hazard* and during which phase of development. For example, if a supplier is building/designing an item that can be used in different parts of the automotive system, they might not necessarily have enough information about the *hazards* at the next higher level, considering it could vary depending on where and under which *operating situations* it is used. In such cases, the *hazards* would be identified at the item level. Otherwise, *hazards* are identified at the vehicle level and then, if needed, they are refined to the item level. Similarly, if the analysis is performed during the concept phase, there may not be much information available regarding what items constitute the system. Note that our comparison of *hazard* definitions mentioned in Section 3.2 shows that STPA's definition of *hazard* could be more inclusive than the ISO 26262's definition of *hazard*. STPA Step 1 can also partially support in the identification of the *vehicle level hazards* because experience shows that new *hazards* can be identified while determining and linking the *unsafe control actions* to *hazards* (Hommes 2015). Since linking the *unsafe control actions* to *hazards* is an intermediate step, to reduce complexity of the figure, it is not documented in Figure 3.2.

Obtaining the *hazardous events* (block i4) as a combination of *operational situations* and *hazard* is straightforward when the *operational situations* are identified. Thus *hazards, operating modes and operational situations* are represented as parameters needed to derive the *hazardous events*. As shown in Figure 3.3, the *hazardous events* can be obtained in STPA by combining the results of block s3 with blocks s11, s7 and s9.

Documenting the *consequences of hazardous events* (block i5) can be partially supported by STPA. ISO 26262 describes the *consequences of hazardous events* as effects that can occur for a given *hazard* in different *operational situations* (ISO26262-3 2011). The consequences result in various levels of injuries including loss of human life as it is the case for the identified *accidents* in STPA Step 0. Hence the *accident* identification step of STPA may be used to identify the hazardous event's *consequences*. However it is important to reiterate the fact that *accidents* of STPA are general in nature and may not be as fine-grained as the standard's *consequences of hazardous events*, as STPA does not consider the presence of the *accident* in *different operational situations*. Thus, we say STPA can *partially* support deriving the *consequences of hazardous events*. Additionally, it is important to note that the order of identification of *hazards* and *consequences/accidents* vary in the standard and in STPA. The standard first identifies the *hazard* and then determines what could be the *consequences of the hazard*, whereas STPA first identifies what are considered as *losses/accidents* for the system and then identifies what *hazards* could cause them. There are varied opinions about which way is better, but it is not the focus of this thesis.

The **Classification of hazardous events** is about estimating values for the impact factors *S, E* and *C* in order to assign an *ASIL* to the *hazardous*

events (blocks i6, i7, i8 and i9). *S* can be estimated considering the *hazardous events* and the *consequences* that can occur in various *accident* situations (ISO26262-3 2011). The standard suggests using injury scales like the Abbreviated Injury Scale (AIS) and *Maximum Abbreviated Injury Scale (MAIS)* in accordance with the table presented in Figure 2.10 to help determine the *S* of the *consequences of the hazardous events*. STPA does not recommend probabilistic risk assessment. However, Leveson points out the possible use of "prioritizing or assigning a level of severity to the identified losses when tradeoffs among goals are required in the design process" (Leveson 2011). The *severity* suggested in Leveson 2011 is not the same as estimating the *severity* in ISO 262626. In ISO 26262, the *severity* is based on the *hazards*, *operational situations*, and *consequences of the hazardous event*. Thus, based on the *operational situations*, the *hazard* might lead to a different consequence. However, *severity*, as it appears in STPA, is based on the *severity of consequence* alone. Nevertheless, using the results obtained from block i2, i3 and i5 i.e., *operational situations, hazards and consequences of hazardous events*, we can estimate the *S* impact factor (block i6). Similarly, as shown in Figure 3.3, using the guidelines summarized from ISO 26262, we can determine the *S* impact factor by adding the applicable process to STPA.

Estimation of both *E* and *C* requires the results from previous blocks (block i2 - *operational situations* and block i3 - *hazards*). Additionally, to determine *E*, one should evaluate the duration or the frequency of occurrence of driving and operating situations in which a *hazard* can occur. The table in Figure 2.11 can be used as guidance to determine the *E* parameter. Estimating *C* involves estimating the probability that the driver or other persons at potential risk are able to gain sufficient control of the *hazardous event* to avoid the specific

harm (ISO26262-1 2011). The table in Figure 2.12 can be used as a guideline to determine the *C* parameter. Similarly, as shown in Figure 3.3, using the guidelines summarized from ISO 26262, we can determine the impact factors *E* and *C* in the STPA process. The appendix of ISO 26262 Part 3 contains some examples of *S, E* and *C* to guide with the classification of *hazardous events*. Based on literature review (Hommes 2012c) and our discussion with safety experts from our industrial partner, it appears that there is no standard set of guidelines across the suppliers and OEMs to determine these impact factors and hence is quite subjective. It would be highly beneficial to have a common standard between the various OEMs and suppliers to determine these impact factors to ensure consistency in the results of hazard analysis. SAE International has taken a positive step in this direction by presenting an SAE recommended practice to "provide guidance for identifying and classifying hazardous events, which are as per ISO26262 2011" (SAE 2015). Although this is taking us one step forward, the current focus of the SAE 2015 document is limited to collision related hazards and not the wider scope of ISO 26262. Review of SAE 2015 is beyond the scope of this thesis.

Once the *hazardous events* are classified as per ISO 26262's guidelines, the values of the impact factors obtained from blocks i6, i7 and i8 are used to determine an *ASIL* (block i9) using the table shown in Figure 2.13. If any of the impact factors have the least value i.e., S0 or E0 or C0, an *ASIL* is not determined and *QM* is assigned to denote that there is no need to comply with ISO 26262 requirements. Similarly we can determine the *ASIL*s in the STPA process using the values of the impact factors from previous blocks and table shown in Figure 2.13.

STPA can be used to determine the *safety goals* of ISO 26262 (block i10)

using *safety constraints* derived in Step 0 of STPA. According to ISO26262-3 2011, "Safety goals are top-level safety requirements for the item. They lead to the functional safety requirements needed to avoid an unreasonable risk for each hazardous event." *Safety constraints* are derived in STPA Step 0 by negating the *hazards*, which correspond to high level *safety requirements*. Thus the *safety constraints* of STPA Step 0 can be mapped to ISO 26262's *safety goals*. As mentioned earlier, the level of detail in the *safety goals* could also vary depending on how early in the development process the hazard analysis is applied.

Among the four clauses of the concept phase of ISO 26262 Part 3, the clauses other than HARA are 1) **Item Definition**, 2) **Initiation of Safety Lifecycle** and 3) **Functional Safety Concept**. STPA helps support not only the HARA outputs but also some additional work products of the concept phase of ISO 26262 i.e., Item Definition and Functional Safety Concept. **Item definition** is a prerequisite for the HARA clause and this information is presumed to be available before we start the hazard analysis. *Control structure*, one of the results of STPA Step 0, provides additional support to the item definition work product. For example, drawing the *control structure* as part of STPA Step 0 is based on the scope of the system under study and understanding its function, including the interaction between the components and its environment. STPA's safety *control structure* being hierarchical in nature and based on system's theory is additional information to help an analyst in accomplishing part of the item definition output (block i1). This result of STPA Step 0, can be an alternative diagram to clearly depict the relationship between the components. Moreover, the *control structure* being control-oriented, adds a lot of value to the item definition work product (*An*

STPA Primer, V.1 2013). Since the **Initiation of the Safety Lifecycle** clause is optional, we will not discuss it in this thesis.

To comply with the *Safety Goals* derived in HARA of ISO 26262, the **Functional Safety Concept** clause determines safety measures to be specified in the *Functional Safety Requirements (FSRs)*. As mentioned in Section 3.3.2, one of the requirement of the **Functional Safety Concept** clause suggests using some safety analyses techniques like FMEA, FTA or HAZOP. The specific requirement of *8.4.2 Derivation of functional safety requirements* is:

"*8.4.2.3 Each functional safety requirement shall be specified by considering the following, if applicable:*

a) operating modes; b) fault tolerant time interval; c) safe states; d) emergency operation interval, and e) functional redundancies (e.g. fault tolerance).

NOTE This activity can be supported by safety analyses (e.g. FMEA, FTA,HAZOP) in order to develop a complete set of effective functional safety requirements."

Thus we can see that techniques like FMEA, FTA and HAZOP are suggested to help in deriving the *functional safety requirements*. Depending on the effects and causes of the failure modes identified by the FMEA process, the analysts can derive the functional requirements. In HAZOP, the analyst has to think about the causes, consequences, hazards and recommendations for each of the deviation of the system parameters, based on the guide words selected. More about safety analyses is found in Part 9, Clause 8 of the standard and a short summary is also provided in Section 3.3.2.

The *FSRs* are defined in terms of functional redundancies, operating modes, failure mitigation strategies, etc. (ISO26262-3 2011). Building the *Functional Safety Requirements* (block i11) output can be partially supported

by STPA Step 1 and Step 2. In STPA Step 1, we derive *safety constraints* to mitigate against the *unsafe control actions*, which give us more detailed *safety requirements*. STPA Step 2 *safety constraints* specify the ways to eliminate or mitigate against the identified *causal factors* using similar concepts as the ones included in the *FSRs*, i.e., monitor and control, use fail-safe mechanism, redundancy, etc. (Hommes 2012a).

Hence, using the guidelines presented in this section along with the "as-is" application of STPA, STPA can be used to support all the outputs of ISO 26262 generated by following its HARA requirements. Essentially, we can see how the unmapped blocks of ISO 26262, as shown in Figure 3.2, can be obtained using the approach presented in this section, resulting in using STPA in an ISO 26262 compliant process, as shown in Figure 3.3. In the next section, we will present a list of all the instances where ISO 26262 refers to the various hazard analysis techniques.

3.3.2 References to Hazard Analysis Techniques in ISO 26262

In this section, we analyze all the parts of the standard to determine the instances where ISO 26262 suggests using the traditional techniques like FMEA, HAZOP and FTA. We will also determine if STPA can be used to complement and/or replace the traditional hazard analysis techniques suggested in the ISO 26262 standard.

