CHALMERS
UNIVERSITY OF TECHNOLOGY

Development of a Method to Evaluate Product Defects in Trucks

Creation of a method to simplify recall decision process of a defect that can lead to personal injuries

Master's thesis in Automotive Engineering

JULIA EUGENSSON

Department of Mechanics and Maritime Sciences
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2018

Master's thesis in Automotive Engineering 2018:11

Development of a Method to Evaluate Product Defects in Trucks

Creation of a method to simplify recall decision process of a defect that can lead to personal injuries

JULIA EUGENSSON

Department of Mechanics and Maritime Sciences
Division of Vehicle Safety
Chalmers University of Technology
Gothenburg, Sweden 2018

Development of a Method to Evaluate Product Defects in Trucks
Creation of a method to simplify recall decision process of a defect that can lead to personal injuries
JULIA EUGENSSON

Supervisor: Karsten Heinig, Volvo Trucks
Examiner: Astrid Linder, Department of Mechanics and Maritime Sciences

Master's Thesis 2018:11
Department of Mechanics and Maritime Sciences
Division of Vehicle Safety
Chalmers University of Technology
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: Volvo FH on road [1].

Typeset in LaTeX
Gothenburg, Sweden 2018

Development of a Method to Evaluate Product Defects in Trucks
Creation of a method to simplify recall decision process of a defect that can lead to personal injuries
Master's thesis in Automotive Engineering
JULIA EUGENSSON
Department of Mechanics and Maritime Sciences
Division of Vehicle Safety
Chalmers University of Technology

Abstract

The number of vehicle recalls due to product defects has increased during the last years. A large number of recalls is expensive for a company, both by direct costs as well as damaged reputation. If a defect of a part is detected, an analysis is performed to investigate if the defect can cause personal injuries, as well as how likely it is for the defect to occur. The objective of this thesis was to create a general method to evaluate defects that potentially can cause harm, as well as rate them regarding severity in order to support the recall process.

The method is based on different types of existing hazard analyses. The hazard analyses most used are FMEA and ISO 26262, where it is found that each defect should be evaluated with regards to severity, probability of exposure and controllability. Severity rating tables are created by studying data from STRADA, injuries in maintenance and efficiency of safety systems, among other things. Probability of exposure rating tables are created by studying, for example, usage specifications of sold trucks and Swedish road data, as well as maintenance routines and usage of safety systems. The controllability rating tables are created by studying similar evaluations in ISO 26262 and the occurrence of the possible defects. All hazardous scenarios (i.e. all possible harmful situations that can take place if a defect occurs) are identified by studying internal defect data as well as external recall data. Possible crash scenarios resulting from the hazardous scenarios are found, and the corresponding rating for severity, exposure and controllability is identified for each scenario. The ratings are combined into an ASIL rating, which clarifies if the defect is safety related (i.e. can cause any personal injuries), as well as a rating how severe the defect is. The highest ASIL is identified for each hazardous scenario and occurrence, and these are gathered in tables sorted depending on the effect for the customer.

When using the method, the analyst has to identify the hazardous scenario the defect can result in and the occurrence of the defect (e.g. sudden, previous notice). After this, the worst case ASIL is found from the applicable table. If the current hazardous scenario does not exist, the case have to be analyzed using the tables for severity, probability of exposure and controllability. In conclusion, the method simplifies the evaluation of the severity of a defect, and creates a rating which can be used to support the recall decision. However, the method has to be verified further on new potential safety hazardous cases, as well as on different analysis engineers to ensure repeatability.

Keywords: product safety, product defects, vehicle safety, trucks, hazard analysis, recall, ASIL, FMEA, ISO 26262.

Acknowledgements

First of all, I would like to express my gratitude to my supervisor Karsten Heinig at Volvo Trucks for introducing me to the subject of the thesis, as well as for supporting me with both knowledge and ideas throughout the project. I would also like to thank my examiner Astrid Linder for all help and remarks throughout this project.

