Institute of Software Technology

University of Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Bachelorarbeit

Application of STPA methodology to an automotive system in compliance with ISO 26262

Sara Abidi Nasri

Course of Study: Softwaretechnik

Examiner: Prof. Dr. Stefan Wagner

Supervisor: Dr. rer. nat Asim Abdulkhaleq

Commenced: December 7, 2017

Completed: June 7, 2018

CR-Classification: I.7.2

Abstract

In the automotive domain, functional safety is one of the most important aspects that need to be considered while developing a safety-critical system. Functional safety in road vehicles was standardized in 2011 when ISO 26262 was published. The standard gained a lot of interest and many companies now are using it including Daimler AG.

Hazard analysis and risk assessment (HARA) is described in part 3 of ISO 26262 and analyses the hazards and evaluate the risk. Despite the standard being used for so many years, this method has some limitation especially when applied to a complex system. For example hazards related to human behaviour are not taken into consideration, while the human is part of the system.

System-Theoretic Process Analysis (STPA) a modern method to hazard analysis developed by Nancy leveson at MIT and published in 2012. In STPA more causes of accidents, like human error, are taken into consideration.

The purpose of this thesis in broadening the scope of ISO 26262 by integrating STPA in part 3 of ISO 26262 that contains the hazard analysis and risk assessment methodology. This integration is described in a process diagram and guidelines were presented to help conduct the safety analysis using the new method. Later, it was applied to a Daimler's automotive system that is the cruise control.

The results from previous analysis of the same system were compared with the result of the new method and 2 experts at Daimler AG evaluated the analysis and its results.

In conclusion, it was proven that STPA can be integrated in an ISO 26262 compliant process and that this integration can help increase the safety scope of the standard since more causes of accidents were found. The new method was proven to be feasible, beneficial and easy to learn. This thesis can be the starting point for many future works where the new method is further improved and applied to other automotive systems.

Zusammenfassung

Im automotiven Bereich, ist funktionale Sicherheit einer der wichtigsten Aspekte, die bei der Entwicklung eines sicherheitskritischen Systems berücksichtigt werden muss. Die funktionale Sicherheit in Straßenfahrzeugen wurde 2011 mit der Veröffentlichung der ISO 26262 standardisiert. Der Standard erregte großes Interesse und viele Firmen nutzen ihn, einschließlich Daimler AG.

Gefahren und Risikoanalyse (GuR) wird in Teil 3 von ISO 26262 beschrieben und, wie der Name schon sagt, wird zur Analyse der Gefahren und zur Bewertung des Risikos verwendet. Obwohl ISO 26262 seit vielen Jahren verwendet wird, hat er einige Einschränkungen, insbesondere wenn sie auf ein komplexes System angewendet wird. Zum Beispiel werden Gefahren im Zusammenhang mit menschlichem Verhalten nicht berücksichtigt, während der Mensch Teil des Systems ist.

System-Theoretic Process Analysis (STPA) ist eine moderne Methode zur Gefahrenanalyse, die von Nancy Leveson am MIT entwickelt und 2012 veröffentlicht wurde. In STPA werden mehr Unfallursachen wie menschliche Fehler berücksichtigt.

Ziel dieser Arbeit ist es, den Anwendungsbereich von ISO 26262 durch die Integration von STPA in Teil 3 (der die Gefahrenanalyse und Risikobewertungsmethodik enthält) von ISO 26262 zu erweitern. Diese Integration wird in einem Prozessmodell beschrieben und es wurden Richtlinien vorgestellt, um die Sicherheitsanalyse mit der neuen Methode zu unterstützen. Später, wurde sie auf ein Automobilsystem von Daimler (der Tempomat) angewendet.

Die Ergebnisse früherer Analysen des gleichen Systems wurden mit den Ergebnissen der neuen Methode verglichen und 2 Experten der Daimler AG haben die Analyse und ihre Ergebnisse bewertet.

Zusammenfassend wurde nachgewiesen, dass STPA in einem ISO 26262-konformen Prozess integriert werden kann und dass diese Integration dazu beitragen kann, den Sicherheitsumfang der ISO 26262 zu erweitern, da mehr Unfallursachen gefunden wurden. Die neue Methode erwies sich als machbar, vorteilhaft und leicht zu erlernen. Diese These kann der Ausgangspunkt für viele zukünftige Arbeiten sein, in denen die neue Methode weiter verbessert und auf andere Automobilsysteme angewendet wird.

Contents

List of Figures

List of Tables

List of Abbreviations

AC Accident. 21

AIS Abbreviated Injury Scale. 32

ASIL Automotive Safety Integrity Level. 29

C Controllability. 32

CA Control Action. 22

CS Causal Scenario. 27

E Probability of Exposure. 32

E/E Electrical and/or Electronic. 28

FMEA Failure Mode and Effects Analysis. 15

FMECA Failure Modes, Effects and Criticality Analysis. 15

FSC Functional Safety Concept. 35

FSR Functional Safety Requirement. 35

FTA Fault Tree Analysis. 15

GuR Gefahren und Risikoanalyse. 5

HA Hazard. 21

HARA Hazard Analysis and Risk Assessment. 16

HAZOP Hazard and Operability Study. 44

JAXA Japan Aerospace Exploration Agency. 44

MIT Massachusetts Institute of Technology. 19

QM Quality Management. 29

S Severity. 32

SC Safety constraint. 21

SG Safety Goal. 34

STAMP System-Theoretic Accident Model and Processes. 19

STPA System-Theoretic Process Analysis. 15

UCA Unsafe Control Action. 21

1 Introduction

Safety Has always had a paramount importance especially nowadays with the increasing complexity of systems. More hardware and software components are being built inside the systems which increases the possibility of failure that might lead to a hazard resulting in an accident. This leads to the need of controlling the system which means being able to avoid a specific harm or damage [sta11].

Functional safety is, according to ISO 26262, the abscence of unreasonable risk originating from malfunctioning electrical/electronic systems [sta11]. Unreasonable risk is an unacceptable risk in a certain context [sta11]. Functional safety should not be confused with reliability, that is "probability of correct service for a given duration of time" [Hoo17]. Functional safety should not also be confused with availability, which is "probability of readiness for correct service" [Hoo17]. It should especially not be confused with security that depicts the "absence of unauthorized access to a system" [Hoo17].

1.1 Motivation

As mentioned before, systems are getting more complex, which makes a safety analysis after the system has been developed too expensive and time-consuming. In search of cost-effectiveness and practicality, safety driven designs are required [ILT+10]. It means that the system is investigated and safety requirements are being specified and delivered to the designers during development to help develop a safe system.

Some established techniques for hazard analysis do exist, like Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA) or Failure Modes, Effects and Criticality Analysis (FMECA) [AWL15]. But they only work on an existing design which doesn't comply with the need of safety driven designs. For this purpose, many safety methods were introduced like the Hazard analysis and risk assessment used in the ISO 26262 standard for functional safety in road vehicles [sta11]. In the past few years, a new method emerged: System-Theoretic Process Analysis (STPA) that suggests a new approach for analysing hazards [Lev12].

Due to the fast technological growth, new safety challenges have been imposed and industries need to update their methods to meet the new requirements. For this purpose, new robust techniques are needed and STPA represents one of them. It was applied in many domains such as the aerospace [ILT+10] domain, and is proven to be successful.

As a result, STPA has gained a lot of interest and has been subject of many researches especially that, unlike other hazard analysis techniques, can be used during the development process and it helps identifying the scenarios, in which the hazards might occur. These properties of STPA make it a good candidate to be applied in the automotive domain in accordance with Daimler's already established methodology that is based on part 3 of ISO 26262.

1.2 Problem Statement

As mentioned before, STPA has been applied in many domains, but its usage in the automotive domain is reduced due to the lack of details and guidelines in the method's description. Therefore an integration of STPA in ISO 26262 is needed to create a new method and guidelines on the usage of this new method need to be provided. On the other side the established standard of functional safety, that is the ISO 26262 has some limitation and doesn't comply with the rising complexity of the systems so broadening the scope of ISO 26262 is needed.

1.3 Research objectives

The objective of this thesis is to investigate the application of STPA in the automotive domain and to evaluate this application. That means to analyse the benefits as well as the potential problems and limitations. For this purpose an understanding of the both methodologies (STPA and HARA in accordance with ISO 26262) is needed as well as a comparison between them. This helps establishing STPA in Daimler's Hazard Analysis and Risk Assessment (HARA) to broaden the safety scope of ISO 26262. The result of integration is then to be evaluated after being applied to an example of an automotive system.

1.4 Important terminologies

This section defines the important terms that will be used in chapter 2.

Accident: "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" [Lev12].
Hazard:

- According to STPA: "A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss)" [Lev12].
- According to ISO 26262 "Potential source of harm caused by malfunctioning behaviour of the item"[sta11].

Harm: "Physical injury or damage to the health of persons"[sta11].
Item: "System or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied" [sta11].
Malfunctioning behaviour: "Failure or unintended bahaviour of an item with respect to its design intent" [sta11].
Failure: "Termination of the ability of an element to perform a function as required" [sta11].
Hazardous event: "Combination of hazards and an operational situation" [sta11].
Operational situation: "Scenario that can occur during a vehicle's life" [sta11].

1.5 Structure of the thesis

This thesis contains 7 chapters overall. Chapter 1 is the introduction. Chapter 2 is the background. It contains a full description of STPA and its steps. The train door example was used to explain how STPA can be used. Also a description of part 3 of ISO 26262 was presented and the window door regulator was used as an example to explain the steps of part 3 of ISO 26262. At the end of the chapter STPA and part 3 of ISO 26262 were compared and the advantages and disadvantages of each methodology were listed.

Chapter 3 contains the related work done so far concerning STPA, ISO 26262 and the use of STPA in automotive domain. Chapter 4 contains the description of process diagram that illustrates the steps of the suggested hazard analysis method based on the integration of STPA in the process of part 3 of ISO 26262. The chapter also contains an example of the application of the new method to the cruise control system as well as the results of the analysis and a comparison with the old results from the previous Daimler's analysis.

Chapter 5 contains the evaluation. It was based on a questionnaire that was answered by 2 Daimler experts. It evaluates the learnability, usability and effectiveness of the new method as well as its advantages and disandvantages according to the experts. The results of this evaluation is presented in chapter 6. The summary and the future work are in chapter 7.

2 Background

This chapter deals with the foundations of both STPA and ISO 26262 along with examples. At the end of the chapter a comparison between both methodologies is provided as well as the advantages and disadvantages of each one.

2.1 System-Theoretic Process Analysis

STPA is a hazard analysis technique invented by Nancy Leveson at Massachusetts Institute of Technology (MIT) in the year 2012 [Lev12]. It is based on the System-Theoretic Accident Model and Processes (STAMP) model, which is based on system theory to help identify the origins and the causes of an accident [Tho13][KRR+16]. System theory is based on 4 concepts. The first one is emergence, that is considering safety as an "emergent property that arises when system components interact with each other within a larger environment"[Lev12]. The second concept is hierarchy, which breaks the system down into organized levels with a certain hierarchy [AwL+17]. Communication between components is the third concept and the last concept is control, that is controlling communication within the system [MPA+16]. The idea behind system theory is that a system is safe not only if each component is safe but also the interaction between components is safe. System theory does not treat the system as a set of separate components but rather as a set of interacting control loops. Thus, an accident involves a complex dynamic process [Abd17b].

Most of the other hazard analysis techniques are based on the reliability theory, that means the origin of the accident is the component failure [Abd17a]. This is a static approach that might work for simple systems, but for highly complex systems, these methods will not cover all possible causes and origins of an accident and the safety analysis results will not be sufficient. That's why accidents need to be treated as a dynamic process and that an accident is a consequence of lack of control on the interaction between components. To prevent accidents, STAMP suggests formulating constraints that define the component's behaviour and interactions.

The STPA approach for hazard analysis allows identifying more causes of accidents in addition to the causes covered by all hazard analysis techniques, which are component failures. Among the accident causes identified by STPA are unsafe interactions between the system's components, design error, human mistakes and malfunctioning software.