In general, these traditional techniques are cited in the *HARA* and *Safety Analyses* clauses of the standard. The objective of HARA is to identify and categorize the hazards caused by the malfunctioning behaviour of the item and

to formulate safety goals to prevent or mitigate against the unreasonable risks caused by the hazardous events (ISO26262-3 2011). Safety analyses involve examining "the consequences of faults and failures on the functions, behaviour and design of items and elements". They also provide information on the "conditions and causes that could lead to the violation of a safety goal or safety requirement". Safety analyses also contribute to "the identification of new functional or non-functional hazards not previously identified" during HARA (ISO26262-9 2011).

3.3.2.1 Clauses referring to hazard and/or safety analysis in ISO 26262

The main clauses where the traditional hazard and/or safety analysis techniques were suggested are as follows:

1. Part 3 - Clause 7.4.2.2 Hazard identification step of ISO 26262
2. Part 3 - Clause 8.4.2 Derivation of functional safety requirements
3. Part 4 - Clause 7.4.3 Measures for the avoidance of systematic failures
4. Part 5 - Clause 7.4.3 Safety analyses
5. Part 9 - Clause 7 Analysis of dependent failures
6. Part 9 - Clause 8 Safety Analyses

1 and 2, referring to Part 3 of the standard have been covered in Section 3.3.1. The rest are discussed in this section. Some of these items refer to tables that list the different methods to perform a specific task. The degree of recommendation of each method would vary depending on the ASIL. The notations used in the tables in ISO26262 2011 are:

– "++" is to indicate that "the method is highly recommended for the identified ASIL; "

– "+" is to indicate that "the method is recommended for the identified ASIL;"
– "o" is to indicate that "the method has no recommendation for or against its usage for the identified ASIL."

Part 4 - 7.4.3 Measures for the avoidance of systematic failures:

Part 4 of the standard provides guidelines to specify the requirements for product development at the system level; and Clause 7 of Part 4 deals with the requirements specific to the system design.

The specific requirement is:

"*7.4.3.1 Safety analyses on the system design to identify the causes of systematic failures and the effects of systematic faults shall be applied in accordance with Table 1 and ISO 26262-9:2011, Clause 8*" ISO26262-4 2011. The table being referred to is shown in Figure 3.4.

Methods		ASIL			
		A	B	C	D
1	Deductive analysis[a]	o	+	++	++
2	Inductive analysis[b]	++	++	++	++
[a] Deductive analysis methods include FTA, reliability block diagrams, Ishikawa diagram.					
[b] Inductive analysis methods include FMEA, ETA, Markov Modelling.					

Figure 3.4: System design analysis (ISO26262-4 2011)

The table shown in Figure 3.4 suggests using deductive and inductive analysis techniques to identify the *causes* and *effects* of systematic faults and failures respectively. Having studied the STPA methodology, we know that STPA has an elaborate, well-structured process to determine the causes of the unsafe control actions using the causal factor analysis of STPA Step 2. The effects corresponding to *hazard* and *accident* identification of STPA Step 0, can also

be determined by following the STPA process. Thus, the safety analysis requirement 7.4.3.1 of Part 4 of the standard can be supported by STPA. ISO 26262-9:2011, Clause 8 referred to in requirement 7.4.3.1 will be discussed later.

Part 5 - 7.4.3 Safety analyses:

Part 5 of the standard provides guidelines to specify the requirements for product development at the hardware level; and Clause 7 of Part 5 deals with the requirements specific to the hardware design.

The precise requirement is:

"*7.4.3.1 Safety analyses on hardware design to identify the causes of failures and the effects of faults shall be applied in accordance with Table 2 and ISO 26262-9:2011, Clause 8*" ISO26262-5 2011. The table being referred to is shown in Figure 3.5.

Methods		ASIL			
		A	B	C	D
1	Deductive analysis[a]	o	+	++	++
2	Inductive analysis[b]	++	++	++	++
NOTE: The level of detail of the analysis is commensurate with the level of detail of the design. Both methods can, in certain cases, be carried out at different levels of detail.					
[a] A typical deductive analysis method is FTA. [b] A typical inductive analysis method is FMEA.					

Figure 3.5: Hardware design safety analysis (ISO26262-5 2011)

The table shown in Figure 3.5 suggests using deductive and inductive analysis techniques to identify the *causes* and *effects* of faults and failures respectively. Having studied the STPA methodology, we know that STPA has an elaborate, well-structured process to determine the causes of the unsafe control actions

using the causal factor analysis of STPA Step 2. The effects corresponding to *hazard* and *accident* identification of STPA Step 0, can also be determined by following the STPA process. Thus, the safety analysis requirement 7.4.3.1 of Part 5 of the standard can be supported by STPA. ISO 26262-9:2011, Clause 8 referred to in requirement 7.4.3.1 will be discussed later.

Part 9 - 7 - Analysis of dependent failures:

Part 9 of the standard provides guidelines to specify the requirements for ASIL-oriented and safety-oriented analyses; and Clause 7 of Part 9 deals with the analysis of dependent failures.

The precise requirement is:

"*7.4.1 The potential for dependent failures shall be identified from the results of safety analyses in accordance with Clause 8.*

NOTE 1 Both systematic failures and random hardware failures have the potential to be dependent failures.

NOTE 2 The identification of potential for dependent failures can be based on deductive analyses: examination of cut sets or repeated identical events of an FTA can indicate potential for dependent failures.

NOTE 3 The identification can also be supported by inductive analyses: similar parts or components with similar failure modes that appear several times in an FMEA can give additional information about the potential for dependent failures" ISO26262-9 2011.

In both these cases (Note 2 and Note 3), STPA can complement FTA and FMEA if we consider repetition of *hazards* in STPA Step 1 (UCA linking) as an equivalent step i.e., depending on the number of times a *hazard* is linked to an *UCA*, we could identify its potential for dependent failures.

Part 9 - 8 - Safety Analyses:

The objective of safety analyses as prescribed in Part 9, clause 8 of the ISO 26262 standard is to "examine the consequences of faults and failures on the functions, behaviour and design of items and elements. Safety analyses also provide information on conditions and causes that could lead to the violation of a safety goal or safety requirement."

"Additionally, the safety analyses also contribute to the identification of new functional or non-functional hazards not previously identified during the hazard analysis and risk assessment" (ISO26262-9 2011).

These objectives can also be met by following the STPA process. The *accidents* identified in STPA Step 0 help in deriving the consequences of faults and failures. Causal factor analysis i.e., STPA Step 2 helps in generating the causes that could lead to the violation of a *safety goal or safety requirement*. As pointed out in our analysis, STPA Step 1 also helps in identifying the new *hazards* not previously identified in STPA Step 0. Thus, the objectives of safety analyses can be met using STPA.

3.3.3 Summary

STPA focuses on identifying the hazards and ways to mitigate against them and does not involve risk assessment (Leveson 2011). Hommes 2012c mentions the possible subjectivity in estimating the likelihood factors of complex and relatively new systems as part of risk assessment. While we agree that there is a certain level of subjectivity in determining the *probability of exposure and controllability*, evaluating these parameters is necessary for risk-based *ASIL* assessment, if one wishes to follow the ISO 26262 standard. Hence, in this

thesis, we present our approach of how STPA can be augmented so that it can be used in an ISO 26262 compliant process. For STPA to handle ASILs we mainly need to follow the guidelines provided in the ISO 26262 standard and do not really have to modify STPA. Thus, STPA can in fact, support all the outputs of ISO 26262 generated as a result of following its HARA requirements. Even though "as-is" STPA does not use risk assessment in terms of deriving the impact factors and their corresponding ASILs, STPA can definitely be used as a complementary hazard analysis technique to identify the accidents, hazards, to determine their causes and to derive safety constraints to eliminate, mitigate and/or control the unreasonable risks. In the next chapter, we provide an excerpt of an illustrative example to demonstrate how the ISO 26262 guidelines summarized in this chapter can be used in addition to STPA steps, to follow an ISO 26262 compliant process.

Chapter 4

Illustrative Examples Based on an Automotive Subsystem

In this chapter, we provide examples that illustrate how we applied the guidelines presented in Chapter 3 on a simplified version of a realistic automotive subsystem from our industrial partner. The system selected for our example is the Battery Management System (BMS) of a *Plugin Hybrid Electric Vehicle (PHEV)*. Section 4.1 provides a description of the system and its intended functionality. Section 4.2 presents isolated examples of our results of using STPA in an ISO 26262 compliant process, and Section 4.3 documents a few important conclusions drawn from applying STPA with some additions that enables us to perform an ISO 26262 compliant HARA.

Information about the battery management system was mostly gathered and documented by Dr. Morayo Adedjouma, former Postdoctoral Fellow at McMaster University. Dr. Pawel Malysz, former Principal Research Engineer at McMaster University provided valuable domain expertise on the battery management system. Information from Weicker 2014 and documentation and

feedback from our industrial partner were also very helpful.

4.1 BMS of a PHEV

In this section, we provide basic information about the PHEV and the BMS selected for this example application. A PHEV is a hybrid electric vehicle that uses both an electric motor and an *Internal Combustion Engine (ICE)*. A PHEV can use energy storage devices like rechargeable batteries, which can be charged by the power obtained from regenerative braking or by connecting to the electrical grid using a plug. These rechargeable batteries are monitored and protected by the BMS.

The BMS ensures the safety of the battery pack by measuring, controlling and communicating the status of the multiple cells of the battery pack with the relevant systems (Weicker 2014). The BMS monitors the operational parameters of the battery cells like Voltage (V), Temperature (T) and Current (I). It also protects the battery cells in cases such as battery cell abuse or operation outside safe conditions to avoid battery failure. The cells can be protected using processes like charge control, charge equalization in all cells and thermal management. The system reports the battery cell status: the *State of Charge (SOC)*, the *State of Health (SOH)*, and the *State of Power (SOP)* to the *Hybrid Powertrain Controller (HPC)* (Weicker 2014). SOC is the capacity left in the battery, SOH is the measure of the battery capability to deliver its outputs and the SOP is the measure of available battery power (Weicker 2014). The BMS also includes warning mechanisms like alarms and sends fault/error status when the battery parameters exceed the limits. To ensure efficient management of the battery pack, the BMS must also accept and fol-

low control actions from the HPC. The BMS also stores the manufacturer's cell specification, e.g., chemistry, capacity, voltage limits, temperature limits, current limits, etc., for reference and the usage history of the battery cells for maintenance purpose. Thus, the primary functions of the example BMS are to: 1) control the charging (open/close contactors), 2) provide accurate information on charge and discharge to the HPC system, 3) equalize cell charge using passive cell balancing, 4) heat and cool the battery pack, 5) isolate the battery in case of emergency (Adedjouma et al. 2015).