Furthermore, I would like to thank András Bálint for his supporting with STRADA, and Mats Svensson for knowledge and support in vehicle safety.

I would also like to thank all of my colleagues at Volvo Trucks, who always have made me feel welcome and have helped me whenever I have had any questions.

Lastly, I would like to thank my family and partner for supporting me through this project by proofreading, giving input and listening to ideas, as well as with moral support.

Julia Eugensson, Gothenburg, April 2018

Contents

List of Figures

List of Tables

List of Acronyms

AAAM	Association for the Advancement of Automotive Medicine
ACC	Adaptive Cruise Control
AEBS	Autonomous Emergency Braking System
ASIL	Automotive Safety Integrity Level
CSE	Customer Safety Effect
CO	Carbon Monoxide
DAS	Driver Alert Support
DVSA	Driver and Vehicle Standards Agency
E/E	Electrical/Electronic
ESC	Electronic Stability Control
FAA	Federal Aviation Administration
FARS	Fatality Analysis Reporting System
FCW	Forward Collision Warning
FMEA	Failure Mode and Effects Analysis
FMVSS	Federal Motor Vehicle Safety Standards
FTA	Fault-Tree Analysis
GPSD	General Product Safety Directive
GTA	Global Transport Application
GTT	Group Trucks Technology
HA	Hazard Analysis
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
LCS	Lane Changing Support
LKS	Lane Keeping Support
MLIT	Ministry of Land, Infrastructure, Transport and Tourism
MVR	Motor Vehicle Repair
NASA	National Aeronautics and Space Administration
NHTSA	National Highway Traffic Safety Administration
NRC	Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
PSC	Product Safety Committee
RSC	Roll Stability Control
RPN	Risk Priority Number
SAE	Society for Automotive Engineers
STRADA	Swedish Traffic Accident Data Acquisition
VRU	Vulnerable Road User
YSC	Yaw Stability Control

1

Introduction

1.1 Background

Product failure can occur in all products and at any time. However, the result of a failure can vary vastly depending on the problem and product. A large defect in for example a nuclear plant or an airplane can result in the loss of many lives, when a defect in many smaller products usually mainly results in loss of function of the product.

In the development phase of any product, a risk assessment has to be performed to ensure that the product will not fail and cause harm to the user or any other person or property. The extent of this assessment varies with product and part, depending on the potential risk a failure may cause. Even if the objective of the assessment is to be as comprehensive as possible, product defects will occur. When a defect is detected, it is important for the concerned manufacturer to make a decision on how to proceed with the problem. If the problem is considered severe, the product will be recalled and corrected or exchanged. The assessment process to determine if a product defect can cause injuries (i.e. is safety related) is not standardized within Volvo Group. The assessment is mainly based on the judgment of the different analysts, whom are spread worldwide throughout the organization. This creates a large processing time for each case, which is not a sufficient allocation of resources.

According to a study by National Highway Traffic Safety Administration (NHTSA), in 94% of all accidents the driver is the critical reason for the pre-crash event (note that this not necessary is equal to the cause of the crash). The corresponding number for the vehicle is 2%, and the environment 2% [2]. However, the number of human errors are likely to be reduced with the increasing share of active safety systems and automation in vehicles [3]–[5]. The number of product defect related accidents are today increasing rather than decreasing, which will result in an increase in the share of product defect related accidents compared to all accidents. This is shown in Figure 1.1, which illustrates prognosis of human and product related accidents. Left figure shows absolute number of accidents over time, and right figure shows the share of accidents over time. A higher share of product caused accidents in comparison to accidents caused by humans might gives an impression of unsafe products, which is not in line with the goal of *Zero accidents with the Volvo Group products* [6].