As mentioned before, STPA is based on the STAMP model. It can identify unexpected accident scenarios with a little knowledge about the system, that's why STPA can be used at an early development stage of a system. Using STPA at the first stages of the design gives

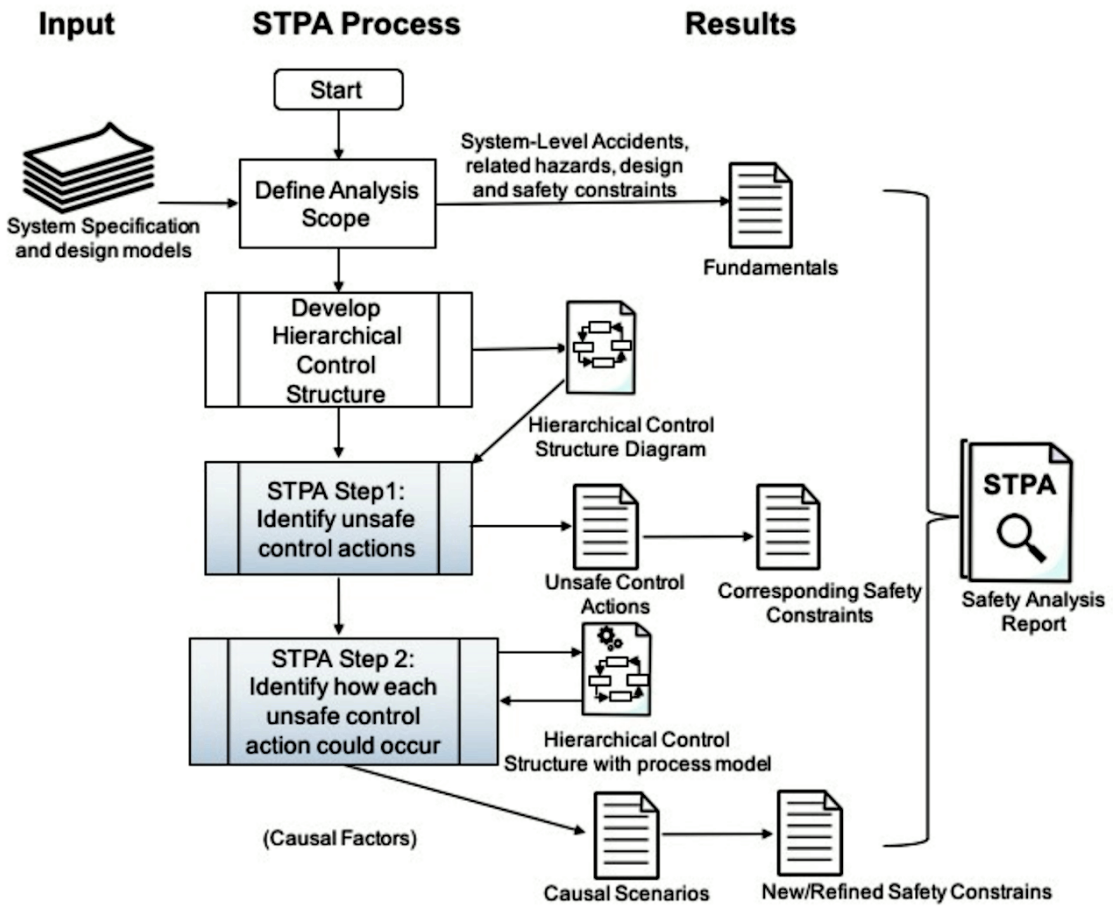

Figure 2.1: Overview of STPA [Abd17a]

guidelines to the developers to design a safe system. Once the design is there, STPA can still be used to improve it. This creates a loop between STPA and design, which in turn creates and refines constraints to avoid the inadequate controls that could lead to hazards.

2.1.1 Steps of STPA

The process of STPA includes 2 main steps: step 1 and step 2 plus a preparation step, that is step 0. Each step will be described and explained in the following sections. An overview of STPA steps is in figure 2.1.

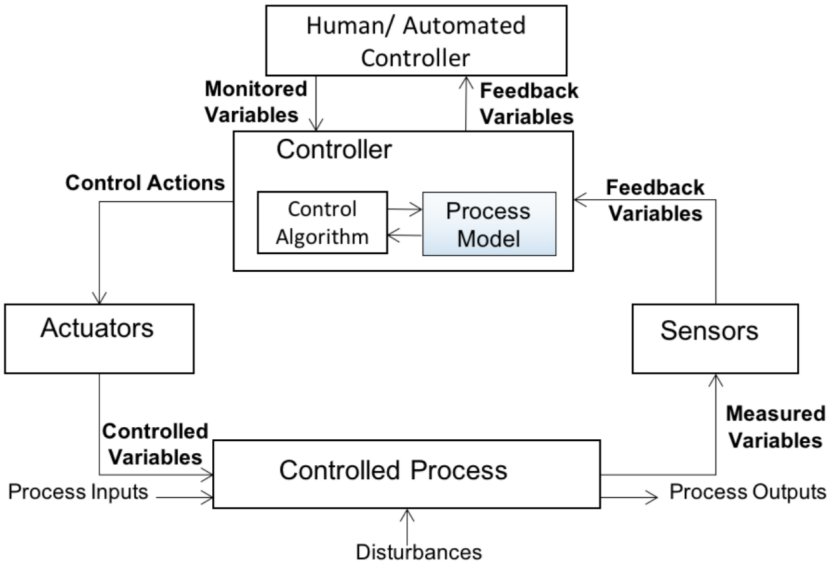

Figure 2.2: Basic control structure diagram [Abd17a]

STPA step 0

Step 0 is a preparation step performed at system level [Abd17a]. Its main goal is identifying fundamentals as a base for step 1. These fundamentals include accident, hazard and safety constraints.

First of all a description of the system must be provided. As mentioned before, it is not necessary to have full knowledge of the system so the description provided must not be detailed. An Accident (AC) is identified and according to it the Hazard (HA) leading to this accident is also identified. This hazard concerns the entire system and will always be related to this accident in the next steps of STPA. After defining the hazard at the system level, the corresponding Safety constraint (SC) is formulated. The formulation of the safety constraint is easy as it is only a negation of the hazard. Of course these constraints will be later refined and detailed.

The last part of STPA step 0 is constructing the safety control structure diagram. This diagram contains 4 main parts: the actuator, the sensor, the controller and the controlled process. It describes the major components of the system under investigation as well as their interactions (e.g. control actions, feedback) and roles.

While drawing the diagram, it is important to take into consideration

- What or who controls what,
- What commands are sent, and
- What feedback is received.

A basic control structure diagram is shown in figure 2.2

STPA step 1

Once the preparation step is completed, its output is used to further analyse the causes of the accidents identified, and to refine the safety constraints. Using the diagram from step 0, it is possible to identify Unsafe Control Action (UCA) in step 1 [Lev12].

Control Action (CA) is the commands sent from the controlling process to the controlled process in a loop. This control action might lead to a hazardous state. It is then called Unsafe Control Action. The goal of this step is identifying what are the unsafe control actions and to which hazard they lead. These control actions are important to understand the causes of an accident. They are only hypotheses. Then, they are investigated against the 4 possibilities listed below, in order to decide whether they lead to a hazard or not.

Since according to STPA, an accident is a caused by inadequate control, control actions are unsafe if they are:

- Not provided or not followed leads to hazard.
- Provided but lead to hazard.
- Provided too late or too early or out of sequence.
- Stopped too soon or applied too long.

The last possibility is only applied for continuous non discrete control actions like for example descending an airplane to avoid collision.

Each of the above listed items represent columns in a table and control actions are the rows. Every control action is tested against each of these possibilities and it will be decided whether the control action is hazardous or not. If not, then this control action is not considered. At the end, there will be only control actions leading to hazard will be used in the last step.

If a human is part of the control loop, it is important to specify in which context the human might take a decision and the decision is evaluated to determine whether it is hazardous or not.

For each of the unsafe control actions defined, a safety constraint is formulated and associated to it. At this level, the safety constraints have a context and are more detailed than the ones defined in step 0.

The STPA analysis is continued further in step 2.

STPA step 2

As mentioned before Step 1 is not sufficient, that's why step 2 is important [Lev12] because providing only safety constraints is not enough if the scenario, in which the hazardous state is reached is not specified.

Causal scenarios are a description of how the unsafe control action might occur. These scenarios are useful to provide guidance at the design stage or at later stages [Lev12]. STPA doesn't just specify hazards but also the way they might occur and this is what distinguishes STPA from any other hazard analysis technique.

To identify the causal scenario, the control structure diagram form Step 0 is needed. In Step 0 the diagram didn't contain many details as the analysis was performed at the system level. At this step, a process model is added to the controller. The process model specifies the functionalities of the corresponding component. It describes how the controller processes the information received of other components and how it takes the decision to send a certain control action.

After completing the diagram with the necessary information, each in Step 1 identified unsafe control action is investigated to identify the causal scenario. The investigation is performed as follows: the control loop corresponding to the unsafe control action is the one to focus on. Then from the process model of the controller, it is possible to derive the causal factors leading to hazard by analysing each variable in the process model and its relation to the unsafe control action. STPA provides guide words to help identify causal factors (cf. figure 2.3).

At the end of this step, safety constraints are refined and more details are added to it. These details are simply the new information contained in the causal sceanrios. The safety constraints are turned into safety requirements. These requirements are the final output of STPA that should be given to the designers to conceive a safe model, or if the design is already there, to help improve it and make it safer.

STPA can be performed many times until the system is free from unreasonable risk. It should be also revised each time an accident happens to see why the analysis didn't identify the cause and add new requirements. Whenever a change is applied to the design, the STPA modell should be updated [Lev12].

2.1.2 Extended STPA

Extended STPA was introduced by John Thomas in 2013 [Tho13]. It extends the analysis of the unsafe control action by adding a combination of variables extracted from the loops of the control structure diagram. This allows creating a context in which the unsafe control action might occur. That means that under each of the 4 possibilities (provided, not provided, provided too late, provided too soon), there is a set of variables whose combination describes in which context can for example not providing a control action lead to hazard. In some context not providing a control action doesn't lead to a hazard but in

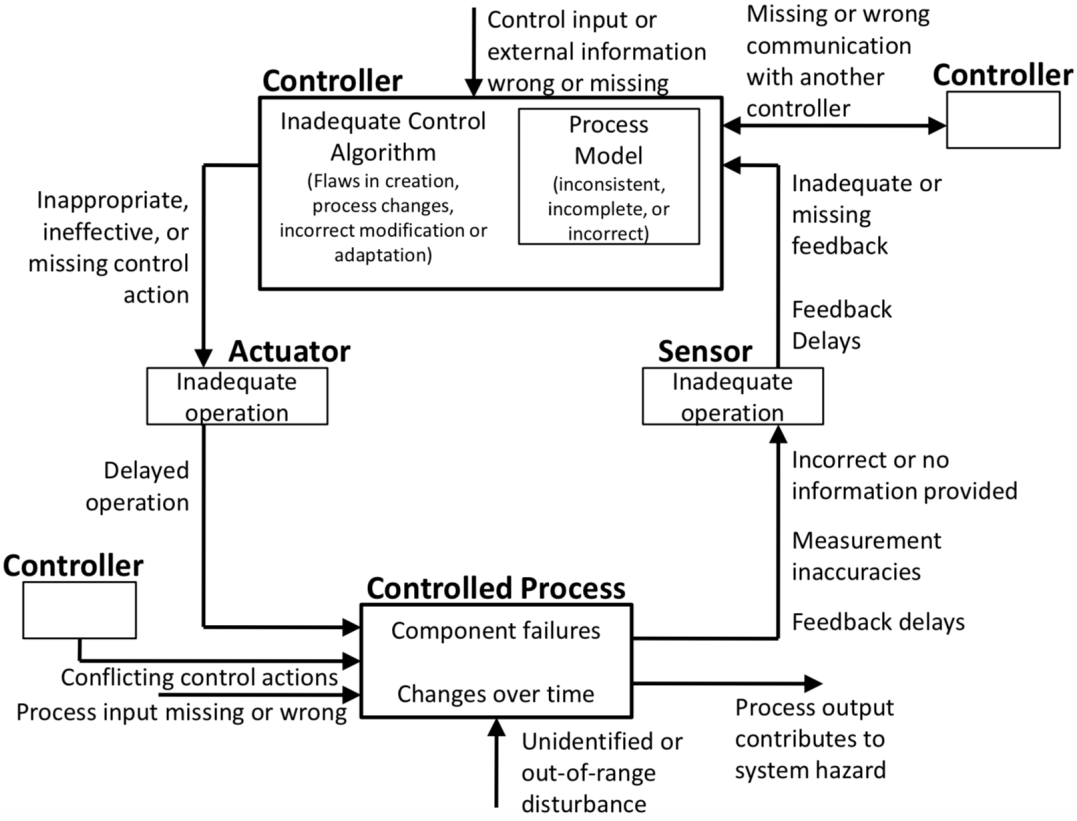

Figure 2.3: Guidewords in the control structure diagram [Lev12]

some other context it can be hazardous under certain circumstances, if combined with one or more variables. Extended STPA goes more into the details of the system to formulate the scenarios leading to a hazard. After collecting all the combinations, it is to decide whether they are hazardous or not. The hazardous combinations are then formulated into unsafe control actions and safety constraints. The analysis continued further to STPA step 2. The extention of STPA is only at step 1.

2.1.3 STPA train door example

In the following section, STPA steps will be further explained using the train door example from the STPA tutorial by John Thomas [Tho13]. The system functions as follows: The train door is opened or closed depending on the command sent by the controller to the actuator. These commands depend on variables like the train position (aligned with platform), emergency state, door obstruction. These variables are sent to the cotroller by the sensor.

It is important to mention that there is no complete scheme and description of the train door system so the system analyzed is a simplified one.

STPA step 0: Define fundamentals

Accidents and hazards along with safety constraints are identified through the process of brain storming.

System level accident:

- A 1: Person(s) is (are) injured.

Possible hazards leading to it:

- H 1: Door closes while a person is still standing in the doorway.
- H 2: Door opens when the train is moving or not at platform.
- H 3: Door does not open during an emergency.

System level safety constraints:

- SC 1: Door **must not** close while a person is still standing in the doorway.
- SC 2: Door **must not** open when the train is moving or not at platform.
- SC 3: Door **must** open during an emergency.

The structure control diagram in this step is kept simple (cf. figure 2.4).