4.2 Results of Applying STPA on the BMS

We performed hazard analysis on the BMS of a PHEV using STPA for our industrial partner and the detailed results were reported in an internal report for our industrial partner (Adedjouma et al. 2015). In this section, we present isolated examples drawn from our results of applying STPA on the BMS, highlighting how STPA can support generating the required outputs of the concept phase of ISO 26262. Not all the details of the analysis and the control structure are shown here due to confidentiality reasons.

We first applied standard STPA on the Battery Management System which resulted in Figure 4.1. As we can see in Figure 4.1, there were some gaps in STPA with respect to its compliance to the ISO 26262 standard; the gaps corresponding to the unmapped blocks of ISO 26262 on the left hand side. We then applied the additional guidelines we presented in Chapter 3, the result of which are the blue blocks presented in Figure 4.2. It is important to note that to use STPA in compliance with ISO 26262, we did not have to modify the original technique, but augment it with additional guidance.

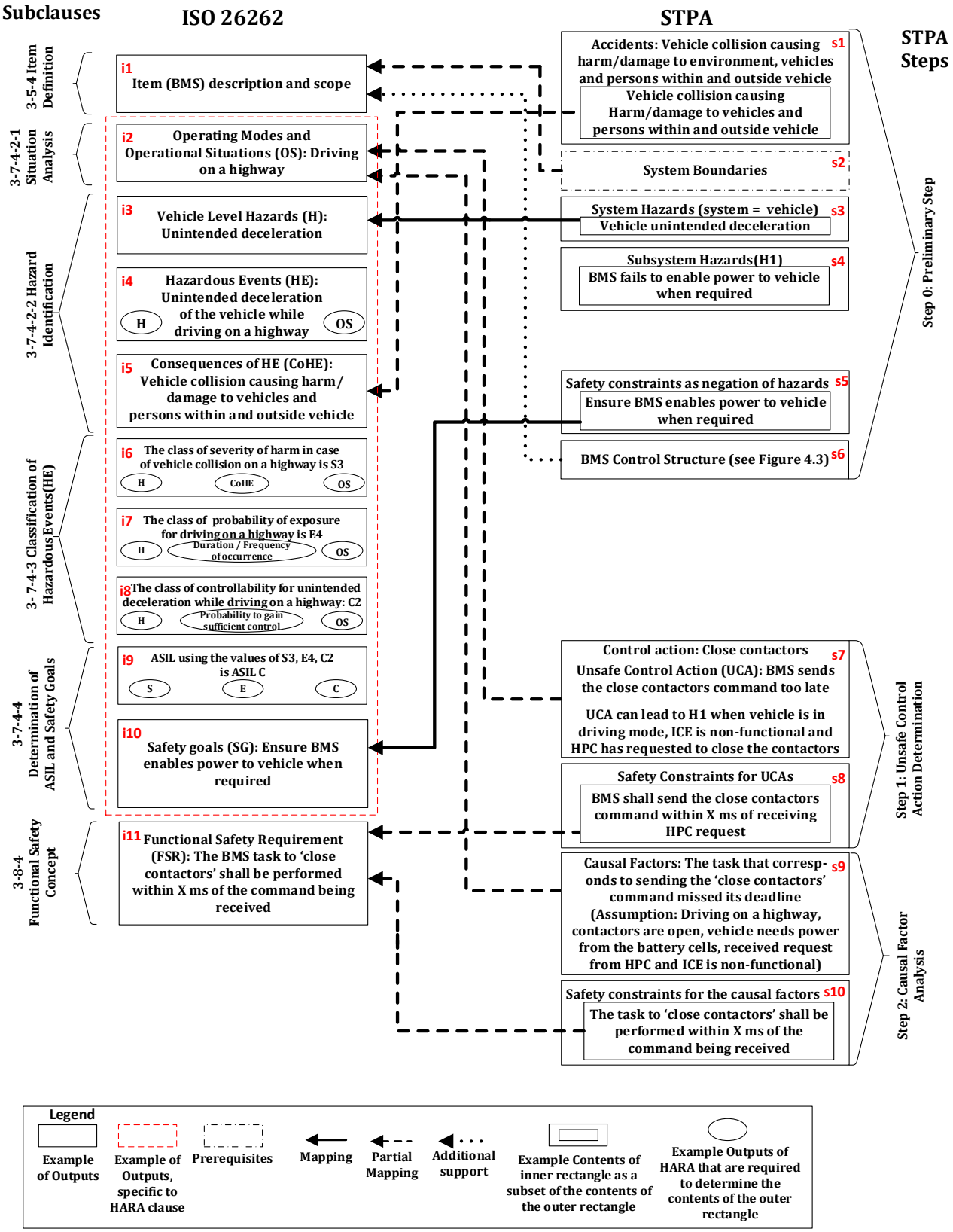

Figure 4.1: Sample of an excerpt of applying HARA and STPA on BMS

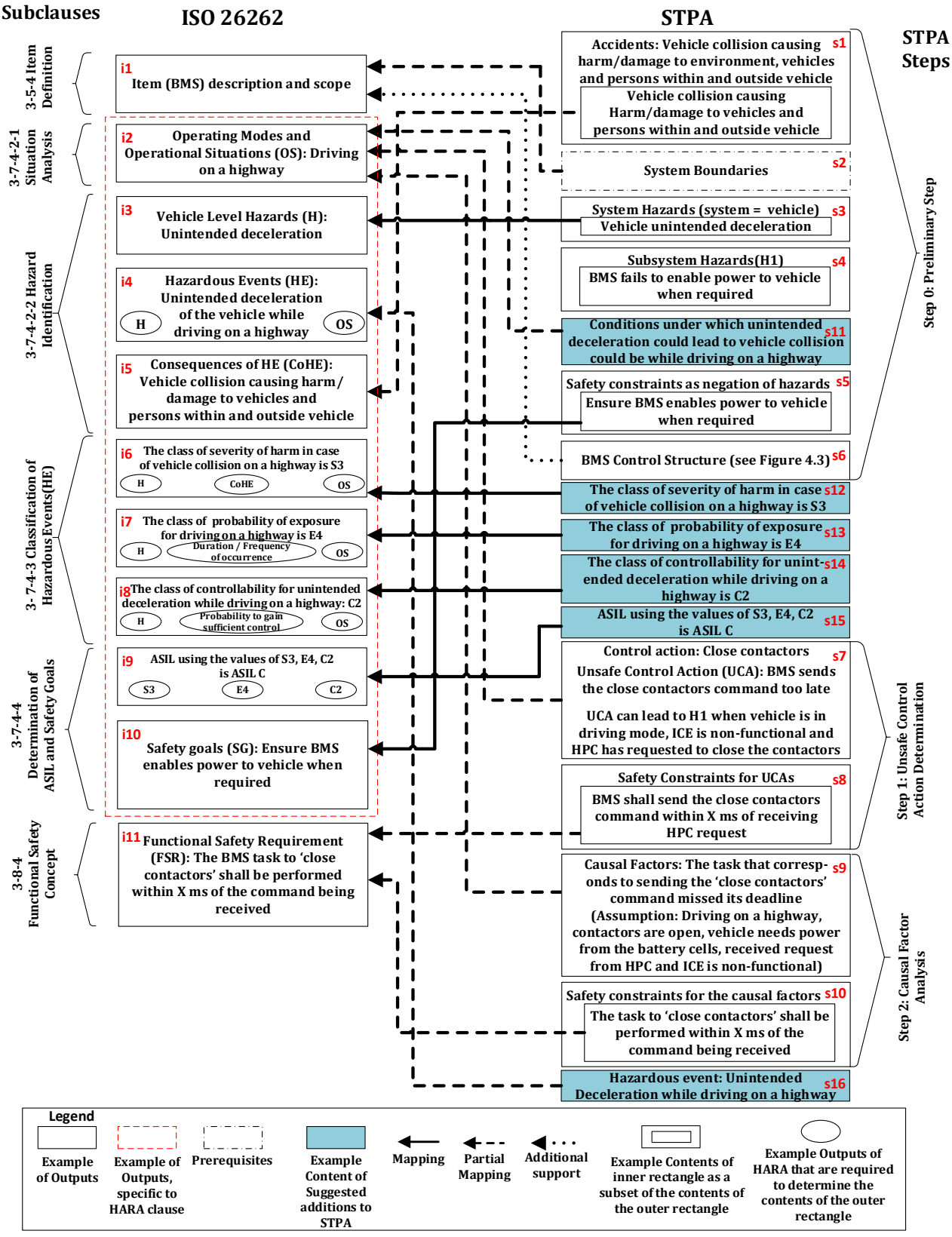

Figure 4.2: Sample of an excerpt of applying HARA and STPA in compliance with ISO 26262 on BMS

In this example, we first discuss the STPA steps in the sequence in which they are generally performed. We then see how the obtained STPA results can help in generating the various results of the concept phase of ISO 26262. Example results of applying STPA in an ISO 26262 compliant process are included in Figure 4.2. Note that Figure 4.2 represents the same mapping as Figure 3.3, with small, illustrative examples embedded. As part of STPA Step 0, we identify the accidents, related hazards, corresponding safety constraints, and define the control structure of the system (BMS). Table 4.1 shows a sample from an excerpt of our STPA Step 0 results. In this example, the assumption is that we have information about the basic components and functions of the BMS.