The number of potentially safety related issues have in the last few years increased significantly for many manufacturers, which naturally leads to more decisions regarding potential actions. An objectivity of these decisions, as well as a shortening of the handling time of each case could be ensured with a method applicable to all issues, markets and products. An additional problem with the current decision process is that it does not include a way to visualize the severity of

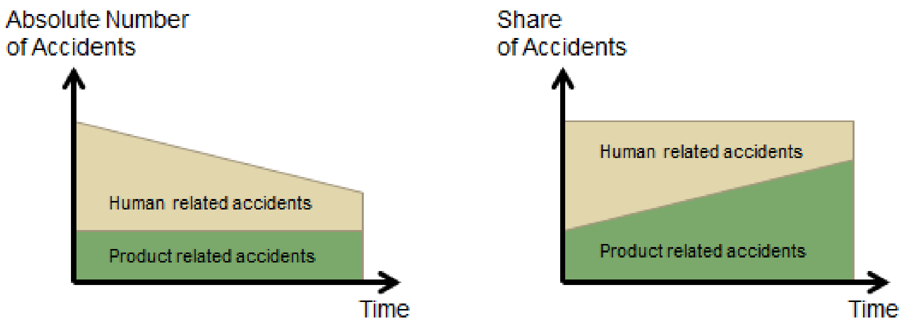


Figure 1.1: Illustration of number vs. share of product related accidents. Illustration from Volvo Group.

the defect, which may lead to inefficient allocation of resources. In risk assessment methods (for example FMEA and ISO 26262), the potential problems are usually graded, which enables the appropriate preventative work for each defect. This could be used for potential product safety defects to be of help in the decision process. It creates an opportunity to easily compare different cases.

1.2 Problem statement

Due to the diversity of engineering sites and as a consequence of different traditions and markets, different approaches to evaluate potential safety related issues are used today within the Volvo Group.

The approach to grade effects of potential safety related issues is today not fully harmonized. A method including both evaluation and rating would enable quantification of the assessments, and can be used to support the decision of a potential recall.

1.3 Objective

The objective is to develop a general and comprehensive method to evaluate and rate potential hazardous product defects for Volvo Trucks. The method should enable an objectivity to each decision and be easy to use.

1.4 Scope

The method should be applicable to all product safety related defects throughout the Volvo Trucks fleet. However, the methodology should to a great extent also be applicable to the other Volvo Group truck brands.

The method should be created with regards to the Swedish market, but it should also be possible to easily extend to other markets.

The method should be able to be used for any analysis engineer with knowledge of the recall decision process and the products of Volvo Trucks.

2

Theory

This report covers several areas of research, as well as many data sources. This theory chapter is therefore quite comprehensive, to ensure that the reader has sufficient information to understand the results and conclusions drawn. The chapter starts with presenting information regarding product safety and legislation, both in the automotive industry in general and Volvo Group specifically. The next section will present the different data sources used. Lastly, different methods for hazard analysis will be presented, which includes methods already used within Volvo, but also methods used within other industries.

2.1 Product safety

The number of recalls and the incidents due to a part which has been recalled within the automotive industry has increased largely during the last years, which can be seen in Figure 2.1. The impact of these recalls is devastating to the affected companies, both regarding direct costs and reduction in consumer satisfaction. This has made product safety and liability a growing focus area in many companies. The increased number of recalls is not mainly a result of less safe products, but rather stricter legal requirements and a higher degree of complexity in the vehicles. At the same time, both safety and quality is rated as two of the most relevant factors for a customer in the vehicle selection process [7].