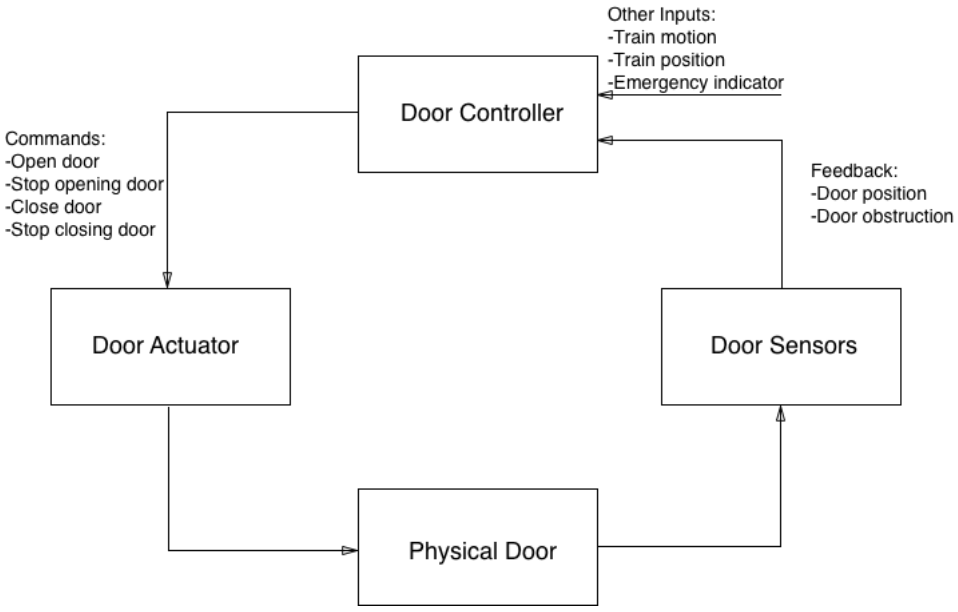

Figure 2.4: Control structure diagram [Tho13]

Control Action	Guide Word	Train State	Emergency	Train Position	Person in Doorway
Open Door Command	Provided	Stopped	Yes	Not Aligned with platform	Doesn't matter
		Stopped	No	Not Aligned with platform	Doesn't matter
		Moving	No	Not applicable	Doesn't matter
		Moving	Yes	Not applicable	Doesn't matter
	Not Provided	Stopped	Yes	Aligned with platform	Doesn't matter
		Stopped	Doesn't matter	Doesn't matter	Yes
	Provided too early/ too late	Moving	No	Doesn't matter	Doesn't matter
		Moving	Yes	Doesn't matter	Doesn't matter
		Stopped	Yes	Doesn't matter	Doesn't matter
		Stopped	No	Doesn't matter	Doesn't matter

Table 2.1: Analyzing control action using the 4 STPA guide words [Tho13].

STPA step 1: Identify unsafe control actions

The *Open door command* is investigated in table 2.1. For the entries of the table, the extended STPA approach was used to add a context to the unsafe control actions. For the sake of simplicity, only one control action is taken into consideration and that is the *Open door command*.

In the table 2.1, the possibility of the control action being applied for too long or stopped too soon is not applicable because the *open door command* is not a continuous non discrete command.

More combinations in the table 2.1 are of course possible, but they are not hazardous, so the table contains only the combinations that lead to a hazard.

Now the unsafe control actions can be formulated using table 2.1.

- UCA 1: Door open command provided while train is moving and there is no emergency [H-2].
- UCA 2: Door open command provided too late while train is stopped and emergency exists [H-3].
- UCA 3: Door open command provided while train is stopped,no emergency,and not at platform [H-2].
- UCA 4: Door open command provided while train is moving and emergency exists [H-3].
- UCA 5: Door open command not provided while train is stopped and emergency exists [H-3].
- UCA 6: Door open command not provided while door is closing on someone [H-1].

The next step is turning these UCAs into safety constraints:

- SC 1.1: Door open command **must not** be provided while train is moving and there is no emergency.
- SC 2.1: Door open command **must not** be provided too late while train is stopped and emergency exists.
- SC 3.1: Door open command **must not** be provided while train is stopped, no emergency, and not at platform.
- SC 4.1: Door open command **must not** be provided while train is moving and emergency exists.
- SC 5.1: Door open command **must** be provided while train is stopped and emergency exists.
- SC 6.1: Door open command **must** be provided while doors are closing on someone.

The safety constraints from step 2 are more detailed and context oriented than the ones identified in step 0.

STPA step 2: Identify causal factors

This step is not included in the tutorial.

In this step, UCA from STPA step 1 and the control structure diagram from STPA step 0 are used. The process model will be added to the controlling component in the diagram (cf. figure 2.5). In our case the process model is added to the *door controller*. For each UCA, we focus on the loop in the diagram responsible for it. For the sake of simplicity only one UCA from the above listed will be considered.

For UCA 1, possible Causal Scenario (CS)s are:

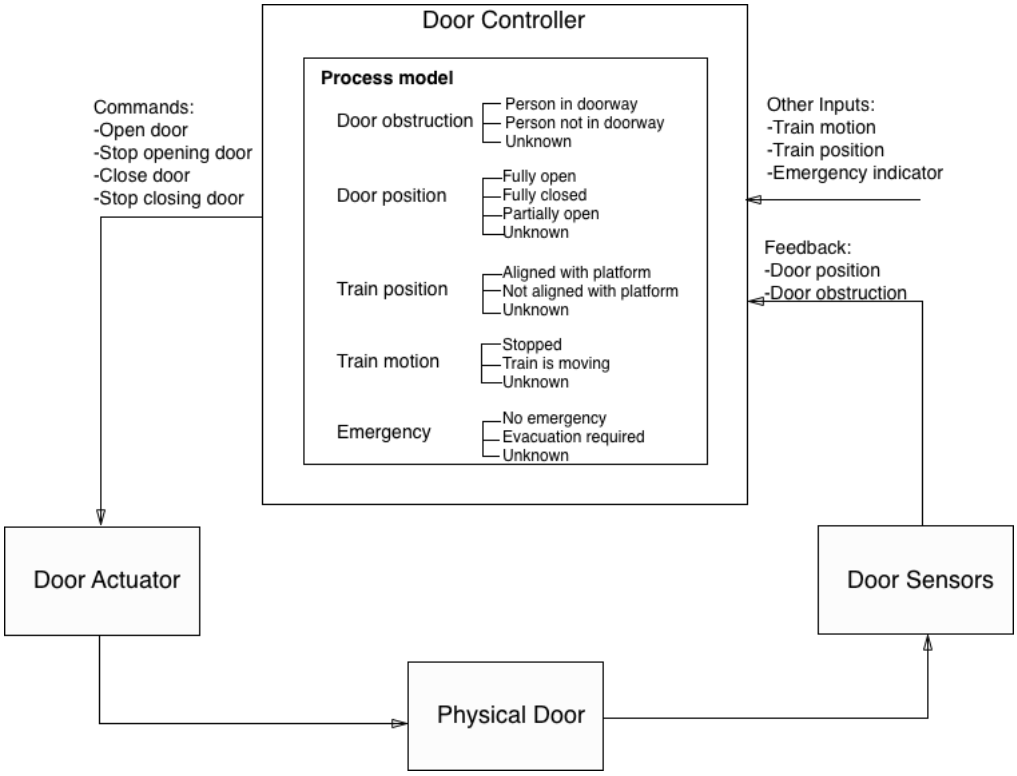

Figure 2.5: Control structure diagram of step 2 [Tho13]

- CS 1.1: Train motion input says that the train is stopped when it's still moving.
- CS 1.2: Train position input says that the train is aligned with platform when it's not.
- CS 1.3: Emergency indicator indicates an emergency when train is moving.
- CS 1.4: Door sensor indicates that a person is in doorway when train is moving.
- CS 1.5: Door open command is given when a person is in doorway but not followed by the door actuator.
- CS 1.6: Door open command given during emergency and train is stopped but not followed by the door actuator.

These are some of the possible causal scenarios for UCA 1 derived from the control structure diagram. The final safety constraints are:

- SC 1.1: Door controller must detect wrong input in combination with other inputs (door sensor indicated train is aligned while other input says it is still moving).
- SC 1.2: Door controller must detect whether its commands are followed or not.

The final safety constraints are the output of STPA.

2.2 ISO 26262

The ISO 26262 Standard was published in 2011 and deals with functional safety in Electrical and/or Electronic (E/E) systems in road vehicles. It is an adaptation of IEC 61508 and analyses hazards resulting from malfunctioning bahaviour of the E/E systems [sta11].

It contains 10 parts that cover the entire safety life cycle that includes management, development, production, operation, service, decommissioning of the elements of the system and describes the necessary steps in each part of the cycle. It also "provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved" [sta11]. ISO 26262 uses the V-Model (cf. figure 2.6) starting from concept phase (part 3) and ending in production and operation (part 7). Part 3 and Part 7 are found on the same level in figure 2.6 since they are interconnected in a causal sequence. The rest of the parts are independent and are performed at different levels which can be seen in the V-Model shown in figure 2.6.

Part 1 is concerned with definition of important terms that are used in the other parts of ISO 26262. Part 2 deals with management of functional safety. It contains 3 sections that describe the safety management during concept phase and after the item's release for production. Part 3 is the concept phase that will be detailed in section 2.2.1. Parts 4, 5 and 6 are executed using the V-Model. In part 5 (hardware development) and in part 6 (software development) a V-Model is also used. Part 7 is concerned with the production and operation. Part 8 specifies the supporting process. Part 9 is dedicated to ASIL-oriented and safety-oriented analysis. Finally, part 10 provides guidelines on ISO 26262.

ISO 26262 attributes a lot of importance into taking safety management and safety culture into consideration for the sake of safety. The standard doesn't only analyse hazard but also evaluates the risk using the Automotive Safety Integrity Level (ASIL). ASIL (Automotive Safety Integrity Level) has 4 levels going from the lowest to the highest: A, B, C and D. Each of these ASIL values are attributed to the safety requirements. Quality Management (QM) is attributed in case ASIL classification can not be attributed.

As mentioned before, hazard analysis and risk assessment is defined and described in part 3 of ISO 26262, that's why the emphasis in this document will be on part 3 of the standard.

2.2.1 ISO 26262-3: Concept phase

The purpose of the concept phase is conceiving an item, which means preparing the design and description of the functionalities, interactions etc. The concept phase also includes the hazard analysis. After completing the item conception and after conducting the hazard analysis, the product development phase begins. The concept phase contains 4 main parts: item definition, initiation of safety life cycle, hazard analysis and risk assessment, and finally the functional safety concept.

An overview of the concept phase along with description, prerequisites and the output of each step are in table 2.2.

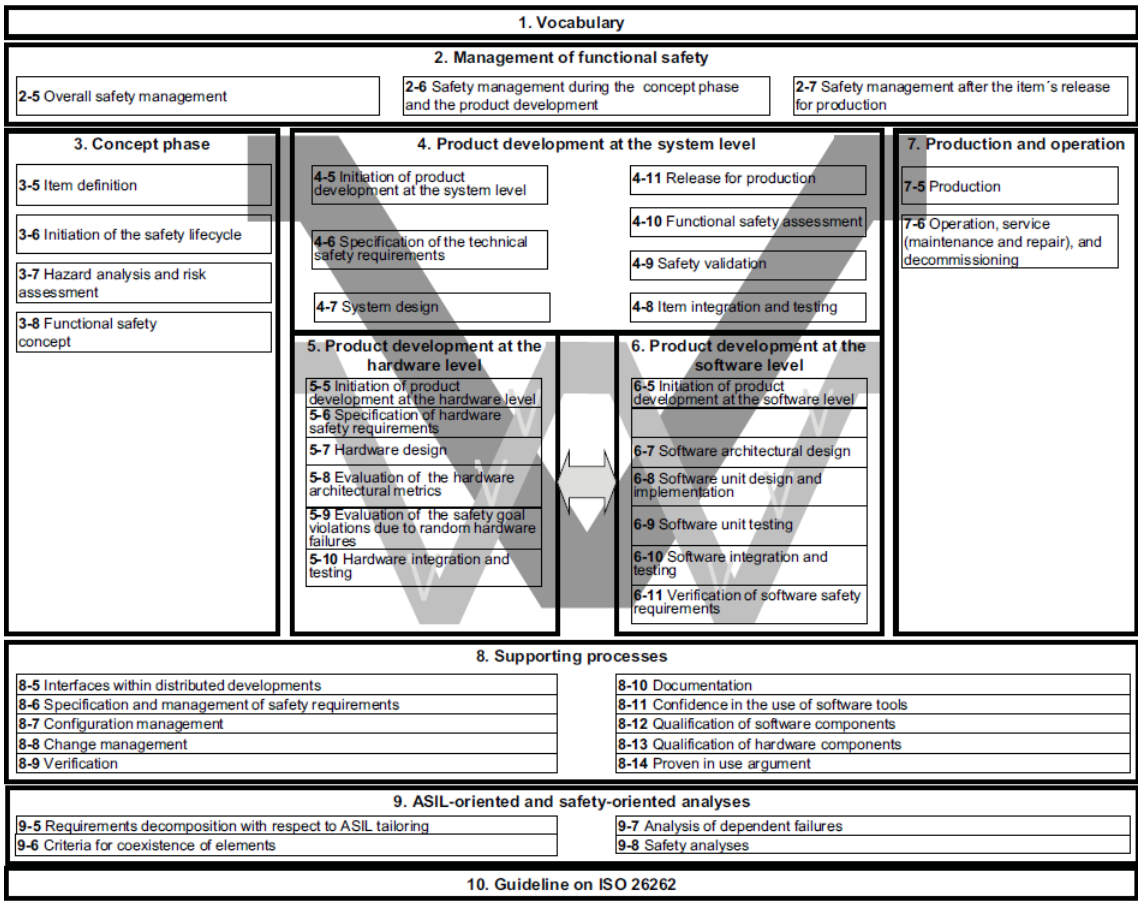

Figure 2.6: Overview of ISO 26262 [sta11]

In the following sections, each of the concept phase clauses will be described.

Item definition

Item definition is the first clause of the concept phase and is the input of the next clauses. It has as a goal defining and describing the item to be analysed. The description should contain the functional and non-functional requirements, the dependencies as well as the item's interactions with the environment and assumptions related to it. In addition, the boundary of the item and its interfaces should be listed in the definition. This definition helps the safety analysist to better understand the item.

Initiation of the safety life cycle

Item definition is the input for this clause.

Clause	Objectives	Prerequisites	Output
Item definition	Definition and description of the item to be developed along with its dependencies and interactions.	None	Item definition
Initiation of the safety life cycle	Distinguish between new item development and modification to an existing item. Define activities to be performed in case of modification.	Item definition	Impact analysis Safety plan
Hazard analysis and risk assessment	Identify possible hazards and categorize them. Define safety goals	Item definition	Hazard analysis and risk assessment. Safety goals. Verification review report.
Functional safety concept	Derive functional safety requirements from safety goals.	Item definition Hazard analysis and risk assessment. Safety goals	Functional safety concept. Verification report of the functional safety concept.