Table 4.1: Sample of an excerpt of results of STPA Step 0

Accident	System (Vehicle) Hazard	Subsystem (BMS) Hazard	Safety Constraint
Vehicle collision causing harm/damage to vehicles and persons within and outside vehicle (AC1)	Vehicle experiences unintended deceleration (V_H1)	BMS fails to enable power to vehicle when required (H1) (Assumption: Driving on a highway, ICE is non-functional)	Ensure BMS enables power to the vehicle when required (SC1)

The accidents of STPA can partially support the determination of consequences of hazardous events of ISO 26262, and hazards identified in Step 0 can help support the hazard identification subclause of ISO 26262 as shown in Figure 4.2. In this illustrative example, the accident example of STPA exactly matches the example of the consequences of the hazardous event identified in the standard, i.e., when driving on a highway, if there is an unintended decel-

eration, *the vehicle could be involved in a collision causing harm/damage to vehicles and persons within and outside vehicle.*

As mentioned in Section 3.3.1, in STPA, hazards are first identified at the system level. In cases where the system level hazards cannot be eliminated or adequately controlled at the system level, they need to be refined into the subsystem/component level hazards. Thus, an example of the system (vehicle) level hazard for this example is *V_H1: Vehicle experiences unintended deceleration.* A simple negation of the *hazard* would be *Vehicle should avoid unintended deceleration.* But to achieve this, i.e., to avoid the hazard, we would need to look at the components like ICE, gas level, brakes and BMS. For example, *Avoid having the brakes applied inadvertently, Ensure BMS enables power to vehicle when required, etc.* For our example, we will focus on the BMS. Thus, an example of a BMS level hazard identified is *H1: BMS fails to enable power to vehicle when required.* 'When required' covers instances like vehicle is dependent on power from battery to drive the electric motor.

As discussed in Section 3.3.1, we explicitly document the operational situations during the process of linking hazards to accidents. This is shown in block s11. When analyzing in what situations the hazards *V_H1: Vehicle experiences unintended deceleration* and *H1: BMS fails to enable power to vehicle when required* could lead to *AC1: Vehicle collision causing harm/damage to vehicles and persons within and outside vehicle*, we can come up with the following operational situations *OS1: Driving on a highway, OS2: Snow and ice on road, etc.* We also consider the worst-case environmental conditions in our analysis, *e.g., no gasoline, making the ICE non-functional and the vehicle completely dependent on the power from the battery cells.* In this case, the BMS will function as though it were in an *Electric Vehicle (EV).* Combining the hazard

and operational situation, an example of the hazardous event *(HE)*, shown in block s16, is: *Vehicle experiences unintended deceleration while driving on a highway.*

An example of a safety constraint derived as the negation of the hazard *H1* is given by safety constraint *SC1: Ensure BMS enables power to the vehicle when required.* Safety constraints derived as the negation of hazards in this step can be used to support the safety goal determination subclause of ISO 26262, as the safety goals are defined in terms of high-level requirements. It is important to note that once the safety constraints are determined for the relevant step, there are chances of having conflicting safety constraints. Resolving these conflicts is an important part of system design process (Leveson 2011).

The next step of STPA is drawing the control structure. As expected, both STPA and ISO 26262 recommend getting a basic understanding of the system before performing a hazard analysis (Leveson 2011), (ISO26262-3 2011). The control structure of STPA is a graphical representation of the functional model of the system (Leveson 2011). Information needed to draw the control structure requires knowledge of the functionality and purpose of the system, a description of the system's interfaces and identification of its dependencies, i.e., the interactions within the system, the interactions with other elements and the environment. As the control structure of STPA gives a clear picture of the various interactions of the system, it is a very good pictorial representation of the system and provides additional support to the **item definition** work product.

We defined several versions of the BMS control structure with different levels of detail. It is very important to define the important components and interactions of the various systems and subsystems in the control structure as

this is one of the most important preliminary steps of STPA. As mentioned in Leveson 2011, we first start with a high level representation of the system and add more details as we proceed. This helps the analyst deal with the complexity of the system by gradually adding more details. Moreover, as the analyst learns more details or receives more feedback from the domain experts, the control structure is further refined. Figure 4.3 shows the control structure used for the analysis, i.e., a detailed BMS control structure with control flows and feedback arrows labeled. The components and arrows were identified based on the general functionalities of a battery management system elicited through literature review (Weicker 2014) and with the help of domain experts as summarized in Section 4.1. The HPC, the contactors, the battery pack and the 12V battery are the external systems that interact with the BMS. Other systems in the BMS environment are the fan/pump components for the thermal management system, the on-board charger, and the external charger. The components of the BMS are shown inside the blue dotted box in Figure 4.3, namely, the *Battery Control Module (BCM)*, *Battery Monitoring Module (BMM)*, the history log module and the cells specification module. The blue arrows (power flows) represent the power/energy circulating to and from the battery cells. The black arrows (control action flows) are the commands that the BMS sends to the other systems with which it interacts. They are analyzed in STPA Step 1. The red arrows (feedback flows) are the feedback information exchanged between the BMS and its environment. The BMS receives information from each battery cell like voltage, temperature and current. The BMS provides the battery information like SOC, SOP, SOH and battery fault status to its environment. The feedback flows are analyzed during STPA Step 2. Since the control structure gives a very good representation of the

system and gives a clear picture of the various interactions of the system, it adds a lot of value to the **item definition** work product of the concept phase of ISO 26262. This covers all the results of Step 0 of STPA.

The *Control Action (CA)* selected for Step 1 of this example application is *CA1: close contactors*. *CA1* is the BMS command to the contactors to close, which would enable power flow. This command is sent after the BMS receives the authorization from the HPC or a close request from the HPC. When the contactors are closed: 1) in charging mode while the vehicle is plugged in, the battery cells will receive power from the electric grid; the HPC will receive power from the battery cells; 2) in driving mode, the battery cells can receive power HPC from regenerative braking and the HPC can receive power from the battery cells.

In STPA Step 1, we categorize the control actions into 4 categories of inadequate controls. Let us consider the control action *CA1: close contactors* under the category 'Safe control action provided too late, too early, wrong order'. An example of unsafe control action would be *UCA1: BMS sends the close contactors command too late*. When analyzing the ways in which a control action can be unsafe and linking them to the hazards, the analyst has to identify the context (operational situations) which makes the control action hazardous. In this case, the *UCA1* can lead to the *V_H1: Vehicle experiences unintended deceleration*, when the vehicle is in an operational situation like *driving mode, ICE is non-functional making the vehicle completely dependent on the battery cells for power*. The assumption here is the HPC has already requested the BMS to close the contactors and that the HPC gives the command only when safe to do so. Thus, this part of Step 1 of STPA, i.e., determining the conditions under which the control actions could be hazardous, can par-

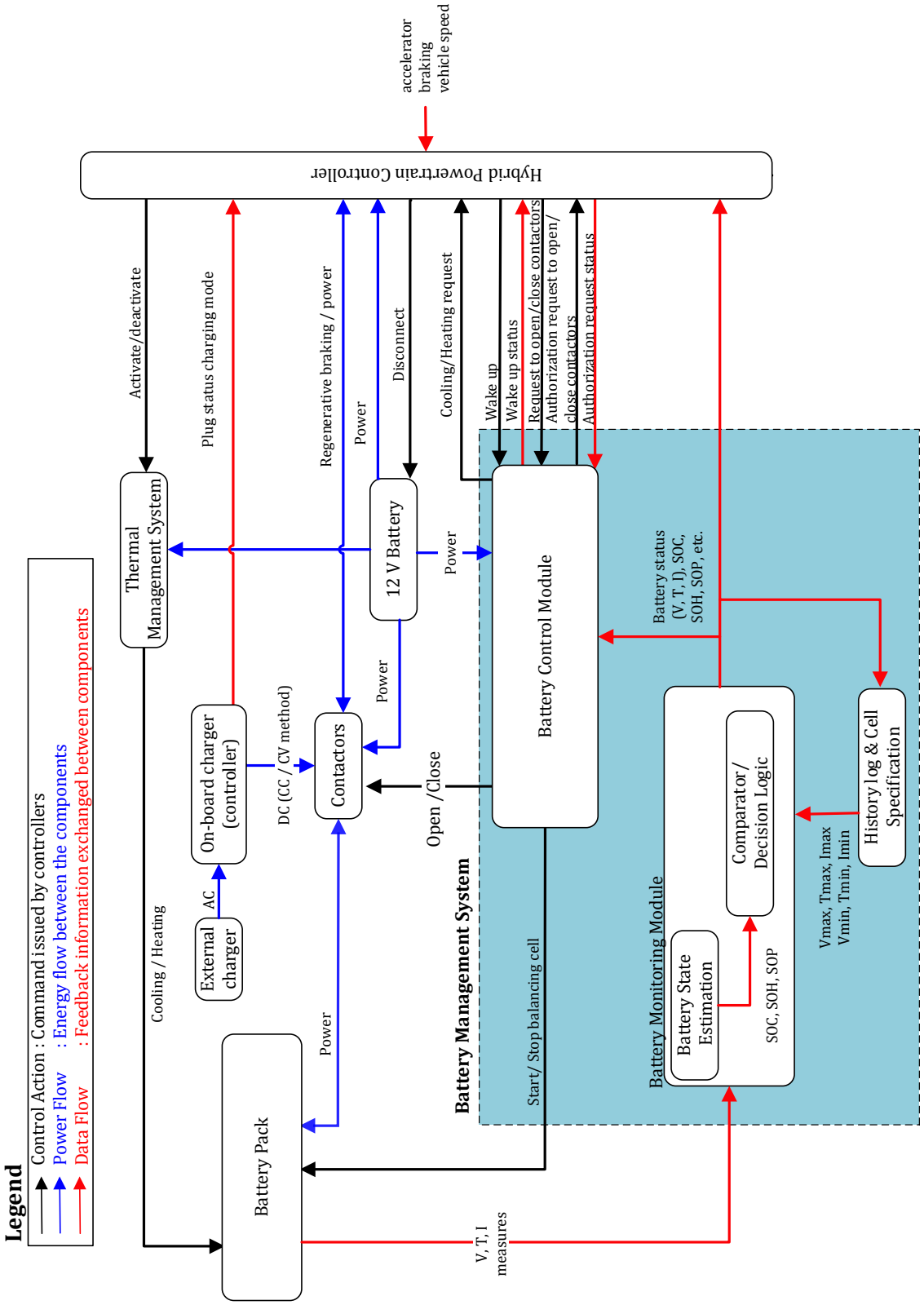

Figure 4.3: BMS control structure (Adedjouma et al. 2015)

Table 4.2: Sample of an excerpt of results of STPA Step 1 for the control action, CA1: close contactors

Control Action	Required control action not provided	Unsafe control action provided	Safe control action provided too late, too early, wrong order	Continuous safe control action provided too long or stopped too soon
Close contactors	...	...	UCA1: BMS sends the close contactors command too late [H1] UCA1 can lead to H1 when ICE is non-functional, HPC request is received and driving on a highway	...

tially support in listing the operational situations. Furthermore, when linking UCAs to hazards of Step 0, one can sometimes identify new hazards that were not previously identified. Hence we can link Step 1 to the hazard identification step of ISO 26262 as well. Step 1 also involves translating the UCAs into safety constraints and further refining the safety constraints from Step 0. An example of safety constraint for *UCA1* is *UCA1_SC1: BMS shall send the close contactors command within X ms of receiving the 'close contactors' request from HPC*. Since this safety constraint of Step 1 describes what needs to be done to achieve the safety goal, it represents a functional safety requirement.