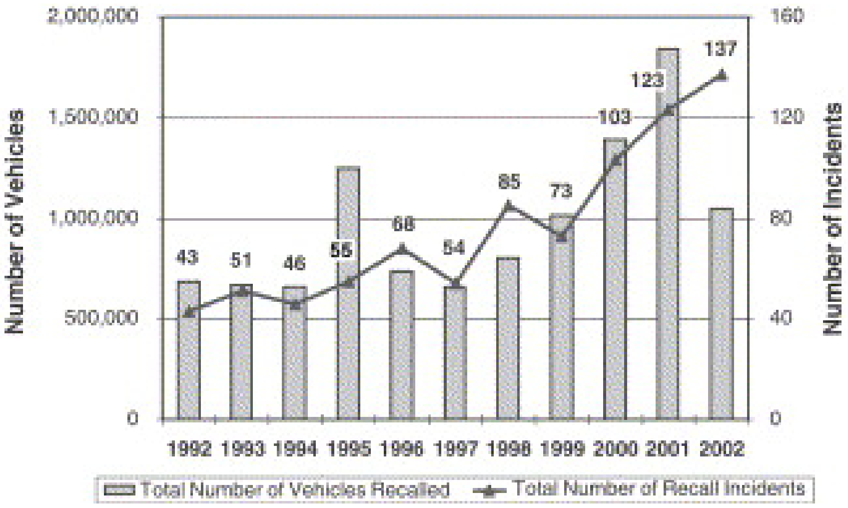


Figure 2.1: Number of recalls and number of recall incidents in the UK between 1992-2002 [8].

Product safety according to Volvo Group means *"producing a product that is not likely to cause* *personal injury within its intended purpose and any reasonably foreseeable misuse."* A safe product should not contain any safety related defects, it should comply with applicable legislation and safety standards and be safe to use during its normal life cycle. Traffic safety, on the other hand, is according to Volvo Group reducing the risk for traffic accidents, as well as minimizing the consequences for all road users.

The work regarding product safety is in Volvo Group enforced in two different phases of the product life; the project and the maintenance phase. Product safety in projects investigates if there are potential safety related risks, i.e. events which could lead to injuries for the customer, and how to avoid them. Product safety in maintenance, on the other hand, reviews if there is a safety related defect, which is an already occurred event, that can lead to an injury. Further in this report, only product safety in maintenance will be investigated.

2.1.1 Potential actions for product defects

There are several methods to determine if an issue is a safety related defect, and if so, how to reduce the risk of injuries. This section will describe the process used within Volvo Group.

When an issue or a risk is reported from the market or detected within the Volvo Group, the need for further investigation is reviewed. If it was decided that no further investigation is needed, the case is closed. If an investigation on the other hand is needed, the relevant truck brand or product safety process working group proceeds with the investigation. The investigation includes collection of all relevant facts which will allow to judge the root cause, severity and probability (as number of issues on the entire affected fleet) of an issue. The documentation can also include possible solutions for production if relevant. The decision of the defect is safety related is based on this information. When the decision of safety related or not is made, it is registered to serve as evidence for later use, as well as a reference for further improvement of product safety knowledge. If the issue was determined to be safety related, an internal campaign, technical service bulletin, recall or service campaign has to be issued to all markets where the concerned products are present. An internal campaign is issued if the product has not reached the customers, which includes everything from project phase until the vehicle leaves the factory. A technical service bulletin is information from the manufacturers to the dealers used to prevent issues or clarify uncertainties. A service campaign is not mandatory and not issued due to a safety defect but most commonly a non-compliance with safety regulations. The affected vehicles will be updated, changed or repaired free of charge at the next service. A recall can be voluntary from the manufacturer or federally mandated when a safety issue is detected. Depending on the severity of the defect covered by the recall, the urgency for the customer for the customer to get the vehicle repaired varies. The decision of which action that should be issued depends on the defect and the local processes required by law.

Recalls are costly, both in direct costs of for example repairs and liability, as well as indirect costs of damaged reputation. Therefore, most companies are reluctant to issuing recalls too early, before a thorough investigation has been performed. If a product recall on the other hand is stalled, the company may suffer from much higher costs due to fines, liability damages and damaged reputation. Therefore, it is of great importance that a correct decision is made as soon as possible after the affected company has received the information regarding the defect. The importance of a fast decision increases with the severity of the defect [9].