Table 2.2: Overview of the concept phase [sta11]

The initiation of the safety lifecycle starts with identifying whether the item under investigation is a to be modified or developed, in other words identify whether the item already exits or not. If the item already exists and is to be modified, then the activities that will be performed should be defined, like identifying the modifications to be applied and their impact on the item's safety. In case of a new development, the cycle is continued with the hazard analysis and risk assessment.

Hazard analysis and risk assessment

This is the most important clause of the concept phase and is the focus of this thesis. It has as an objective identifying and classifying possible hazards to formulate safety goals that will help preventing the unreasonable risk. The item definition is also the input of this clause. Hazard analysis and risk assessment contains 5 parts: situation analysis, hazard identification, classification of hazardous events, determination of ASIL and safety goals and finally verification.

Situation analysis Situation analysis describes "the operational situations and operating modes in which an item's malfunctioning bahaviour will result in a hazardous event" [sta11]. It also describes how far can the item behave in a safe manner.

Hazard identification In this step, hazards are identified using several techniques such as brain storming, field studies or FMEA. The analysis is conducted at vehicle level where hazards are identified observing the behaviour of the item.

This identification is done by combining different operational situations from the situation analysis. Guidewords can be used for this purpose and are listed along with an example in table 2.3.

Guideword	**Example**
Without requirement	Window opens without request
Failure	Car window is doesn't open despite request
Too weak	Not relevant for car window
Too strong	Not relevant for car window
Too late	Car window is opened too late
Too early	Car window is opened too early
Wrong direction	Not relevant
intermittently	Car Window opens intermittently

Table 2.3: Guidewords to derive hazards in HARA analysis [Poh15]

Only hazards associated to the item are taken into consideration and if the item doesn't directly affect safety, then the analysis is terminated. Furthermore, to each hazard identified, consequences are associated. If the function of the item is distributed over many systems then the analysis is as follows:

- "Analyse the functional space used by the error-free function [Poh15]".
- "Analyse the area outside the functional space which is still accepted by the receiver's side [Poh15]".
- "Analyse the unlimited real space theoretically possible without limit [Poh15]".

At the end of this step, the identified hazards are associated to the situations from the situation analysis.

Classification of hazardous events All hazardous events identified previously that are within the scope of ISO 26262 are classified. This classification is made considering 3 factors: Severity (S), Probability of Exposure (E) and Controllability (C)[sta11].

Severity is estimated based on the potential harm of each hazardous event to persons potentially at risk [sta11]. For this purpose, the sequence of events of the situation must be taken into consideration. Possible injuries is also an important factor to help determine severity, that's why it is possible to use the Abbreviated Injury Scale (AIS). Severity can also be determined based on combination of injuries.

Severity classes range from S0 to S3, with S0 being the lowest and S3 being the highest(cf. figure 2.7). If the hazard's severity is a S0 class, then an ASIL classification is not necessary.

	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 2.7: Classes of severity [sta11]

Probability of exposure characterizes the operational situations, and is determined "based on a rationale for each hazardous event" [sta11]. It also has 5 classes from E0 to E4 (cf. figure 2.8). If the class E1 is assigned, no ASIL classification is necessary. An important factor to be considered while estimating the probability of exposure is the number of vehicles containing the item. But this doesn't mean that the fewer vehicles equipped with the item the less the class becomes.

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

Figure 2.8: Classes of probability of exposure [sta11]

The last factor is the controllability. It also has 4 classes form C0 to C3 (cf. figure). It is also estimated based on a rationale that indicates to which extent can the hazardous event be controlled by the persons potentially at risk to avoid the harm. An estimation of class C0 doesn't require a determination of ASIL.

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

Figure 2.9: Classes of controllability [sta11]

Determination of ASIL and safety goals Based on severity, probability of exposure and controllability, an ASIL class can be determined. Figure 2.10 shows how can ASIL class be

determined based on combinations of S, E and C. ASIL classes range from A to D, with D being critical. In addition to the 4 mentioned classes of ASIL, there is an additional class QM. Quality management denotes that there is no safety requirement to comply with.

It is important to note that if an ASIL estimation is difficult, then a higher ASIL should be assigned instead of a lower one. After Assigning an ASIL class A, B, C or D to all the

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 2.10: ASIL determination [sta11]

hazardous events, a Safety Goal (SG) for each hazard is formulated. Safety goal is a "top-level safety requirement for the item" [sta11]. One safety goal can be assigned to different hazards. If this is the case, then the safety goal will receive the highest ASIL among the determined ASILs. Safety goals can also be combined if they are similar. From these safety goals, safety requirements are determined to avoid the unreasonable risk. In the case of a safety goal being only achieved by transitioning or maintaining certain safe state (s), then this state should be documented. An example of a such safe state is a locked vehicle stationary.
It is important to note that the ASIL assigned to the safety goals evaluates the safety goal and not the system.

Verification This is the final step of HARA where all the formulated safety goals should be verified and reviewed by the team. The important factors to be considered while verifying are:

- "Completeness with regard to situations and hazards [sta11]".
- "Compliance with item definition [sta11]".
- "Consistency with related HARA [sta11]".
- "Consistency of the assigned ASILs with the corresponding hazardous events [sta11]".

The output of this clause is the hazard analysis and risk assessment, the safety goals and the verification review.

Functional safety concept

With this clause, terminates the concept phase of ISO 26262. In this clause, Functional Safety Requirement (FSR) are formulated from the previously determined safety goals. To formulate the requirements, it is important to take the entire function into consideration, form the input (sensor) to the output (actuator). Functional Safety Concept (FSC) should also specify how the requirements are combined together to fulfill the safety goal. These requirements are allocated to the architectural elements of the item. Other than the inputs mentioned in table 2.2, assumptions made on the preliminary architectural elements can be a further support. At least one safety requirements should be assigned to each safety goal and one requirement can be assigned to more than one goal.

These factors should be taken into consideration while formulating functional safety requirements:

- Operating modes.
- Fault tolerant time interval.
- Safe states.
- Emergency operation interval.
- Functional redundancies.

Techniques like fault tree analysis (FTA) can support this clause. Safety goals are the input of FTA as top event. Using FTA is meaningful for goals with ASIL C, D.

Further information that should be added to the functional safety concept:

- Emergency operation if a safe state cannot be reached within an acceptable time interval.
- Actions that should be taken by the driver or a person potentially at risk to reach the safe state.
- The means and controls available for the driver or the person potentially at risk to reach the safe state.

Warning and degradation concept are also part of the functional safety requirement. It is a "specification of how to alert the driver of potentially reduced functionality and how to provide his reduced functionality to reach the safe state [sta11]".

2.2.2 Example: Car window regulator

This example is from Daimler's previous analysis of the system [Wei13]. The analysis was simplified to fit in this thesis.

Item definition

The window can be opened or closed using the window regulator switches in the door. The windows can be moved manually by pressing the switch longer or automatically by briefly pressing the switch. In the second case, a pinch protection is activated and in the case of trapping, the closing process is stopped and the window is automatically open by at least 125 mm. If manual mode is active and trapping is detected, then the window will be automatically opened by a maximum of 20 mm when the control switch is released. Child safety button can be activated to disable opening the 2 windows in the back.

The function Pre-safe shuts deactivates the pinch protection in case of danger.

The function passenger protection requests opening the window by 50mm after an airbag release.

Hazard analysis and risk assessment

Situation analysis 7 situations are identified: parking (general situation), parking with kids playing in the car, accident(general situation), accident with a car falling into water, highway, city traffic, country road.

Hazard identification 4 hazards are identified:

- H1 :Window opens without request.
- H2: Window closes without request.
- H2: Window doesn't close despite request.
- H4: Window doesn't open despite request.

In table 2.4, it is identified in which situation can the hazard be relevant.

Classification of hazardous events and determination of ASIL In table 2.5, the hazards are classified using the 3 parameters S, E and C and ASIL class is determined. For simplicity reasons only H1 is analysed. The situations in the table are a result of relevant situation selection from situation's tree. It is important to note that a justification of the chosen classes of S, E and C should be in the documentation.

Situation	H1	H2	H3	H4
Parking	relevant	relevant	relevant	relevant
Parking with kids playing in the car	relevant	relevant	not relevant	not relevant
Accident	relevant	relevant	relevant	relevant
City traffic	relevant	relevant	not relevant	not relevant
Country road	relevant	relevant	relevant	not relevant
Highway	relevant	relevant	not relevant	not relevant
Accident with car falling into water	not relevant	not relevant	not relevant	relevant

Table 2.4: Assigning hazards to the situations

Hazard	Driving situation	S	E	C	ASIL
H1.1	Parking	1	3	1	QM
H1.2	Parking with kids playing in the car	1	3	1	QM
H1.3	Accident	2	1	3	QM
H1.4	City traffic	1	4	1	QM
H1.5	Country road	1	4	1	QM
H1.6	Highway	1	4	1	QM

Table 2.5: Classification oh hazards and determination of ASIL

Determination of safety goals and the corresponding ASIL One safety goal is identified:

- SG1: Serious injuries due to pinching situation when closing the window are prevented (ASIL A).

It is important to mention that the ASIL associated to the safety goal evaluates the safety goal itself and not the system.

Safety concept is then created with detailed requirements derived from the safety goals.

2.3 Comparison between STPA and ISO 26262-3

In this section STPA and ISO 26262-3 will be compared using different criteria.

2.3.1 Comparison between terminologies

STPA and ISO 26262-3 are approaches that aim to analyse the hazards, but they have different terminology. Each approach defines terms like hazard differently and some terms are defined in one approach and not in the other.

Table 2.6 contains mapping of definition of terms from STPA to ISO 26262-3 and vice versa.

Term	**Definitions in STPA [Lev12]**	**Definitions in ISO 26262-3 [sta11]**
Accident	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.	No mapping
Risk assessment	No mapping	Examination of a characteristic of an item or element.
ASIL	No mapping	One of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk.
System	A set of interrelation components	Set of elements that relates at least a sensor, a controller and an actuator with one another.
element	No mapping	System or part of a system including components, hardware, software, hardware parts and software units.
Item	No mapping	A system or array of systems to implement a function at the vehicle level to which ISO 26262 is applied.
Error	No mapping	Discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition.
Failure	No mapping	Termination of the ability of an element to perform a function as required.

Fault	No mapping	Abnormal condition that can cause an element or an item to fail.
Functional safety concept	No mapping	consists of functional requirements and preliminary architectural assumptions.
Safety constraints/functional safety requirements	**Safety constraints**: Are related to the system components—physical, human, and social—that enforces the safety property.	**Functional safety requirements**: Specification of implementation-independent safety bahaviour, or implementation-dependent safety measure, including the safety related attributes.
Harm	No mapping	A physical injury or damage to the health of persons.
Hazard	A system state or set of conditions that together with a particular set of worst-case environmental conditions will lead to an accident.	No mapping
Hazardous event	No mapping	combinations of hazard and operational situations.
Malfunctioning behaviour	No mapping	Failure or unintended behaviour of an item with respect to its design intent.
Risk	No mapping	Combination of the probability of occurrence of harm and the severity of that harm.
Unreasonable risk	No mapping	Risk judged to be unacceptable in a certain context according to valid societal moral concepts
Safety	emergent property that arises when system components interact with each other within a larger environment	Absence of unreasonable risk
Different terms	**Corresponding safety constraint**: Top-level safety constraints derived from the UCA.	**Safet goal**: Top-level safety requirements as a result of HARA.

Control action	A command sent from the controlling process to the controlled process to perform a certain action.	No mapping
Unsafe control action	A control action that might lead to a hazard.	No mapping
Causal factor	Describes how UCA might occur.	No mapping
Safe state	No mapping	Operating mode of an item without an unreasonable level of risk.
Operational situation	No direct mapping (Partially process model)	Scenario that can occur during a vehicle's life.
Operating mode	No direct mapping (Partially process model)	Perceivable functional state of an item or element.
Process model	Added to the controlling process in the control structure diagram to determine its variables	No direct mapping (Partially operating mode and operational situation)
Control structure diagram	Break the item into components and specify their interactions	No direct mapping (Partially item definition)
Item definition	No direct mapping (Partially control structure diagram)	Describes the item, its dependencides and interactions.

Table 2.6: Comparison of terminologies in STPA and ISO 26262-3
(Updated from [AwL+17])

From table 2.6 it is to conclude that ISO 26262 includes more definitions of terms that have no mapping in STPA.

2.3.2 Comparison between procedures

Both methods can be used without having a lot of knowledge about the system. Yet they differ in the analysis process (cf. table 2.7).

2.3.3 Advantages and disadvantages of STPA and ISO 26262-3

For each of ISO 26262-3 and STPA, the advantages as well as the disadvantages are listed below.

	STPA	**HARA/ISO 26262-3**
Phase	used in all stages of the development of the system.	used at the concept phase of the item.
Describing the item using	Control structure diagram	Item definition
Identifying hazards	Identify accidents then the related hazards.	Identify the different functions of the item and then formulate the hazards.
Operational situation	Not considered	Considered
Safety constraints/Safety goals	Refined at each step.	Formulated at the end of the analysis.
Output	Safety constraints	Functional safety concept

Table 2.7: Differences between STPA and ISO 26262-3

Advantages and disadvantages of STPA

Advantages of STPA:

- Applied in all stages of the development of an item.
- Takes hazards resulting from unsafe interactions between system components into consideration which helps define more hazardous scenarios including human error and environmental factors.
- Defines not just hazards but also the way they might occur.
- Detailed safety constraints.
- Models the system and its boundary

Disadvantages of STPA:

- No suggested technique to define hazards, accidents and causal scenarios.
- Unlike ISO 26262 and HARA, STPA has no glossary for all terms
- It is no clear how to perform the analysis of multi control actions (parallel control actions).