Causal factor analysis (Step 2) involves examining the control loop of the control action and identifying the causes of unsafe controls. The control loop includes the controller that initiates the control action, the actuator, the sensor, and the controlled process, i.e., the element being controlled by the control

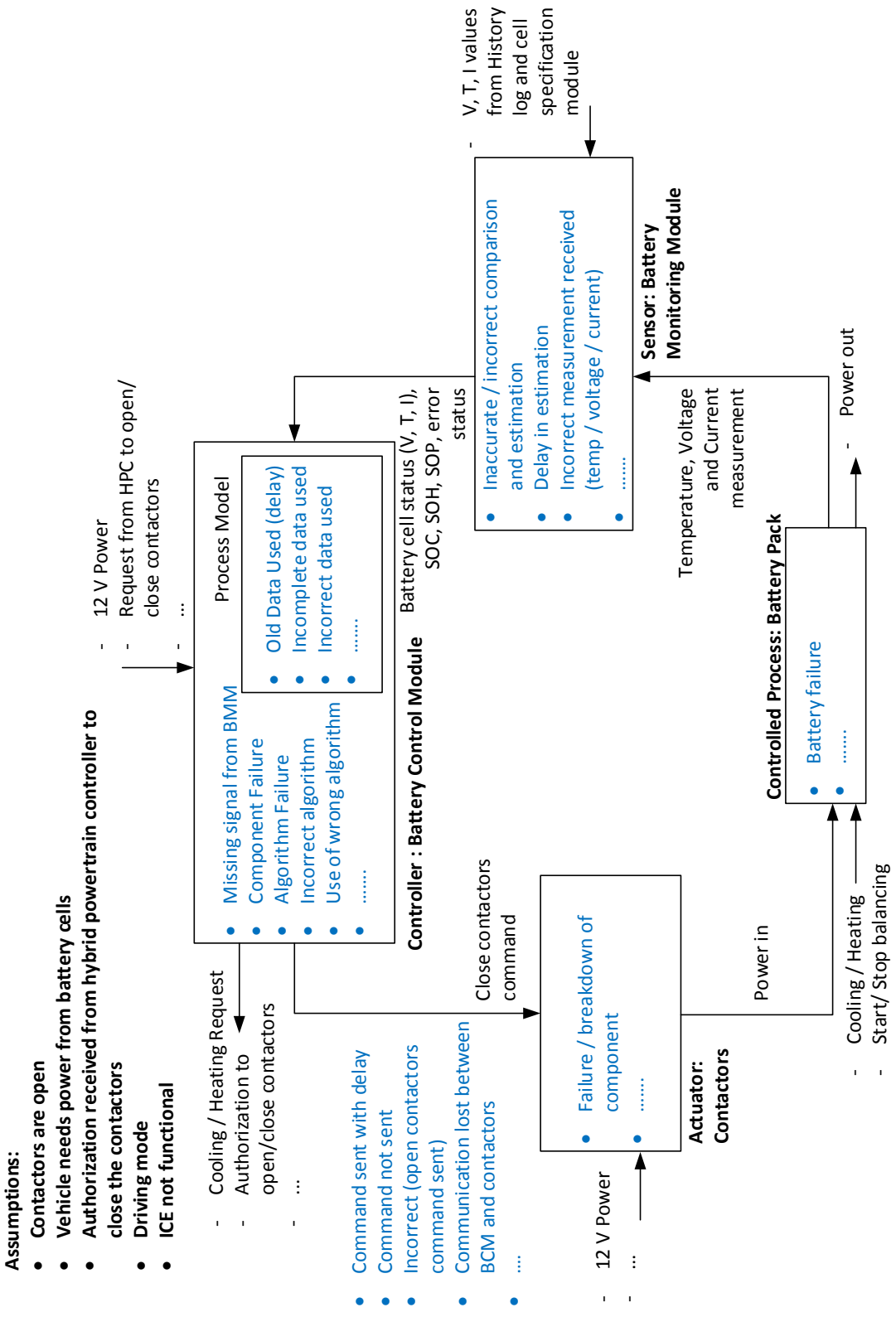

Figure 4.4: Causal factor analysis for control action, CA1: Close Contactors

actions (Leveson 2011). A unique control loop is identified and used for all identified unsafe control actions of the selected control action. Then, a causal factors analysis diagram is defined for the unsafe control actions based on the guide words provided by STPA (Leveson 2011). Part of our causal factor analysis for *UCA1* is shown in Figure 4.4, where the specific causes of the unsafe control actions which may lead to the hazards are shown in blue. For the loop in Figure 4.4, the BCM, as a controller, will issue the control action to *Close Contactors* and will send the control action to the actuators that will realize the command. The controlled process in the loop is the battery cell pack. The BMM is in charge of measuring/collecting the effects of the control action on the battery cells and reporting back to the BCM. During the causal factors analysis we assume that the BMS has already received the 'close contactors' request from the HPC to close the contactors. For the sake of simplicity, in Figure 4.4, we have only shown a few of the causal factors of the contactors, the battery pack, the BMM, the BCM including its process model[1] and the ones between the BCM and the contactors. Other causal factors e.g., authorization request not received from the HPC, 12 V power disconnected etc., are not shown here, but were included as part of the work for our industrial partner. The causal factors identified in STPA Step 2 can help fulfill one of the objectives of the safety analyses as per ISO 26262 (Clause 8 of ISO26262-9 2011), i.e. to identify the "causes that could lead to the violation of a safety goal or safety requirement". Once the causes are identified, the analyst needs to identify the safety constraints to mitigate or eliminate those causes, in a process similar to Step 1. An example of a safety constraint identified in Step 2 for the BMS is shown in Table 4.3. One of the causes which could result

[1]See Section 2.1.1 for more details on process model

in *UCA1* is causal factor *CF1: The task that corresponds to sending the close contactors command missed its deadline (Assumption: Driving on a highway, contactors are open, vehicle needs power from the battery cells, received request from HPC and ICE is non-functional).* An example of a Step 2 safety constraint identified for *CF1* is *SC1_CF1: The task to close contacts shall be performed within X ms of the command being received.* This Step 2 safety constraint could partially support the functional safety requirements of ISO 26262. ISO 26262 specifies the characteristics and parameters that a safety requirement should include, e.g., the fault tolerant time interval if available, the safe state, the operating mode, etc.. However, the level of details needed when defining the safety constraints during STPA is not pre-determined as the constraints could vary between the various industries based on the specific standard and on the phase of the development during which the analysis is performed (e.g., concept vs production).

Table 4.3: Sample of an excerpt of results of STPA Step 2

Causal Factor	Safety Constraint
The task that corresponds to sending the 'close contactors' command missed its deadline (CF1) (Assumption: Driving on a highway, contactors are open, vehicle needs power from the battery cells, received request from HPC and ICE is non-functional)	The task to close contacts shall be performed within X ms of the command being received (SC1_CF1)

We will now discuss the blocks of the concept phase of ISO 26262, which were not part of the original STPA, not even implicitly. *Classification of hazardous events* and *Determination of ASILs* are the main subclauses of the concept phase of ISO 26262 that do not have a corresponding step in STPA.

As pointed out in Chapter 3, these unmapped blocks can be obtained by following the guidelines summarized in Section 3.3.1, while applying the STPA process. The severity of potential harm is estimated based on the Figure 2.10 as mentioned in ISO 26262 (ISO26262-3 2011) and categorizations like the AIS scale. For the selected case, the class of severity of harm in the case of vehicle collision while driving on a highway is *S3* (Life-threatening injuries). Probability of exposure of operational situation is estimated based on Figure 2.11. For the selected example, the class of probability of exposure for driving on a highway is *E4* (Greater than 10 % of average operating time). Controllability of the hazardous events is estimated based on Figure 2.12. For the selected example, the class of controllability for unintended deceleration while driving on a highway is *C2*, i.e. 90 % or more of all drivers or other traffic participants are usually able to avoid harm. These values are just meant as examples as we do not have domain expertise. Ideally, a detailed justification would be included to explain why the team decided on a certain value for the selected impact factor. To be on the safer side, a higher level of impact factors have been chosen. The ASIL for the above chosen impact factors is *ASIL C*, based on Table 2.13. Hence, we can observe that, to use STPA in an ISO 26262 compliant process, there is no need to modify STPA, but just to follow some additional steps.

4.3 Summary

In summary, using the additional guidelines of ISO 26262 presented in Section 3.3.1 along with STPA, we performed a STPA hazard analysis on the BMS in an ISO 26262 compliant manner.