2.1.2 Legal requirements

2.1.2.1 Vehicle safety legislation

All industrialized countries have various legislations regarding vehicle safety to prevent and reduce accidents. However, these legislations vary greatly from country to country. Since Volvo Group's products are used in all parts of the world, it is important to ensure that all safety related regulations are fulfilled. In the US, National Highway Traffic Safety Administration (NHTSA) issues the Federal Motor Vehicle Safety Standards (FMVSS) to regulations as directed by the laws adopted by the US Congress [10]. In the EU, on the other hand, the European Commission regulates the legislation and policies, according to the General Safety Regulation (EC) No 661/2009 and other relevant policies [11]. The governments are constantly monitoring the compliance of vehicles to the legal requirements. Failure to comply may lead to a non-compliance recall.

2.1.2.2 Recall legislation

More than 299 million vehicles have been recalled since 1966. A recall is usually found and initiated by the manufacturer, but can also be demanded by the government in a specific country. In the US, for example, the federal government in the form of the National Highway Safety Administration (NHTSA) monitors the number of cases of product failures and injuries or fatalities by police reports, customer reports or other reporting systems [12]. If NHTSA finds a significant number of cases for the same vehicle model appearing to be linked to the same type of problem it may initiate a defect investigation. If this shows a significant trend linked to the same fault this may lead to a safety recall. A government recall could be either voluntary, influenced or ordered. The capture rate (the required number vehicles that have to be repaired) is higher for an ordered recall than for a voluntary recall. The recall is done without any cost to the customer, but the option for the manufacturer is to: repair, replace or refund the recalled products [13]. In addition, if the vehicle defect has caused an injury, a law suit may be filed in a court of law. This may lead to high cost to the damage that the manufacturer has to pay to the plaintiff. For some cases, a so called *Classaction law suit* may be filed on behalf of a number of plaintiffs claiming to be subjected to their cars causing expenses or injuries. Classaction law suits are normally very costly. Vehicle recall information is usually collected and announced by a governmental agency to give the consumers an overview of the market. For example: in the US, the recall statistics is governed by NHTSA, in the UK it is collected by the Driver and Vehicle Standards Agency (DVSA) and in Japan it is gathered by the Ministry of Land, Infrastructure, Transport and Tourism (MLIT).

2.1.3 Customer Safety Effects - CSE

If a failure of a certain part or function potentially can lead to a Customer Safety Effect (CSE), the part or function is marked as potentially safety related. The CSEs are defined within Volvo Group by studying data from previous recalls and accidents. The effects are divided in to the following categories:

- Vehicle stability and trajectory.

- Thermal event.
- Integrity of the vehicle.
- Braking of the vehicle.
- Start and operation of the vehicle.
- Effects on the driver, passenger and maintenance personnel.
- Safety features.

All categories described have subcategories, and all potential safety related product defects within the company are sorted in to one of these. A figure showing the subcategories is found in Appendix A.1.

2.2 Data collection

Product failures can occur during normal driving, as well as in maintenance/service, at standstill and in a crash. To analyze the potential defects in all situations, injury data from different data sources is required. This data will be presented in this section. Furthermore, data regarding usage will also be presented in this section.

2.2.1 Injury statistics during driving from STRADA

Swedish Traffic Accident Data Acquisition (STRADA) is an information system for injuries that have occurred within the transport sector in Sweden. STRADA was implemented 1996 and contains information from both police and hospitals. It contains geographic location, severity, age and sex of the injured, what traffic rules applicable at the scene, type of vehicle etc. The objective of STRADA is to provide data to traffic safety related work on a local as well as a national level. It is an initiative to improve traffic safety and an important part of the *Vision Zero* initiative, which was adopted in 1997 and strives towards no loss of lives in traffic in Sweden [14]. STRADA is mainly used by researchers, insurance companies and traffic safety organizations, even though anyone can access the data [15]. There are several global initiatives for collecting accident data, such as CARE (within EU) and International Traffic Safety Data and Analysis Group, but none are as comprehensive and easily accessible as STRADA.

The information in the STRADA database is divided into two parts: one part with data recorded by the police, and one part with data from hospitals. The two different parts contain different information, and can be connected to each other through different identification numbers (however all information is completely anonymous). Within this report, only the part recorded by the police will be used. The connection between the two databases in STRADA can be found in Appendix C.1.