Advantages and disadvantages of ISO 26262-3

Advantages of ISO 26262-3:

- Includes risk assessment process: risk is evaluated using ASIL.

- Contains detailed definitions of each term.
- Specifies the operating mode and the operational situation while performing the analysis.
- Takes safety management and safety culture into consideration [MPA+16].

Disadvantages of ISO 26262-3:

- No guidance on how to define the item.
- Determination of E, and C are not standardized [MPA+16].
- Doesn't take human errors, environmental factors and hazards resulting from unsafe interactions between system's components into consideration.

Despite all these differences, STPA and ISO 26262-3 can be used together in a compliant process and chapter 4 describes how to.

3 Related Work

This chapter discusses the previous work related to ISO 26262 and STPA.

In [Tho13], John Thomas introduced the extended STPA, which extends step 1 of STPA and helps formulate unsafe control actions using a combination of the process model variables. This way the unsafe control actions will have a context which makes the formulation of safety constraints more specific. But it is difficult to apply especially to complex systems since it generates a large number of combinations an thus a large number of constraints.

The A-STPA tool [AW14b] is a tool developed by Asim Abdulkhaleq and Stefan Wagner at the university of Stuttgart that represent a platform to conduct safety analysis using STPA methodology. Also the XSTAMPP platform [AW15] develeped by Asim Abdulkhaleq and Stefan Wagner, helps conducting safety analysis and includes X-STPA, a tool used for extended STPA, and helps generate combinations from the variables of the process model. X-STAMPP translates the safety constraints into the formal LTL language which allows an automated verification of the safety requirements.

In [AW13], STPA was applied to an adaptive cruise control to investigate the use of STPA in the automotive domain. STPA identified more causes of hazard but still has some problems regarding guidance in step 2. STPA doesn't specify a certain method to examine the loops in the control structure diagram and derive causal factors. Also it cannot be used for more than one controller.

In [AwL+17], Abdulkhaleq et al. applied STPA in compliance with ISO 26262 in the automotive domain to support the HARA process. STPA was applied to a fully automated vehicle and was proven to be effective and can be efficiently integrated in the concept phase of ISO 26262.

Also Mallaya et al. [MPA+16] investigated the use of STPA in an ISO 26262 compliant process. The paper states that STPA need to be augmented in order to be applied in compliance with ISO 26262 since the latter includes the risk assessment process.

In [Abd17a], two automotive case studies were introduced: ACC with stop and go, and Autonomous vehicle. It illustrates the results of the use of STPA in automotive domain that show that STPA can be successfully applied to automotive systems.

STPA was also applied to software-intensive systems in [AWL15]. The purpose was developing a safe software by embedding the safety analysis process in the development process. STPA can also be applied to an existing software as well. Similarly, in [AW14a] STPA was applied to a software system and the safety requirements were formulated. These

requirements were then verified against violation at the code level. From these two papers it is to conclude that STPA can be directly used for software.

Ishimatsu et al. applied STPA to a software system in the HTV, that was developed by Japan Aerospace Exploration Agency (JAXA) [ILT+10]. The STPA analysis results were compared to the previous results of the fault tree analysis. The comparison showed that STPA identified causal factors in addition to the failures that were already identified in the fault tree analysis. This experiment showed that STPA can be successfully applied in the aerospace domain.

Kraus et al. introduced the SAHRA tool [KRR+16], which is a platform that helps conduct the STPA analysis. It uses UML to model the STPA control structure as well as a Mindmap based analysis editor for step 1 and 2.

Kriso et al. [KTA+12] represented in 2012 an executive summary of ISO 26262 that describes functional safety according to the standard as well as how the functional safety can be achieved.

Hommes in [Hom12] applied STPA to an adaptive cruise control. The author compared STPA to existing standards in the industry and found that STPA has more categories of requirements. The author in [Hom15] used STPA together with Hazard and Operability Study (HAZOP) and FMEA to generate the functional safety concept.

4 Applying STPA in an ISO 26262 compliant process

This chapter discusses the integration of the STPA methodology in the concept phase of ISO 26262. The process diagram as well as a description of each step and the necessary inputs is provided in the following sections.

4.1 Establishing STPA in the concept phase of ISO 26262

This section describes the process diagram of the integration of STPA in ISO 26262-3 as shown in figure 4.1. The diagram contains 11 steps overall. The steps are a combination of steps from ISO 26262-3 and STPA.

These steps do not confirm 100% with the steps of the both previously mentioned methods, as they were modified in order to be compliant.

The modifications are:

- Splitting STPA step 1 and 2 to facilitates the integration of STPA into ISO 26262-3. Since different outputs from different steps in ISO 26262-3 are needed as inpt in STPA step 1 and 2 at different levels, the STPA steps had to be splitted.
- Not defining safety constraints at STPA step 0 since they will not be used later in the process diagram.
- Formulating the hazardous events using the unsafe control actions.
- Using safety constraints instead of safety goals.

More details of the adaptation of the STPA steps and the description of each step in the process diagram are in the following subsections.

4.1.1 Overview

The table 4.1 contains an overview of the steps of the process diagram along with the necessary inputs and the outputs of each step.

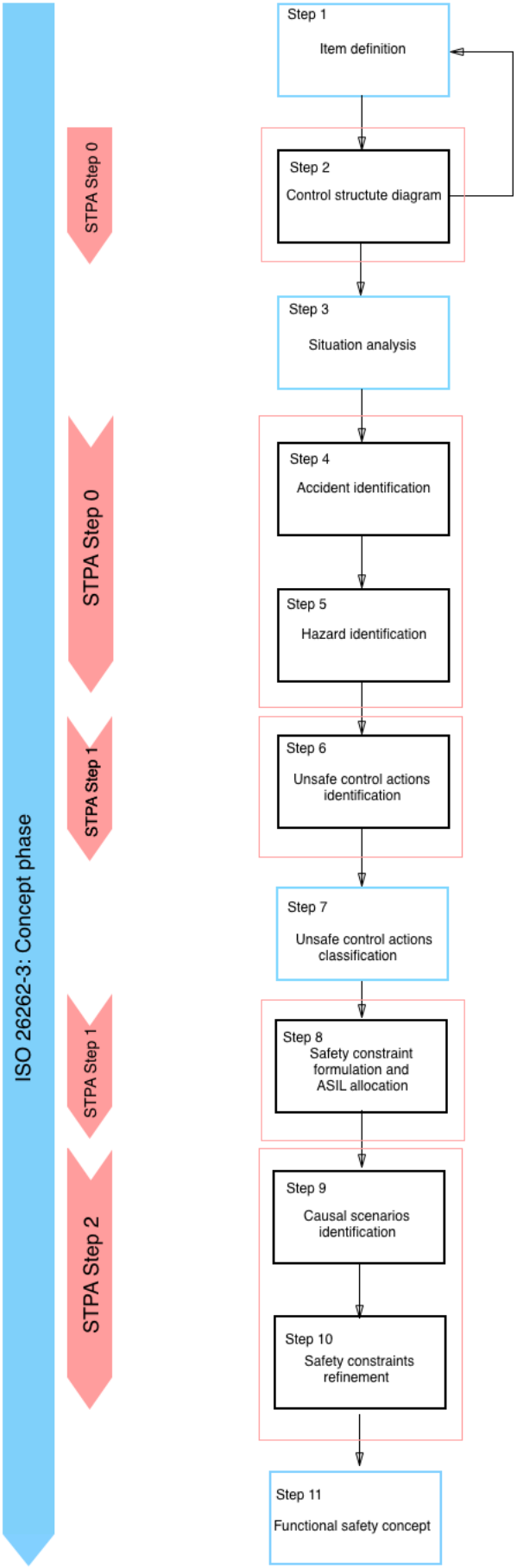

Figure 4.1: Integration of STPA into the concept phase of ISO 26262

Step	Input	Output
Item definition	None	Item definition
Control structure diagram definition	Item definition	Control structure diagram
Situation analysis definition	Item definition	Operational situations Operating modes
Accident identification	Item definition Situation analysis	Accidents
Hazard identification	Accidents Operational situations Operating modes	Hazardous events
Unsafe control actions identification	Hazardous event Control structure diagram	Unsafe control actions
Hazardous event formulation and classification	Unsafe control actions Item definition Operational situations Operating modes	Hazardous event ASIL
Safety constraint formulation and ASIL allocation	Unsafe control actions ASIL Hazardous events	Safety constraints ASIL ASIL
Causal scenarios identification	Unsafe control action Control structure diagram	Causal scenarios
Safety constraints refinement	Safety constraints Causal scenarios ASIL	Safety constraints
Functional safety concept	All results from previous steps	Functional safety concept

Table 4.1: Overview of the integration of STPA in the concept phase of ISO 26262

4.1.2 Step 1: Item Definition

Item definition is the starting point of the analysis. At this step, the Item's components are described using the functional and non-functional requirements, the dependencies, the item's interactions with the environment, assumptions related to it, the boundary of the item and its interfaces.

The output of this step serves as an input for the next step. The Item definition does not stop at this stage, it is continued in the next step using the control structure diagram. Both of these steps help identifying the item to give the safety analysist the necessary information about the item.

4.1.3 Step 2: Control Structure Diagram

The input of this step is the item definition. This step is derived form STPA step 0. In this process diagram STPA step 0 was divided in order to fit in the process of ISO 26262-3. While item definiton is a text, this step is a graphic illustration of it. It translates the text into a diagram and adds more information to it if necessary.

The diagram contains 4 major components: the controller, the actuator, the controlled process and the sensor. Commnads sent and feedback received are derived from the item definition with the possibility of adding more information that wasn't included in the item definition. If while drawing the diagram, an information was missing it can be added to the item definition, that's why there is a loop between the first two steps.

If a human is involved in the functioning of the item, the human controller component should be added to the diagram along with commands sent and feedback received. It is important to mention the context in which a human can take a certain decision. This specification should be mentioned in the item definition or in case it wasn't mentioned, it can be added after the diagram has been drawn as there is a loop between the first two steps.

The human is not considered in the item definition at first because the item definition is derived from ISO 26262-3, and it doesn't take human behaviour into consideration. The description of the human component can be done before the start of the second step. But since in ISO 26262-2 it is not mentioned how it can be done, it is better to go with the STPA approach as the diagram provides guidance on what information should be considered to describe the human component. That's why this step completes the item definition and together they define the item completely, which in later steps help derive accidents and hazards.

The loop between both step is performed until the diagram is complete, which means all the information presented in the item definition is represented in the diagram in addition to the human controller in case a human is involved.

4.1.4 Step 3: Situation Analysis

This step also belongs to ISO 26262-3 and doesn't differ from the one described in section 2.2.1. Here, we specify the "operational situations and operating modes in which a system's malfunctioning behaviour could occur"[sta11], for example *parking*, *driving in a highway*, etc.

This step serves as guideline to first understand the functioning of the system in different situations and second, it helps identifying accidents and hazards and making them more specific and concrete, since certain accidents can only happen in certain situations. This helps covering the entire functionality of the system and helps identifying the most number of accidents and hazards possible.

4.1.5 Step 4: Accident Identification

This step is derived from STPA step 0. In the diagram, it is noticeable that STPA step 0 was splitted. In this step accidents are identified. A technique to identify the accidents is not specifed neither in STPA nor in ISO 26262-3. But in our case the item definition and situation analysis serve as a guideline and can help identifying the accidents.

The accidents concern the system as a whole, so identifying them starts first from understanding the basic functionality of the system specified in the item definition and the control structure diagram. Then it is to specify how a possible malfunctioning behaviour of the system can lead to an accident taking into consideration the operational situation. There could be one or more accidents. Accidents should be given an identifier to facilitate the analysis. An identifier can be for example AC1 (accident number 1: vehicle crashes with another vehicle and people are injured).

Brain storming or field studies are also helpful means that could assist the safety analysist to identify the accidents.

4.1.6 Step 5: Hazard identification

After identifying the accidents, for each one of them we identify possible hazards leading to it, taking into consideration of course the operational situation. Step 3 (situation analysis) and step 4 (accident identification) serve as guideline to identify the hazards as they narrow the possibilities. But brain storming or other techniques are still needed because there is no established technique for hazard identification. The hazards identified should be linked to the accident and could be given an identifier e.g. H1.1 (hazard one corresponding to accident 1: Sudden acceleration of the vehicle leads to a crash with another one).

4.1.7 Step 6: Unsafe control actions identification

This step corresponds to STPA step 1. At this level, we go back to the control structure diagram in step 2 of the process diagram. For each control action sent from the controller to the actuator, we investigate the way this control action can be unsafe, in other words, how it can lead to a hazard. For this purpose 4 possibilities are taken into consideration: provided, provided too early/too late, stopped too soon/applied too long, not provided. A table containing all the 4 possibilities is created, and we start investigating each control action. Each control action have to be combined with the operational situations to add

context to it and investigate whether in this context this control action is hazardous or not. If the control action is unsafe it is kept in the table, otherwise it is removed. At the end of this step, unsafe control actions are identified and can be given an identifier. An example of unsafe control action can be: Accelerate command provided when driving through in intersection. An exmaple of an identifier can be USC 1.1.1 (unsafe control action 1 corresponding to hazard 1 corresponding to accident 1).

A more detailed description on how to identify unsafe control actions is provided in section 2.1.1.

The table containing the unsafe control actions is the output of this step.

4.1.8 Step 7: Unsafe control actions classification

The previously formulated unsafe control actions are classified using the automotive safety integrity level ASIL. ASIL has 4 classes going from A to D with D being the most critical. The determination of ASIL calss is based on 3 factors: severity (S), probability of exposure(E) and controllability (C). Quality management class QM can also be attributed to the hazardous event in case S0, E1 or C0 was given. For example, for severity class S2, exposure class E1 and controllability class C3 the ASIL class is QM. The detailed description of the determination of S, E and C as well as the ASIL class are in section 2.2.1 as in diagram the classification step doesn't differ from the one used in ISO 26262-3.