The application of the concept phase requirements of ISO 26262 are mainly based on our understanding of the standard. Ambiguities in the standard, lack of guidance in terms of additional examples and lack of publicly available published sources with complete application of ISO 26262 are some of the key challenges encountered during the course of determining if STPA could be used in an ISO 26262 compliant process. We believe that the explicit comparison of the terms used in ISO 26262 and STPA, along with a complete HARA mapping and isolated examples on an automotive subsystem, should help bridge the gap and help the readers see how STPA can be used in an ISO 26262 compliant process.

Chapter 5

High-Level Mapping Between the Outputs of STPA, FMEA and 7FM

In this chapter, we present the potential mapping between the outputs of STPA and variants of FMEA. Essentially, the mapping shows the connection between the *outputs* that should be obtained as a result of following the processes of STPA and FMEA. Section 5.1 provides the context and motivation of this chapter and in Section 5.2, we present a high-level mapping between the outputs of STPA, FMEA (based on SAE 2009) and 7FM, a variant of FMEA (based on Lindland 2007). In Section 5.3, we discuss the categories of failure modes of FMEA and 7FM; and the categories of Unsafe Control Actions (UCAs) of STPA.

5.1 Context

As mentioned in Chapter 2, STPA follows a top-down approach, whereas FMEA is generally used in a bottom-up manner. However, FMEA can also be used in a top-down manner by analyzing the failure modes from the higher levels (system) to the lower levels (component) (Song 2012) e.g., 7FM is a top-down FMEA technique. Our mapping is between the outputs of STPA and system level functional FMEAs, performed in a top-down manner. For the purpose of this comparison, we refer to the worksheets from SAE FMEA and 7FM. The main difference between these two worksheets is the ordering of the columns even though they are filled in the same order.

As FMEA and its variants have been in use for a very long time (original FMEA document dates from November 1949 (Ericson II 2005)), we believe that the majority of safety analysts familiar with ISO 26262 are familiar with FMEA as well. Given the potential benefits of applying STPA in the automotive domain, we map outputs of STPA to outputs as documented in the worksheet of automotive FMEA, i.e., SAE version of FMEA (SAE 2009). Further, we map STPA to 7FM (Lindland 2007), a variant of FMEA. Thus, our work showing the link between FMEA and STPA should help the wider audience see the connection between functional FMEA techniques and the STPA technique. It is important to note that we are trying to map the outputs of these techniques when performed at the same level.

In this thesis, we mainly focus on a general high level potential mapping between the expected outputs of FMEA and STPA as a result of following their processes, and not on comparing their effectiveness in terms of which one identifies a more comprehensive set of causes. For more details on the

comparison of the types of accident causes identified in FMEA and STPA, along with an analysis of the benefits and challenges of both, the reader is encouraged to refer to Sotomayor 2015 and Song 2012. A short summary is presented in Section 2.3.1.

5.2 Mapping the outputs between STPA, FMEA and 7FM

In this section, we present the mapping between the outputs of STPA, FMEA and 7FM as shown in Figure 5.2. STPA steps, including the sub steps as explained in Section 2.1.1 are summarized in Figure 5.1 for easy reference.

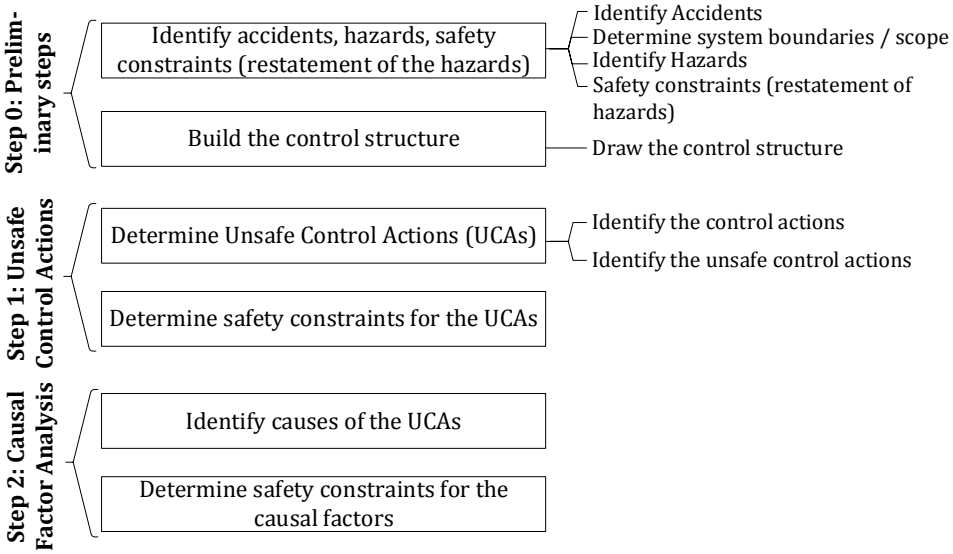

Figure 5.1: Overview of STPA with sub steps

As there is no significant difference between the worksheets of 7FM and FMEA except for the order of the columns in the worksheet (although the

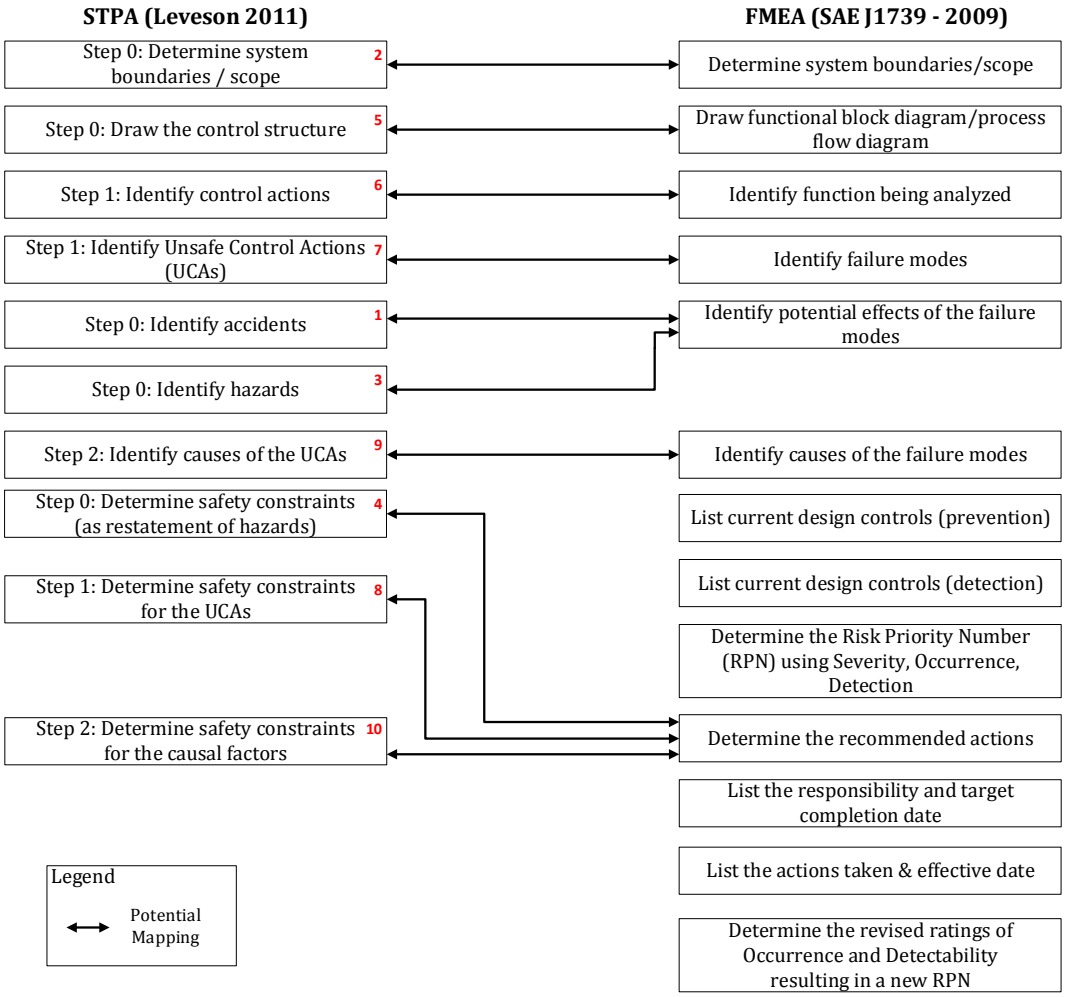

Figure 5.2: Potential mapping between STPA outputs and FMEA/7FM outputs (columns of worksheets)

order of performing the steps is the same), Figure 5.2 represents the mapping between outputs of STPA and both FMEA and 7FM worksheets. In cases where 7FM would be different from FMEA, we explain how 7FM maps to FMEA and STPA.

On the left hand side of Figure 5.2, we present the expected outputs of the STPA process. On the right hand side of the Figure 5.2, we present the expected outputs of the SAE and 7FM version of the FMEA process. We

then present the potential mapping between these expected outputs of STPA and FMEA using bi-directional arrows. The FMEA blocks are presented in the sequence in which they are performed. To increase the readability of the figure by avoiding arrows crossings, the STPA blocks are presented in the order in which they map to the FMEA blocks and not in the order in which they are performed. The numbers written inside the STPA blocks represent the order in the sequence in which they need to be performed. For example, accidents need to be identified (block 1) before identifying the control actions (block 6).

The FMEA technique starts by defining the system scope and its boundaries. Pictorial tools like functional block and boundary diagrams aid in defining and representing the scope of the analysis. STPA's preliminary step also includes defining the system scope and system boundaries, which can be represented using the control structure diagram. These diagrams help the analyst see the big picture and hence aid in the analysis.

FMEA and 7FM techniques involve identifying the *functions* of the system/subsystem/component under study. The *function* of FMEA and 7FM can potentially be mapped to the *control action* of STPA. *Control actions* in STPA are the commands issued by the controller. According to STPA, we do not consider data flow and feedback flow as part of the *control action*. However, in 7FM, the *functions* include the data flow and feedback flow. Thus, there is a partial mapping between the *functions* of 7FM and the *control action* of STPA. It is important to note that, in STPA, the 'data flow and feedback flow' are eventually analyzed in the causal factor analysis when the entire control loop is being analyzed (STPA Step 2).

Identifying the *failure modes* in FMEA and 7FM are mapped to STPA Step 1, i.e. identifying the *unsafe control actions*, because, in both cases we

determine the ways in which the function/control action could be hazardous. Here the difference is in the type and number of categories used to determine the unsafe control actions/failure modes. Mapping *control actions* of STPA to *functions* of 7FM and FMEA would mean mapping the four *unsafe control action* categories of STPA to the seven *failure mode* categories of 7FM and the various categories of FMEA[1] respectively. The categories of STPA and FMEA (both SAE FMEA and 7FM) will be presented in the next section (Section 5.3).

We mapped the *effects* of failure modes of FMEA and 7FM to *hazards* and *accidents* identified as part of Step 0 of STPA. In STPA, we identify the *hazards* and *accidents* before identifying the *control actions* and their respective *UCAs*. However, in FMEA, the *effects* are determined after the *functions* and *failure modes* are identified. The selection of what level of *effects* to consider depends mainly on the goal of performing the FMEA. As per the SAE 2009 manual and 7FM (Lindland 2007), the *effects* of the *failure mode* should be considered as the *effect* of the *failure mode* on the next level up assembly, the final product, and the end customer when known. In the case of 7FM, the seven categories used in *failure mode* determination would be used to document the *effects* as well. This is shown using an example in Figure 5.3. For the sake of simplicity, we use the *function* (*control action* of STPA), 'close contactors' from Chapter 4.

The causal factors analysis is performed in STPA as well as FMEA and 7FM. In 7FM, the same seven categories used in *failure mode* and *effect* identification are used to help document the *causes* of the *failure mode*. As shown

[1] SAE 2009 suggests that "there are at least five different types of potential failure modes discussed during the FMEA process."

7 Failure Modes	Function 1: Close Contactors	Function 2
[O] Omission	What would be the effect on the next higher system if the function, 'Close contactors' is omitted?	What would be the effect on the next higher system if function 2 is omitted?
[+] Excessive	..	..
[-] Incomplete	..	..
[V] Erratic	..	..
[U] Uneven	..	..
[+T] Too Slow	..	..
[-T] Too Fast	..	..

Figure 5.3: Determining the effects in 7FM (Based on Lindland 2007)

in Figure 5.4, we determine what could be the cause for the 'close contactors' function to be omitted. The causal factor analysis step of STPA is well guided. For example, the causal factors analysis step in STPA involves identifying the control loop for each *control action* and using the specific control loop to identify the *causes* for each of the UCAs identified in Step 1. In addition to this, STPA also provides some guide words for the potential causes as shown in Figure 2.2. Thus, when compared to STPA, there is no guidance for causal

7 Failure Modes	Function 1: Close Contactors	Function 2
[O] Omission	What would be the cause for the function, 'Close contactors' to be omitted?	What would be the cause for function 2 to be omitted?
[+] Excessive	..	..
[-] Incomplete	..	..
[V] Erratic	..	..
[U] Uneven	..	..
[+T] Too Slow	..	..
[-T] Too Fast	..	..

Figure 5.4: Determining the causes in 7FM (Based on Lindland 2007)

factor analysis in FMEA and 7FM. Hence, there is partial mapping between the causal factor analysis of STPA (Step 2) and identifying the causes in 7FM and FMEA.

The *safety constraints* determined in Steps 0, 1 and 2 of STPA can potentially be mapped to the *recommended actions* of FMEA as both of them deal with how to prevent and mitigate the effect. *Current design controls (prevention and detection)* of FMEA mainly deals with the current design controls that help in preventing the cause from occurring and detecting the cause and/or failure mode before the item is released to production (SAE 2009).

The remaining unmapped blocks of FMEA are mainly related to risk assessment and classification processes. Since the standard STPA technique does not support risk assessment, there do not exist any STPA steps corresponding to the risk assessment steps of FMEA. However, we can use the guidelines provided in FMEA to obtain the values needed for risk assessment in STPA, though this is not going to be discussed in this thesis. In the next section, we discuss the categories of unsafe control actions and failure modes of STPA and variants of FMEA respectively.

5.3 Discussion: Categories of Unsafe Control Actions and Failure Modes

In this section, we present the various categories of unsafe control actions of STPA and categories of failure modes of SAE FMEA and 7FM. A detailed analysis on how each category maps to another is beyond the scope of this thesis.

Table 5.1 presents the unsafe control action categories of STPA. To give clearer picture, we have split the 3rd category of STPA into 3 sub categories and the 4th category of STPA into 2 sub-categories. Failure mode categories as mentioned in SAE 2009 are presented in Table 5.2. Although SAE 2009 mentions that "there are at least five different types of potential failure mode categories discussed during FMEA process", each category is not explained in detail. Failure mode categories as mentioned in Lindland 2007 are presented in Table 5.3. As discussed in Section 2.1.4, Lindland 2007 provides an explanation for each of the seven categories of the failure modes.

Table 5.1: STPA's unsafe control action categories (Based on Leveson 2011)

UCA 1: Required control action not provided
UCA 2: Unsafe control action provided
UCA 3.1: Safe control action provided too late
UCA 3.2: Safe control action provided too early
UCA 3.3: Safe control action provided in wrong order
UCA 4.1: Continuous safe control action provided too long
UCA 4.2: Continuous safe control action stopped too soon

Table 5.2: Failure mode categories as suggested in SAE 2009

FM1: loss of function (i.e. inoperable, etc.)
FM2: partial function (i.e. performance loss, etc.)
FM3: intermittent function (i.e. operation starts/stops/starts often as a result of moisture, temperature, etc.)
FM4: degradation (i.e. performance loss over time, etc.)
FM5: unintended function (i.e. operation at the wrong time, unintended direction, etc.)

SafetyHAT, a software tool by Becker and Hommes 2014 that facilitates STPA for the transportation systems, presents two categories of UCAs in addition to the four categories of UCAs of STPA. The two additional categories, *Safe control action provided, but the intensity is incorrect (too much or too*

Table 5.3: 7FM's failure mode categories (Based on Lindland 2007)

FM1: Omission
FM2: Excessive
FM3: Incomplete
FM4: Erratic
FM5: Uneven
FM6: Too Slow
FM7: Too Fast

little) and *Safe control action provided but executed incorrectly*, were added based on the developers' experience in applying STPA to transportation systems (Becker and Hommes 2014). Since the number and type of categories can be added or modified by each industry and analyst, we will not go into a detailed comparison of the mapping between the categories of STPA, FMEA and 7FM. However, we will discuss some key points that we observed while examining these categories.

The main differences that we noticed between the categories of STPA, 7FM and FMEA are presented below. 7FM includes failure mode categories based on change in variation, e.g. erratic or uneven, whereas the original version of STPA does not have an explicit category for this. Similarly, failure mode categories of 7FM account for failures due to magnitude, whereas, original STPA's four categories do not explicitly mention the failures due to the incorrect magnitude or intensity. Although, STPA's UCA 2, "Unsafe control action provided" could potentially account for the incorrect magnitude/intensity, having an explicit category would be useful. Practitioners recognized the need for this additional category to original STPA and added "Safe control action provided, but the intensity is incorrect" in Becker and Hommes 2014. Each technique can be modified to include more/fewer categories to reflect practitioners' experience and based on the nature of the analyzed system. The difference in the

categories used in the techniques also reflects the difference in the nature of the system towards which the techniques were geared. FMEA/7FM and STPA were developed with different systems in mind: the categories in STPA seem to be geared more towards modern complex digital systems, while the guide words used in FMEA seem to be aimed more at analog systems. From this point of view, at the very least, STPA is a useful technique to use in addition to the traditional hazard analysis techniques.

Chapter 6

Conclusions and Future Work

This chapter presents our conclusions and future work.

6.1 Conclusions

In this thesis, our aim was to determine if each of the requirements of the Hazard Analysis and Risk assessment (HARA) clause mentioned in Part 3 of the ISO 26262 standard could be satisfied when using STPA as a hazard analysis technique. We reviewed existing work to examine if there were any published studies to determine if STPA could be used in compliance with the standard. To the best of our knowledge, this thesis represents the first detailed account of the topic.

When we started our analysis, one of the main challenges we encountered was the inconsistency of the terminologies used in various hazard analysis techniques and the ISO 26262 standard to specify the same term. Based on our literature review and our discussion with the various ISO 26262 users, ISO 26262 is quite ambiguous and could be interpreted in various ways. Thus, we

first presented a detailed comparison of some of the important terms used in the ISO 26262 standard and the STPA technique in Chapter 3 (Section 3.2).

Once we laid the groundwork and explained the basic concepts, we determined if STPA could satisfy the requirements of the hazard analysis and risk assessment clause of the ISO 26262 standard. Whenever there was an unsatisfactory fulfillment of HARA requirements by STPA, we provided guidelines to help an analyst fill the gaps. Thus, we provided the first augmented version of STPA that complies with the ISO26262-3 2011 HARA clause.

We also provided a sample of a realistic automotive example, the battery management system of a PHEV, to help the reader see the connection between the various artefacts generated as a result of following STPA and ISO 26262's HARA process. We performed STPA hazard analysis on the Battery Management system (BMS) of our industrial partner and then simplified the results to be included in this thesis. Although we have omitted some specific details of the BMS for confidentiality reasons, the isolated examples in this thesis convey our approach. The examples used are not exhaustive and are only intended to illustrate the various concepts discussed in this thesis. Unfortunately, the complete STPA example cannot be presented here due to the aforementioned confidentiality requirements of our industrial partner.

Since FMEA and its variants are some of the most popular traditional hazard analysis techniques being used, another contribution of this thesis was a high level mapping between the outputs of STPA, Seven Failure Modes FMEA and the SAE version of FMEA. We also discussed the various categories of unsafe control actions and failure modes used in these techniques.

In conclusion, we determined that to use STPA in an ISO 26262 compliant process, we had to augment it. The suggested additions to STPA are to cover

the risk assessment part of the HARA clause of ISO 26262. Thus, using the augmented STPA provided in this thesis, an analyst could use STPA in compliance with ISO 26262. Based on our experience and knowledge, the topics discussed in this thesis have already gained significant interest from academia and the automotive industry (NHTSA 2014), (Hommes 2015), (Hommes 2012c). Thus, this thesis should help a wider audience see the connections between the various techniques and to envisage how STPA can be used in an ISO 26262 compliant process.