The unsafe control action along with ASIL are the output of step 7 of the process diagram.

4.1.9 Step 8: Safety constraints formulation and ASIL allocation

This step corresponds to part 2 of STPA step 1. Just like STPA step 0, step 1 was also splitted to fit into the process diagram.

For each unsafe control action, one or more safety constraints must be formulated using the negation. Safety constraints are either formulated using unsafe control actions from step 6 or the hazardous events formulated in step 7. In the first case, the ASIL allocated is the highest among all the ASILs associated to the hazardous events related to the unsafe control action as defined in ISO 26262. In the second case, ASIL associated to the hazardous event is directly allocated to the safety constraint. The decision whether to formulate safety constraint using option one or option two is must be taken according to the relevance of the operational situation in the safety constraint. In other words, whether different solutions must be found to different situations or one solution is valid for all the situations. The decision is left to the safety analyst. An identifier for safety constraints can be SC 1.1.1 (Safety constraint corresponding to the UCA 1.1.1)

Safety constraints and their ASILs are the output of this step.

4.1.10 Step 9: Causal scenarios identification

This step corresponds to the first part of STPA step 2. Causal scenarios are identified in the same way as in STPA. Causal scenarios describe the way unsafe control actions might occur. For this purpose, the control structure diagram is needed. The process model is added to the controller in the diagram. It can also be added while drawing the diagram at step 2.

Combining the variables in the process model that are related to the unsafe control action, gives many possible scenarios. These scenarios are combined with the operational situations and each scenario is investigated to determine whether it is the cause of the unsafe control action or not. If it is the cause then the scenario is kept and is given an identifier (For example CS 1.1.1.1: Casual scenario 1 corresponding to the USC 1.1.1: the speed value shown to the driver is lower than the actual speed, so he accelerates while driving on the highway).

A more detailed description on how to identify causal scenarios is provided in section 2.1.1.

Causal scenarios are the output of this step.

4.1.11 Step 10: Safety constraints refinement

In this step, for each of the causal scanerios previously identified, one or more safety constraints are formulated. They are formulated by simply negating the causal scenario. They are considered as a refinement of the previous safety constraint as they contain more details. The ASIL classification is allocated to the new safety constraints.

Safety constraints are the output of this step.

4.1.12 Step 11: Functional safety concept

This is the final step of the process diagram and is derived form ISO 26262-3 and contains safety requirements derived from safety constraints previously formulated. It has as an input all results of the previous steps. It is described in detail in section 2.2.1. The only difference is that the functional safety concept in this process diagram contains safety constraints defined in step 10 instead of the safety goals used in the standard.

A functional safety concept is the final output of the analysis.

4.2 Case Study: Cruise Control

This section presents an example of how to apply the new method described in the process diagram to analyse an automotive system. The system to be analysed is the cruise control. This system was chosen because first it is not complicated in comparison with other systems, and second it was previously analysed at Daimler AG and the results of the previous analysis are needed to compare them with our results.

A previous analysis of the system using STPA approach was also done and can be found in [AW14a]. Some similarities between accidents and hazards identified in this thesis and in the mentioned paper can be found but here the formulation is different as more factors in the accident and in the associated hazards formulation are taken into consideration.

4.2.1 Step 1: Item definition

The Item definition is taken from previous case study of the cruise control at Daimler AG [Gab14]. Here only the necessary parts of the item definition are considered for simplicity reasons.

The cruise control is designed to regulate the vehicle's speed. It can be activated and the speed can be increased, decreased or actual speed saved. Under speed of 20 Km/h the cruise control cannot be activated. The system is deactivated when the driver presses the break, the accelerator or using the system's control elements. The system is automatically deactivated if the speed of the vehicle is reduced to 20 km/h or if an error in the system was detected.

Functionalities of the cruise control

The below described functionalities are the ones that can be controlled by the user.
Set: save actual speed.
On: regulate speed to the stored value.
Off: deactivate the cruise control.
Plus: increase actual speed to value n and subsequently maintain it.
Minus: decrease actual speed to value n and subsequently maintain it.
Constant plus: the cruise control speed is constantly increased by value m per time unit t.
Constant minus: the cruise control speed is constantly decreased by value m per time unit t.

4.2.2 Step 2: Control structure diagram

The figure 4.2 shows the control structure diagram of the cruise control. The input received by the controller actually comes from different sensors of different systems, but in the diagram it is reduced to one component called sensors.

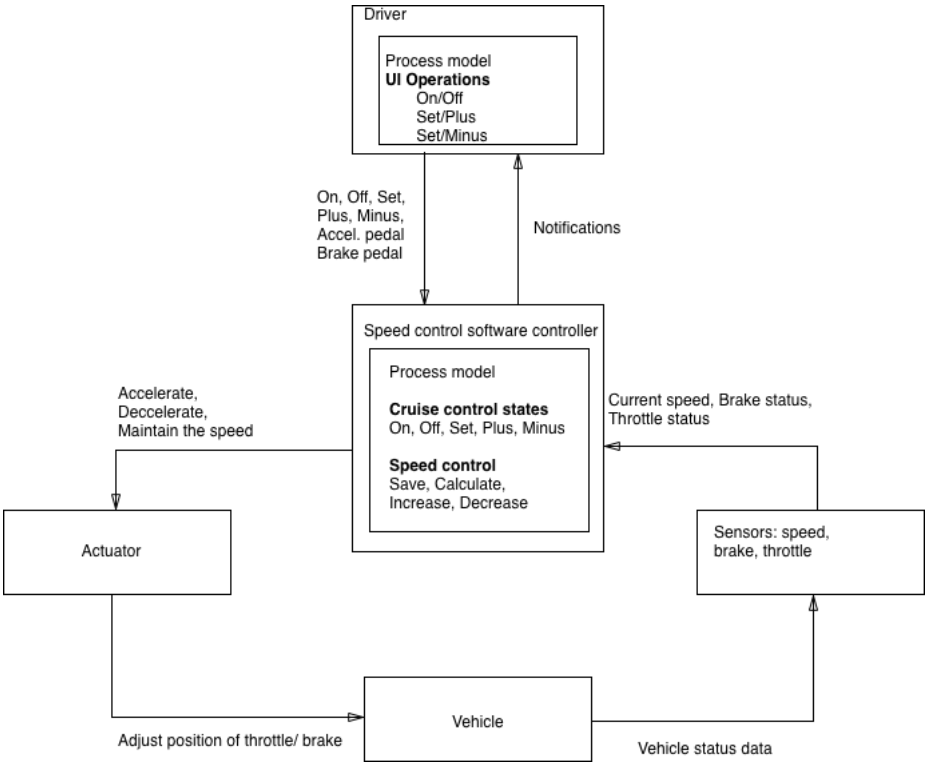

Figure 4.2: Control structure diagram of the cruise control [AW14a]

4.2.3 Step 3: Situation analysis

In this section the different operational situation of a vehicle are mentioned. The situations are chosen from Daimler's specification of the different operational situations in a vehicle's lifecycle [AG]. Depending on the system and its functions, the operational situations are selected.

- **S1**: Parking
- **S2**: Driving through intersection
- **S3**: Urban traffic
- **S4**: Driving on a highway
- **S5**: Off-road

- **S6**: Starting up the car and driving

For simplicity reasons, the situations weren't further specified, like for example in the highway situation there could be a normal as well as a high traffic situation. In our case these distinctions were not considered.

4.2.4 Step 4: Accident identification

There is one accident identified:

AC1: A crash with another vehicle and the occupants are injured while the cruise control is operation.

4.2.5 Step 5: Hazard identification

For the above identified accident two hazards were found:

H1: The cruise control doesn't receive the right command (On, Off, Set, Plus, Minus, Accel. pedal, break pedal) in the right time from the driver.

H2: Unintended acceleration or decceleration of the vehicle or not deccelerating when needed when cruise control is in active mode [AW14a].

Since there is only one accident the identifier of the hazard can be kept simple (H1 instead of H1.1).

The hazards are at a high level, and its role is to help identifying the unsafe control actions.

4.2.6 Step 6: Unsafe control actions identification

In this step, unsafe control actions are identified. For this purpose, the control structure diagram is needed. For each control action sent from the *driver* to the *speed control software controller* as well as from the latter to the *actuator*, we examine if the control action is safe or not using 4 possibilities:

- Provided.
- Provided too early/too late.
- Applied for too long/stopped too soon.
- Not provided.

Each control action is combined with the operational situations. Then we investigate whether in that context the control action is unsafe or not because some control actions are unsafe in a certain context and the operational situation provides that context.

In this example, only one operational situation is chosen for each unsafe control action.

The table 4.2 contains the unsafe control actions. It is important to note that the table contains only the identifier of the unsafe control action and not the entire sentence for visibility reasons.

All the unsafe control actions derived from the table 4.2 are listed below along with their identifier.

Control action	**Provided**	**Provided too early/too late**	**Applied for too long/stopped too soon**	**Not provided**
On	UCA 1.1 [H1]	UCA 1.2 [H1]	N/A	Not hazardous
Off	Not hazardous	UCA 1.3 [H1]	N/A	UCA 1.4 [H1]
Set	Not hazardous	Not hazardous	UCA 1.5 [H1]	Not hazarous
Plus	UCA 1.6 [H1]	UCA 1.7 [H1]	UCA 1.8 [H1]	Not hazardous
Minus	Not hazarous	UCA 1.9 [H1]	UCA 1.10 [H1]	UCA 1.11 [H1]
Accel.pedal	UCA 1.12 [H1]	UCA 1.13 [H1]	UCA 1.14 [H1]	Not hazardous
Brake pedal	Not hazardous	UCA 1.15 [H1]	UCA 1.16 [H1]	UCA 1.17 [H1]
Accelerate	UCA 2.1 [H2]	UCA 2.2 [H2]	UCA 2.3 [H2]	Not hazardous
Deccelerate	UCA 2.4 [H2]	UCA 2.5 [H2]	UCA 2.6 [H2]	UCA 2.7 [H2]
Maintain the speed	Not hazardous	UCA 2.8 [H2]	UCA 2.9 [H2]	Not hazardous

Table 4.2: Identification of the unsafe control actions

Note: Pressing the brake pedal shuts the system down but here we suppose that the system mistakenly was not shut down, so it is hazardous if the driver doesn't press the brake pedal long enough to reach the right speed.

So the unsafe control actions identified are:

- **UCA 1.1**: On command provided while parking[H1].
- **UCA 1.2**: On command provided too early while driving in urban traffic [H1].
- **UCA 1.3**: Off command provided too late while driving on the highway [H1].
- **UCA 1.4**: Off command not provided while driving on the highway [H1].

- **UCA 1.5**: Set command provided too early while driving through an intersection [H1].
- **UCA 1.6**: Plus command provided while driving in urban traffic [H1].
- **UCA 1.7**: Plus command provided too early while driving in the highway [H1].
- **UCA 1.8**: Plus command applied for too long while driving in the highway [H1].
- **UCA 1.9**: Minus command provided too late while driving in urban traffic [H1].
- **UCA 1.10**: Minus command stopped too soon while driving in urban traffic [H1].
- **UCA 1.11**: Minus command not provided while driving in urban traffic [H1].
- **UCA 1.12**: Accel.pedal pressed (provided) while driving in urban traffic [H1].
- **UCA 1.13**: Accel.pedal pressed too soon while driving in urban traffic [H1].
- **UCA 1.14**: Accel.pedal pressed for too long while driving in urban traffic [H1].
- **UCA 1.15**: Brake pedal pressed too late while driving in urban traffic [H1].
- **UCA 1.16**: Brake pedal released too early while driving in urban traffic* [H1].
- **UCA 1.17**: Brake pedal not pressed while driving in urban traffic and there are cars behind [H1].
- **UCA 2.1**: Accelerate command provided while driving in urban traffic [H2].
- **UCA 2.2**: Accelerate command provided too early while driving in urban traffic [H2].
- **UCA 2.3**: Accelerate command applied for too long while driving in urban traffic [H2].

- **UCA 2.4**: Deccelerate command provided while driving in urban traffic and there are cars behind [H2].

- **UCA 2.5**: Deccelerate command provided too late while driving in urban traffic [H2].

- **UCA 2.6**: Deccelerate command stopped too soon while driving in urban traffic [H2].

- **UCA 2.7**: Deccelerate command not provided while driving in urban traffic and there are cars in front [H2].

- **UCA 2.8**: Maintain the speed command provided too early while driving in urban traffic [H2].

- **UCA 2.9**: Maintain the speed command applied for too long while driving in urban traffic [H2].

4.2.7 Step 7: Unsafe control actions classification

For sake of simplicity, in this case study only two unsafe control actions will be selected from the table and will be combined with the all operational situations. The selection of the unsafe control actions is based on how representative they are in determining the S,E, C and ASIL. The table 4.3 and 4.4 contain the hazardous events and the associated S, E, C and ASILs for UCA 1.5 and UCA 2.4 respectively.

Remark 1: For deccelerate command, the parking situation was excluded as it does not combine with the unsafe control action because deccelerating while parking is not hazardous.

Remark 2: Normally, in the situations were the speed is supposed to be under 20 Km/h (e.g. parking) the system should be deactivated, but the case that the system is activated without request or when speed is under 20 Km/h is considered. That's why for example *plus command* is provided while parking is hazardous.

Unsafe control action	**E**	**S**	**C**	**ASIL**
Plus command provided while parking	E4	S1	C3	B
Plus command provided while driving through intersection	E3	S3	C3	C
Plus command provided in urban traffic situation	E4	S2	C3	C
Plus command provided in off-road	E2	S2	C3	A
Plus command provided in highway	E4	S2	C3	C
Plus command provided while starting up the car and driving	E3	S1	C3	A

Table 4.3: Classification of hazardous events for UCA 1.5

The exposure classes were estimated based on the Daimler's catalog [AG].

Severity classes were chosen regarding the type of injury. S1 is chosen if the injury is light and moderate. Class S2 is chosen if the injury is life-threatening. Class S3 is chosen if the injury is fatal and the survival is uncertain.

Controllability is estimated based on the extent to which a situation can be controlled by the car's driver or other drivers. C3 is chosen if the reaction time is too short and the situation is hard to control. C2 is chosen if the situation can be controlled and the car's driver or involved persons have enough time to react.

4.2.8 Step 8: Safety constraints formulation and ASIL allocation

For the identified unsafe control actions, safety constraints are formulated. For each of the safety constraints, an ASIL is allocated. In this case, the operational situation need to be included in the safety constraint. For ASIL allocation we choose the highest one among the ASILs associated to the hazardous events corresponding to the unsafe control action. For sake of simplicity only one operational situation is chosen for each safety constraint.

Hazardous event	E	S	C	ASIL
Deccelerate command provided while driving through intersection	E3	S2	C3	B
Deccelerate command provided in urban traffic situation	E3	S2	C3	B
Deccelerate command provided in off-road	E2	S2	C3	A
Deccelerate command provided in highway	E4	S2	C2	B
Deccelerate command provided while starting up the car and driving	E3	S0	C0	QM

Table 4.4: Classification of hazardous events for UCA 2.4

So the safety constraints are:

- **SC 1.1.1**: On command must not be provided while parking [H1].
- **SC 1.2.1**: On command must not be provided too early while driving in urban traffic [H1].
- **SC 1.3.1**: Off command must not provided too late while driving on the highway [H1].
- **SC 1.4.1**: Off command must provided while driving on the highway [H1].
- **SC 1.5.1**: Set command must not be provided too early while driving through an intersection [H1].
- **SC 1.6.1**: Plus command must not be provided while driving in urban traffic [H1] **[ASIL C]**.

- **SC 1.7.1**: Plus command must not be provided too early while driving in the highway [H1].

- **SC 1.8.1**: Plus command must not be applied for too long while driving in the highway [H1].

- **SC 1.9.1**: Minus command must not be provided too late while driving in urban traffic [H1].

- **SC 1.10.1**: Minus command must not be stopped too soon while driving in urban traffic [H1].

- **SC 1.11.1**: Minus command must be provided while driving in urban traffic[H1].

- **SC 1.12.1**: Accel.pedal must not be pressed (provided) while driving in urban traffic [H1].

- **SC 1.13.1**: Accel.pedal must not be pressed too soon while driving in urban traffic [H1].

- **SC 1.14.1**: Accel.pedal must not be pressed for too long while driving in urban traffic [H1].

- **SC 1.15.1**: Brake pedal must not be pressed too late while driving in urban traffic [H1].

- **SC 1.16.1**: Brake pedal must not be released too early while driving in urban traffic* [H1].

- **SC 1.17.1**: Brake pedal must not pressed suddenly while driving in urban traffic and there are cars behind [H1].

- **SC 2.1.1**: Accelerate command must not be provided while driving in urban traffic [H2].

- **SC 2.2.1**: Accelerate command must not be provided too early while driving in urban traffic [H2].

- **SC 2.3.1**: Accelerate command must not be applied for too long while driving in urban traffic [H2].

- **SC 2.4.1**: Deccelerate command must not be provided while driving in urban traffic and there are cars behind [H2] **[ASIL B]**.

- **SC 2.5.1**: Deccelerate command must not be provided too late while driving in urban traffic [H2].

- **SC 2.6.1**: Deccelerate command must not be stopped too soon while driving in urban traffic [H2].

- **SC 2.7.1**: Deccelerate command must be provided while driving in urban traffic and there are cars in front [H2].

- **SC 2.8.1**: Maintain the speed command must not be provided too early while driving in urban traffic [H2].

- **SC 2.9.1**: Maintain the speed command must not be applied for too long while driving in urban traffic [H2].

Remark: Since for ASIL determination only two UCAs were investigated, so only two in the list above are allocated an ASIL.

4.2.9 Step 9: Causal scenarios identification

For each of the unsafe control actions identified above, causal scenarios have to be identified. For this purpose, we go back to the control structure diagram and focus on the input received by the controller and the driver.

Causal scenarios are also combined with the operational situations defined in step 3. In our case, for simplicity reasons, each causal scenario is combined with only one operational situation (for most of the scenarios the highway situation was selected).

More than causal scenario for each unsafe control action were identified, but here only one for each unsafe control action is listed:

- **CS1.1.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway, so the driver turns the cruise control on while the speed of the vehicle surpasses the allowed value [H1].

- **CS1.2.1**: The driver unintentionally starts the cruise control system while driving in urban traffic [H1].
- **CS1.3.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway, so the driver turns off the cruise control too late after the speed of the vehicle has surpassed the allowed value [H1].
- **CS1.4.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway so the driver doesn't turns off the cruise control and the speed of the vehicle has surpassed the allowed value [H1].
- **CS1.5.1**: The cruise control sets the speed according to the actual speed of the vehicle too early while driving in the highway before the driver slows down and before receiving set command from him so the speed of the vehicle surpasses the allowed speed [H1].
- **CS1.6.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway so the driver increases the speed and the speed of the vehicle surpasses the allowed value [H1].
- **CS1.7.1**: The driver unintentionally increases the speed while driving in the highway so the speed of the vehicle surpasses the allowed value [H1].
- **CS1.8.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway so the driver keeps increasing the speed and the speed of the vehicle surpasses the allowed value [H1].
- **CS1.9.1**: The driver decreases the speed but the cruise controller state is not set to minus immediately while driving in the highway so the speed of the vehicle is decreased too late [H1].
- **CS1.10.1**: The system stops responding to the minus command given by the driver while driving in the highway and the decreasing of the speed stops too soon [H1].
- **CS1.11.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway so the driver doesn't give the minus command the speed and the speed of the vehicle surpasses the allowed value [H1].
- **CS1.12.1**: The accelerator status received by the controller is set to true while driving in the highway although the driver didn't press the pedal and the cruise control accelerates [H1].
- **CS1.13.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway so the driver presses on the accelerator and the speed of the vehicle surpasses the allowed value [H1].
- **CS1.14.1**: The accelerator status received by the controller is set to true while driving in the highway although the driver stopped pressing the pedal and the cruise control keeps accelerating [H1].

- **CS1.15.1**: The correct speed value notification is given to the driver too late while driving in the highway, so the driver presses the brake pedal too late [H1].
- **CS1.16.1**: The cruise control is not shut down although the driver had pressed the brake while driving in the highway [H1].
- **CS1.17.1**: The speed notification given to the driver is lower than the actual speed while driving in the highway so the driver doesn't press the brake pedal and the speed of the vehicle surpasses the allowed value [H1].
- **CS2.1.1**: The accelerator status is set to true while driving in the highway so the controller gives the accelerate command to the actuator and the speed of the vehicle surpasses the allowed value [H2].
- **CS2.2.1**: The cruise control starts working and the controller gives the accelerate command to the actuator while the speed is lower than 20 Km/h while starting up the car and driving* [H2].
- **CS2.3.1**: The cruise control state is set to plus although the driver stopped giving plus command so the controller keeps giving the accelerate command to the actuator while driving in the highway and the speed of the vehicle surpasses the allowed value [H2].
- **CS2.4.1**: The cruise control state is set to minus although the driver stopped giving minus command while driving in the highway so the controller keeps giving the deccelerate command to the actuator and the speed of the vehicle is too low in the highway which causes crash with the vehicle behind [H2].
- **CS2.5.1**: The controller gives deccelerate command to the the actuator but the latter doesn't follow the command while driving in the highway and the speed of the vehicle surpasses the allowed value [H2].
- **CS2.6.1**: The cruise control state is no longer minus although the driver still giving minus command while driving in the highway so the controller stops sending deccelerate command to the actuator and the speed of the vehicle surpasses the allowed value [H2].
- **CS2.7.1**: The accelerator status received by the controller is set to true although the driver stopped pressing the pedal and the cruise control is accelerating while driving in the highway [H2].
- **CS2.8.1**: The speed control sets the speed status to save although set command is not received while driving in the highway so the actual speed is maintained although it surpasses the allowed speed value [H2].
- **CS2.9.1**: The speed control status is not set to decrease although the driver has given the minus command while driving in the highway so the speed of the vehicle surpasses the allowed value [H2].

*: For this scenario, the highway situation is not relevant.

It is noticeable that for some unsafe control actions, the cause is the same, for example the speed value given is lower than the actual speed of the vehicle. The reason for that is that the system was simplified and fewer inputs were considered. The more the variables are the more scenarios can be identified.

4.2.10 Step 10: Safety constraints formulation

In this step, safety constraints are formulated using the causal scenarios identified above.

The final safety constraints are:

- **SC1**: The speed notification given to the driver must not be lower than the actual speed of the vehicle **[ASIL C]**.
- **SC2**: The driver must not unintentionally starts the cruise control system while driving in an urban traffic situation.
- **SC3**: The cruise control must not set the speed according to the actual speed of the vehicle too early before the driver slows down and before receiving set command from the driver..
- **SC4**: The driver must not unintentionally increase the speed.
- **SC5**: The cruise controller state must be set to minus immediately when the driver gives minus command.
- **SC6**: The system must not stop responding to the minus command given by the driver.
- **SC7**: The accelerator status received by the controller must not be set to true although the driver didn't press the pedal.
- **SC8**: The accelerator status received by the controller must not be set to true although the driver stopped pressing the pedal and the cruise control must not keep accelerating.
- **SC9**: The correct speed value notification must not be given to the driver too late.
- **SC10**: The cruise control must shut down when the driver presses the brake pedal.
- **SC11**: The speed control software must not give accelerate command when accelerator status is false.
- **SC12**: The cruise control must not start working and the controller must not give the accelerate command to the actuator while the speed is lower than 20 Km/h.
- **SC13**: the cruise control state must not be set to minus when the driver had stopped giving minus command **[ASIL B]**.

- **SC14**: the cruise control state must not be set to plus when the driver had stopped giving plus command.
- **SC15**: The actuator must follow the decrease command given by the controller.
- **SC16**: The cruise control state must still be minus when the driver still giving minus command.
- **SC17**: The speed control must not set the speed status to save although set command is not received from the driver.
- **SC18**: The speed control status must be set to decrease when the driver gives the minus command.

Remark 1: In some safety analysis cases, it could be necessary to include the operational situation in the safety constraint if it is relevant. This is not our case.

Remark 2: In our case, since not all inputs of the controller were taken into consideration to simplify the analysis, some causal scenarios do not differ from each other if we remove the operational situation. That's why the number of safety constraint is less then then the number of causal scenarios as in our case they are not related to the operational situations. Here for two or more causal scenarios there is only one safety constraint.

4.2.11 Step 11: Functional safety concept

The functional safety concept specifies "the functional safety requirements with associated information, their allocation to architectural elements, and their interaction necessary to achieve the safety goals" [sta11]. The process of creation of the functional safety concept does not differ from the one defined in ISO 26262-3. Due to the limit of the bachelor thesis, the functional safety concept cannot be created. As a suggestion, this can be part of a future work.

4.3 Comparing outputs

In this section, the safety constraints formulated using the new proposed method are compared with the safety goals from the previous Daimler's study. The comparison is in table 4.5.

To make the table shorter, it only contains the safety constraints to which a mapping to one or more safety goals exist because the number of safety constraints identified surpasses the number of safety goals. On the other hand, all safety goals from the previous study are included in the table even if there is no mapping to the safety constraints.

The mapping in table 4.5 is a partial mapping because the formulation of safety goals and safety constraints is different. Safety constraints are more concrete and detailed than safety goals.

ID	Safety constraints	Safety goals from previous Daimler study
SC6	The accelerator status received by the controller must not be set to true although the driver didn't press the pedal.	An unintentional excessive acceleration is to be prevented (SG 1). Inadvertent acceleration to spin the wheels should be prevented (SG 2).
SC7	The accelerator status received by the controller must not be set to true although the driver stopped pressing the pedal and the cruise control must not keep accelerating.	An unintentional excessive acceleration is to be prevented (SG 1). Inadvertent acceleration to spin the wheels should be prevented (SG 2).
SC10	The speed control software must not give accelerate command when accelerator status is false.	An unintentional excessive acceleration is to be prevented (SG 1). Inadvertent acceleration to spin the wheels should be prevented (SG 2).
SC12	the cruise control state must not be set to minus when the driver had stopped giving minus command.	An unintentional decceleration is to be prevented (SG 3). An inadvertent strong decceleration, which causes the wheels to lock and thus causes instability must be prevented(SG 4).
SC13	the cruise control state must not be set to plus when the driver had stopped giving plus command.	An unintentional excessive acceleration is to be prevented (SG 1). Inadvertent acceleration to spin the wheels should be prevented (SG 2).
	No mapping	A self starting in the wrong direction is to be prevented (SG 5).
SC2	The driver must not unintentionally starts the cruise control system while driving in an urban traffic situation.	Unauthorized starting is to be prevented (SG 7).

Table 4.5: Mapping of the safety constraints to safety goals from the previous study.

5 Evaluation

This chapter contains the evaluation of the new method presented in Chapter 4. The Evaluation has the form of a questionnaire. The questionnaire contains 16 questions overall, 13 of them are put in table and will be answered using the following scores:

- -2 = Strongly Disagree.
- -1 = Disagree.
- 0 = Neither agree nor disagree.
- 1 = Agree.
- 2 = Strongly Agree.

The last three are open questions.

The questions were divided in 3 categories: learnability, usability and effeciency and were answered by two experts from Daimler AG and their answers are listed below.