6.2 Future Work

In this section, we identify some areas for future work that can be used to further extend our work.

As the technology advances, there is a need to upgrade the existing techniques. Thus, extended versions of STPA are being developed. As part of future work, these extended versions can also be checked against the relevant standards to determine their compliance. However, our work provides a good basis for such future comparison.

Since one of the main strengths of STPA is its ability to effectively portray the role of humans and their interactions with the system as claimed in literature review, we need to apply our approach to an automotive subsystem where complex human interaction is involved.

Having access to a complete example of application of HARA as per ISO 26262 could help determine if STPA identifies hazards that are not identified or not considered as hazards in ISO 26262 and vice versa. It would also help in determining the type of safety constraints and/or requirements identified

by both. This comparison could also be used to evaluate and further refine our augmented version of STPA.

Bibliography

Abdulkhaleq, Asim and Wagner, Stefan (2015). "A Controlled Experiment for the Empirical Evaluation of Safety Analysis Techniques for Safety-critical Software". In: *Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering*. EASE '15. Nanjing, China: ACM, 16:1–16:10 (cit. on p. 37).

Adedjouma, Morayo; Lawford, Mark; Mallya, Archana; Pantelic, Vera, and Wassyng, Alan (2015). *STAMP-based Hazard Analysis of Battery Management System (BMS)*. Internal report (cit. on pp. 74, 82).

An STPA Primer, V.1 (2013). MIT Press. USA (cit. on pp. 12, 57, 63).

Antoine, Blandine (2013). *Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems : an example from the medical device industry*. PhD thesis. MIT, USA (cit. on pp. 4, 13).

Becker, Christopher and Hommes, Qi V. E. (2014). *Transportation Systems Safety Hazard Analysis Tool (SafetyHAT) User Guide (Version 1.0)*. http://ntl.bts.gov/lib/51000/51500/51522/SafetyHAT_User_Guide_v1.pdf. [Online; accessed 08-September-2015] (cit. on pp. 97, 98).

Board, JPL Special Review (2000). *Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions*. NASA Jet Propulsion Laboratory (cit. on p. 3).

Born, Marc; Favaro, John, and Kath, Olaf (2010). "Application of ISO DIS 26262 in Practice". In: *Proceedings of the 1st Workshop on Critical Automotive Applications: Robustness & Safety*. CARS '10. Valencia, Spain: ACM, pp. 3–6 (cit. on p. 2).

Breimer, Benjamin (2013). "Design of an Adaptive Cruise Control Model for Hybrid Systems Fault Diagnosis". M.A.Sc. Hamilton, ON, Canada: Dept. of Computing & Soft., McMaster U., Canada (cit. on pp. 4, 13, 37).

D'Ambrosio, Joe; Debouk, Rami; Hartfelder, Dave; Sundaram, Padma; Vernacchia, Mark; Wagner, Sigrid; Thomas, John, and Placke, Seth (2014). *Application of STPA to an automotive shift-by-wire system*. http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/GM-MIT-Research-STPA-Study-Presentation-for-MIT-Workshop-Final-For-Publication.pdf. Presentation. USA: STAMP/STPA workshop, MIT (cit. on pp. 4, 38).

Dardar, Raghad (2013). "Building a Safety Case in Compliance with ISO 26262 for Fuel Level Estimation and Display system". Masters Thesis. Västerås, Sweden: School of Innovation, Design and Engineering, Mälardalen University (cit. on pp. 53, 55).

Ericson II, Clifton A. (2005). *Hazard Analysis Techniques for System Safety*. A John Wiley & Sons, Inc., Publications. USA (cit. on pp. 5, 9, 14–16, 19, 26–28, 55, 58, 90).

Goerges, Stephanie (2013). *The Application of STPA in Commercial Product Development to Identify Causal Factors for Quality Losses*. http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/04_Goerges_STAMP_Workshop-2013_Presentation_FINAL.pdf. Presentation. USA: STAMP/STPA workshop, MIT (cit. on p. 37).

Hommes, Qi D. V. E. (2012a). "Applying System Theoretical Hazard Analysis Method to Complex Automotive Cyber Physical Systems". In: *ASME 2012 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*. American Society of Mechanical Engineers. Illinois, USA, pp. 705–717 (cit. on p. 65).

Hommes, Qi V. E. (2012b). *Applying STPA to Automotive Adaptive Cruise Control System*. STAMP Workshop. Presentation. MIT, USA (cit. on pp. 6, 38, 46).

Hommes, Qi V. E. (2012c). "Review and Assessment of the ISO 26262 Draft Road Vehicle - Functional Safety". In: *Technical Paper, SAE International* (cit. on pp. 46, 62, 70, 102).

Hommes, Qi V. E. (2015). *Safety Analysis Approaches For Automotive Electronic Control Systems*. URL: http://www.nhtsa.gov/DOT/NHTSA/NVS/Public%20Meetings/SAE/2015/2015SAE-Hommes-SafetyAnalysisApproaches.pdf (cit. on pp. 4, 6, 39, 40, 59, 102).

IEC (2010). *IEC 61508 - Functional Safety of E/E/Programmable Electronic Safety-related Systems*. International Electrotechnical Commission (cit. on p. 28).

Ishimatsu, Takuto; Leveson, Nancy G.; Thomas, John; Fleming, Cody H.; Katahira, Masafumi; Miyamoto, Yuko; Ujiie, Ryo; Nakao, Haruka, and Hoshino, Nobuyuki (2014). "Hazard Analysis of Complex Spacecraft using Systems-Theoretic Process Analysis". In: *Journ. of Spacecraft and Rockets* 51, pp. 509–522 (cit. on pp. 4, 36).

ISO26262 (2011). *Road vehicles - Functional safety* -. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on pp. 2, 28, 50, 57, 62, 66).

ISO26262-1 (2011). *Road vehicles - Functional safety - Part1: Vocabulary*. ISO 26262-1:2011. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on pp. 29–31, 47–50, 62).

ISO26262-10 (2012). *Road vehicles - Functional safety - Part10: Guideline on ISO 26262*. ISO 26262-10:2012. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on pp. 28, 49).

ISO26262-3 (2011). *Road vehicles - Functional safety - Part3: Concept phase*. ISO 26262-3:2011. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on pp. 5, 30–34, 43–45, 50, 53, 58–61, 63, 64, 66, 79, 87, 101).

ISO26262-4 (2011). *Road vehicles - Functional safety - Part4: Product development at the system level*. ISO 26262-4:2011. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on p. 67).

ISO26262-5 (2011). *Road vehicles - Functional safety - Part5: Product development at the hardware level*. ISO 26262-5:2011. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on p. 68).

ISO26262-9 (2011). *Road vehicles - Functional safety - Part9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*. ISO 26262-9:2011. Geneva, Switzerland: International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (cit. on pp. 66, 69, 70, 85).

Ladkin, Peter B. (2005). *The Concepts of IEC 61508 - An Overview and Analysis*. http://www.rvs.uni-bielefeld.de/Bieleschweig/fifth/download/B5-Ladkin.pdf. Presentation (cit. on pp. 47, 48).

Leveson, Nancy; Wilkinson, Chris; Fleming, Cody; Thomas, John, and Tracy, Ian (2014). *A Comparison of STPA and the ARP 4761 Safety Assessment Process*. MIT PSAS Technical Report (cit. on pp. 40, 50, 59).

Leveson, Nancy G. (2011). *Engineering a Safer World, Systems Thinking Applied to Safety*. MIT Press. USA (cit. on pp. 1, 3, 4, 8–13, 43–48, 50, 59, 61, 70, 79, 80, 85, 97).

Lindland, John L. (2007). *The Seven Failure Modes - Failure Modes and Effects Analysis*. The Bella Group, Inc. USA (cit. on pp. 5, 7, 20–24, 58, 89, 90, 94, 95, 97, 98).

NHTSA (2014). *Request for Comment on Automotive Electronic Control Systems Safety and Security*. https://federalregister.gov/a/2014-23805. A Notice by the National Highway Traffic Safety Administration. Department of Transportation, National Highway Traffic Safety Administration (cit. on pp. 4, 6, 102).

SAE (2009). *SAE J1739. Surface Vehicle Standard - (R) Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA)*. SAE J1739. SAE International) (cit. on pp. 5, 15–20, 26, 58, 89, 90, 94, 96, 97).

SAE (2015). *SAE J2980. Considerations for ISO 26262 ASIL Hazard Classification*. SAE J2980. SAE International (cit. on p. 62).

Song, Yao (2012). *Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis*. M.A.Sc. Hamilton, ON, Canada (cit. on pp. 4, 9, 13, 16, 36, 37, 90, 91).

Sotomayor, Rodrigo (2015). *A comparison of STPA and automotive FMECA*. http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Sotomayor-Comparing-STPA-and-FMEA.pdf. Presentation. USA: STAMP/STPA workshop, MIT (cit. on pp. 37, 91).

Stringfellow, Margaret V.; Leveson, Nancy G., and Owens, Brandon D. (2010). "Safety-driven design for software-intensive aerospace and automotive systems". In: *Proceedings of the IEEE* 98, pp. 515–525 (cit. on pp. 4, 13, 36).

Sundaram, Padma and Hartfelder, Dave (2013). *Compatibility of STPA with GM System Safety Engineering Process*. http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/04_Sundaram_GM_STPA_Study_Presentation_MIT.pdf. Presentation. USA: STAMP/STPA workshop, MIT (cit. on pp. 4, 38).

Vesely, William; Stamatelatos, Michael; Dugan, Joanne; Fragola, Joseph; Minarick, Joseph, and Railsback, Jan (2002). *Fault Tree Handbook with Aerospace Applications*. Handbook. Washington, DC: National Aeronautics and Space Administration (cit. on pp. 14, 15).

Weicker, Phillip (2014). *A systems approach to Lithium-Ion Battery Management*. Artech House (cit. on pp. 72, 73, 80).