Questions to learnability:

1. The structure of the process diagram was clear and well-structured.

- Answer 1: 1
- Answer 2: 2

2. The new method was easy to learn.

- Answer 1: 2
- Answer 2: 1

3. It is clear to me why the steps in the process diagram are put in this sequence.

- Answer 1: 2
- Answer 2: 2

4. The graphical notation and tables of the new method were helpful for me to document the safety constraints.

- Answer 1: 2
- Answer 2: 2

5. It is clear to me what are the inputs and outputs of each step and their importance.

- Answer 1: 2
- Answer 2:-1

6. It is clear to me what is the importance of each step in the process diagram.

- Answer 1: 1
- Answer 2:-2

7. It is clear to me the importance of the result of each step for the next one.

- Answer 1: 1
- Answer 2:-1

Questions to usability:

1. I wasn't confused when using the new method.

- Answer 1: 2
- Answer 2: 0

2. It is clear to me how to perform the major steps of the new method.

- Answer 1: 2
- Answer 2: 1

Questions to effectiveness:
1. I think the new method is more applicable for identifying the system's relevant safety constraints.

- Answer 1: 0
- Answer 2: 1

2. The new method provides a systematic way to identify safety constraints.

- Answer 1: 2

- Answer 2: 2

3. The integration of STPA in ISO 26262-3 was effective.

- Answer 1: 2
- Answer 2: 1

4. The process diagram doesn't contain redundancies.

- Answer 1: 1
- Answer 2:-1

Open questions:

1. How would you rate the use of the new method for identifying safety constraints?

- Answer 1: The method is well suited to identify safety constraints. In a further step the terminology of safety constraints (STPA term) and safety goals/requirements (ISO 26262 terms) should be harmonized and the related activities combined into one step.
- Answer 2: I believe, it would be able to cover quite complete hazardous events. But more applications would be needed to clear the importance of some process steps as well as practical costs. Otherwise, it would be problematic for a wider application.

2. What advantages has the new method in comparison with the HARA from ISO 26262?

- Answer 1: It includes the STPA control loop as a high level abstraction of the functionality and extends the scope of the analysis beyond EE failures to also cover human bahaviour and other influencing factors.
- Answer 2: Paradigm to structure the system diagram could be a good visualization tool. It could integrate human interactions (e.g. misuse scenarios) into the process, while HARA as defined in ISO 26262 doesn't include this aspect in scope.

3. What disadvantages has the new method in comparison with the HARA from ISO 26262?

- Answer 1: The ASIL dependent methods and measures that are currently described in ISO 26262 are, to a large extent, specific for EE failures to also cover human behaviour and other influencing factors.
- Answer 2: Not clear cost-benefit ratio. It seems to be more time-expensive

The results of the evaluation are in chapter 6.

6 Results

This chapter contains the results of the evaluation from the previous chapter. The scores for each category are calculated by summing the scores given by the 2 experts.

6.1 Learnability

Minimum score: -28
Maximum score: 28
Actual score: 14

The results show that the method is easy to learn, as it is well-structured and the sequence of the steps is clear. Both of the expert agree that the graphic notations and tables help by the documentation. On the other hand, the input and output as well as the importance of each step wasn't clear enough.

6.2 Usability

Minimum score: -8
Maximum score: 8
Actual score: 5

The scores show that the method is easy to use and the user is not confused and it is clear to him how to perform the major steps.

6.3 Effectiveness

Minimum score: -16
Maximum score: 16
Actual score: 8

Both of the experts agree that the method provides a systematic way to identify safety constraints and that the integration of STPA in ISO 26262-3 was effective. Since the method is still not widely used, it cannot be assumed 100% that it is more applicable for identifying the system's relevant safety constraints . This needs more applications of the new method to other automotive systems.

6.4 Advantages and disadvantages

According to both of the experts, the new method is able to cover more causes of hazards and identify safety constraints. The control structure diagram is considered an advantage as it includes the human controller as part of the control loop and takes other influencing factors into consideration as well. They think that these new modifications increase the scope of ISO 26262.

On the other hand, the ASIL classification according to ISO 26262 is specific to E/E failures and it is not proven yet whether it is suited to classify the human behaviour and other influencing factors. The method also is time-consuming as the number if unsafe control actions, causal scenarios and safety constraints related to only one accident is huge, which can be noticed in the cruise control example in chapter 4.

7 Summary and future work

This chapter contains the summary and the future work.

7.1 Summary

This thesis presents a suggested approach of the integration of STPA methodology in the concept phase of ISO 26262. The purpose of this integration is increasing the scope of ISO 26262.

First of all, it was important understanding STPA and HARA from ISO 26262-3. It started by understanding the different terminologies, and chapter 2 contains a table with the definitions of each term used in each methodology with possible mappings. Then it was demonstrated how each step from both methodologies can be performed and were further explained examples. STPA was explained using the train door example and ISO 26262-3 was explained using the window regulator example. A good understanding of STPA and ISO 26262-3 helped compare between both of them and also helped derive the advantages and disadvantages of each methodology. This constitutes the basics needed to integrate STPA in ISO 26262-3.

By the start of the integration the first problem encountered was the terminologies. Despite being fully discussed in chapter 2, the problem encountered during the integration is the difference of the use and formulation of hazards in both methodologies because hazards identified in STPA does not correspond to the hazards identified in ISO 26262-3. In ISO 26262-3, the hazards are more detailed, thus it corresponds to the unsafe control actions defined in STPA step 1. The hazards used in our method correspond to the STPA's hazards, the high level hazards leading to the accident identified in STPA step 0.

Another problem is that some results of steps in ISO 26262-3 are needed as input in STPA step 0 and 1 but at different levels. For example the situation analysis is needed to identify the accidents. But at the same time, the situation analysis comes after the control structure diagram that defines the item. So it was necessary to split STPA step 0. In the same way STPA step 1 was also splitted.

The new method was used to analyse the cruise control system. This system was previously studied and analysed at Daimler, and the results of this study were used to compare them with our results.

While applying the new method to the cruise control system, the problem encountered was the huge number of unsafe control actions, hazardous events, causal scenarios and safety

constraints despite the cruise control system being simplified. So the number was reduced to fit in this thesis.

At the end of the analysis, and while mapping the safety constraints with the safety goals from a previous study, one safety goal had no mapping. The reason is that the number of causal scenarios was reduced and not all inputs and feedbacks were considered for simplicity reasons. Even for safety goals, for which a mapping exists, it was a partial mapping because safety goals are more abstract than safety constraints. So it was really difficult to map the new results to the old ones. But despite the fact that 2 safety goals had no mapping, the number of safety constraints is 18 compared to 7 safety goals, which means 11 safety constraints were new and not were not identified before. This despite the system being simplified. This shows that the new method is effective as it identified more causes of hazards and is easy to use according to the experts' evaluation.

This thesis shows that STPA can be integrated in an ISO 26262 compliant process. The integration of STPA in the concept phase of ISO 26262 helps broaden its scope, thus it is now possible to take the human behaviour and other influencing factors into consideration. The control structure diagram also represents an important modification to the concept phase of ISO 26262, since it transforms the item definition into a diagram that can also contains new information that was not mentioned in the item definition.

Despite all the mentioned advantages, The new method has some limitations. One of them is that it is time-consuming since the number of the safety constraints formulated at the end is huge especially if the system under study is complex. Another limitation is the ASIL classification that, to this date, only classifies E/E related hazardous events. The human behaviour and other influencing factors cannot be classified using the current ASIL. Furthermore, in this method, there is no proposed way to identify accidents and hazards and thus it is done in the same way as in STPA, that is using brain storming or field studies.

7.2 Future work

There are many possibilities for future work that can be used to extend the new method.

It is important to apply the new method on different automotive systems and conduct a full analysis to further compare its results with results of other methods.

The ASIL classification also needs to be upgraded in order to be able to classify hazards resulting from human errors or other influencing factors.

As possible improvements of the new method is identifying a systematic way to identify accidents and hazards. Also the form that should be used to formulate the causal scenarios doesn't yet exist, so it is part of a future work standardizing the formulation of causal scenarios and transforming the results of the new method into a formal specification.

It is also important to harmonize the terms. Terms like hazard needs to have a unified definition and both of the terms safety constraints and safety goals need to be unified as well.

Since the proposed method is time-consuming, it would be very helpful if some steps like the formulation of hazardous events are done automatically with the help of a tool specific to the new method.

The extended STPA is still being under development, and would be very interesting to add elements form the extended STPA to the new method and check its compliance with ISO 26262.

The functional safety concept wasn't discussed in this thesis due to its limit despite being part of the process diagram. So a work on how to derive the functional safety concept and how to transform the safety constraints into safety requirements that can be included in the functional safety concept.

One of the differences between STPA and HARA from ISO 26262 is that STPA can be used at all development stages of an item. This advantage is also an advantage of the new method since it contains the steps of STPA. So as a suggested future work, testing how the new method can be used not only at the concept phase of ISO 26262, but also in other parts of the standard like part 4 that discusses product development at the system level, part 5 and 6 that discuss respectively product development at hardware and software level.

Bibliography

[Abd17a] A. Abdulkhaleq. “A system-theoretic safety engineering approach for software-intensive systems.” PhD thesis. Institute for software technology, University of Stuttgart, 2017 (cit. on pp. 19–21, 43).

[Abd17b] A. Abdulkhaleq. *Using STPA in Compliance with ISO26262 for developing a safe architecture for fully automated vehicles*. https://speakerdeck.com/asimabdulkhaleq. 2017 (cit. on p. 19).

[AG] D. AG. “HARA’s Situation Catolog” (cit. on pp. 53, 58).

[AW13] A. Abdulkhaleq, S. Wagner. “Experiences with applying STPA to software-intensive systems in the automotive domain.” In: *2013 STAMP Workshop, MIT* (2013) (cit. on p. 43).

[AW14a] A. Abdulkhaleq, S. Wagner. “A software safety verification method based on system-thoretic process analysis.” In: *Computer safety, reliability, and security pp. 401-412* (2014) (cit. on pp. 43, 52–54).

[AW14b] A. Abdulkhaleq, S. Wagner. “A-STPA: Open tool support for system-theoretic process analysis.” In: *2014 STAMP conference at MIT*. 2014 (cit. on p. 43).

[AW15] A. Abdulkhaleq, S. Wagner. “XSTAMP: An extendable STAMP platform as tool support for safety engineering.” In: *2015 STAMP conference,MIT*. 2015 (cit. on p. 43).

[AwL+17] A. Abdulkhaleq, S. wagner, D. Lammering, H. Boehmert, P. Blueher. “Using STPA in compliance with ISO26262 for developing a safe architecture for fully automated vehicles.” In: *Automotive-safety and security conference Stuttgart,Germany* (2017) (cit. on pp. 19, 40, 43).

[AWL15] A. Abdulkhaleq, S. Wagner, N. Leveson. “A comprehensive safety engineering approach for software-intensive systems based on STPA.” In: *Procedia Engineering 128 (2015) 2-11* (2015) (cit. on pp. 15, 43).

[Gab14] N. Gabriel. *Item Definition Cruise Control*. 2014 (cit. on p. 52).

[Hom12] Q. V. E. Hommes. *Applying STPA to automotive adaptive cruise control*. STAMP Workshop presentation. MIT,USA. 2012 (cit. on p. 44).

[Hom15] Q. V. E. Hommes. *Safety analysis approaches for automotive electronic control systems*. 2015. URL: http://www.nhtsa.gov/DOT/NHTSA/NVS/Public%20Meetings/SAE/2015/2015SAE-Hommes-SafetyAnalysisApproaches.pdf (cit. on p. 44).

[Hoo17] A. van Hoorn. *Sichere und zuverlässige Softwaresysteme*. 2017 (cit. on p. 15).

[ILT+10] T. Ishimatsu, N. Leveson, J. Thoma, M. Katahira, Y. Miyamoto, H. Nakao. "Modeling and hazard analysis using STPA." In: *Proceedings of the 4th Conference of the international association for the advancement of space safety* (2010) (cit. on pp. 15, 44).

[KRR+16] S. S. Krauss, M. Reif, M. Rejzek, C. Senn, C. Hilbes. *STPA-Sicherheitsabalyse für Komplexe Systeme*. 2016 (cit. on pp. 19, 44).

[KTA+12] S. Kriso, C. Temple, B. Arends, P. Metz, B. Enser. *Executive summary functional safety in accordance with ISO26262*. 2012 (cit. on p. 44).

[Lev12] N. G. Leveson. "STPA: A new hazard analysis technique." In: *Engineering a safer world: Systems thinking applied to safety*. 2012 (cit. on pp. 15, 16, 19, 22–24, 38).

[MPA+16] A. Mallya, V. Pantelic, M. Adedjouma, M. Lawford, A. Wassyng. "Using STPA in an Iso 26262 compliant process." In: *Computer safety, reliability, and security pp 117-129* (2016) (cit. on pp. 19, 42, 43).

[Poh15] M. Pohl. *Methodenhandbuch für präventives E/E-und Software-Entwicklungs-Qualitätsmanagement und funktionssicherheit*. 2015 (cit. on p. 32).

[sta11] I. organization for standardization. *ISO 26262 Road vehicles-functional safety*. 2011 (cit. on pp. 15–17, 29–35, 38, 48, 65).

[Tho13] J. Thomas. *Systems theoretic process analysis (STPA) tutorial*. 2013 (cit. on pp. 19, 23–26, 28, 43).

[Wei13] M. Weiland. *Gefahre-und Risikoanalyse Fensterheber,elektrisch*. 2013 (cit. on p. 36).

All links were last followed on June 6, 2018.

Declaration

I hereby declare that the work presented in this thesis is entirely my own and that I did not use any other sources and references than the listed ones. I have marked all direct or indirect statements from other sources contained therein as quotations. Neither this work nor significant parts of it were part of another examination procedure. I have not published this work in whole or in part before. The electronic copy is consistent with all submitted copies.

---

place, date, signature