The injury level from the police report is defined in a scale from 1 to 4 and 9, defined as:

- 1 = Death

- 2 = Severe injuries
- 3 = Mild injuries
- 4 = No injuries
- 9 = Unknown

The accidents are divided into different categories depending on the accident scenario. The categories applicable to this report will be described further in Section 2.2.1.1.

2.2.1.1 Collision types

A large number of trucks occupy the roads and many of them have a high mileage, which also results in trucks being a part of many crashes each year. If the driving distance of different categories of vehicles are considered, accidents with heavy vehicles kill five times as many passenger car occupants as do accidents with passenger cars per kilometer driven [16]. The categorizing of crash types during driving in this report is the one found in STRADA, with the addition of jackknifing. The accident scenarios used are the following, where the information in the parentheses represents the category in STRADA:

- Single vehicle crashes: driving off straight road (S 1, 3) and driving off road while turning (S 2, 4).
- Crash with bicycle (C).
- Crash with vehicle about to turn off the road (A).
- Accident with pedestrian (F).
- Meeting accident/head on collision (M).
- Crash while overtaking (O).
- Crash in crossing (K).
- Rear ending intersection (U).
- Accident with wild animal (W) or other animal (V1).
- Crash with parked vehicle (V5).
- Crash during reversing (V6).
- Crash with tram (J5).
- Crash with train (J8).
- Jackknifing.

A detailed description of each category is found in Appendix C.2.

2.2.2 Injury data for cases in crash, maintenance or in service

There is no database collecting all data regarding injury in maintenance and service, and the information regarding benefits of safety systems, features and restraints during a crash is still limited. Additionally, only cases in maintenance/service causing severe injuries or fatalities are being reported. A fall not leading to any injuries will for example not lead to a report, why this statistics is harder to analyze since it only contains severe cases. Furthermore, since the information and studies regarding these subjects are limited, data from different countries and studies have to be combined to include all different injury risks. However, it is assumed that the maintenance and service is similar in the different countries. Data regarding different hazard risks involving trucks not during driving will be presented in this section. The statistics used in this section is gathered in Appendix C.3.

2.2.2.1 Vehicle fires

A fire is regardless of the product considered a very severe hazard due to the possible consequences. A fire in a vehicle can be a risk for the occupants, as well as for the surrounding road users and maintenance personnel. Historically, there have been several vehicle fires that have caused a large number of fatalities, for example the fire of a Volvo Truck in the Mont Blanc tunnel in 1999. The fire resulted in 35 deaths [17].

Automotive fires are among the largest cases of fire deaths in the United States. Less than 10% of the automotive fires are caused by a collision, but the escape from the vehicle after a crash is usually very difficult. The result of this is that 60% to 75% of the vehicle fire fatalities occur after a collision [18]. A report by Viklund et al. concludes that fires accounted for 5% of the car fatalities between the years 1998 to 2008. Only a third of these victims had a fire related cause of death with no fatal trauma injuries. However, fire is considered as a deadly post-crash problem [19]. Vehicle fire is also a large problem in maintenance. Around 10% of fatal injuries in Motor Vehicle Repair (MVR) are due to fire or explosion [20].

2.2.2.2 Hot and cold burns

Overheating or leakage of hot fluids can create injuries for driver, maintenance personnel or third party. The most likely injuries will be superficial skin burns. However, if there is a large leakage of hot fluid, the burns can be much more severe. According to a study by O'Mara et al., burns associated with motor vehicles have accounted for 10% of all burn admissions in United States, although very few of these resulted in fatalities. Most of these injuries occurred from regular use and maintenance of the vehicle, and the most common burn injuries are from radiators and carburetors [21]. A study reviewing injury data from automotive repair workshops in Spain has concluded that 2% of the reported injuries are related to burns, scalding and freezing [22]. However, burns can also be caused by fire. To create a cold burn, the temperature has to be very low, and this is an uncommon reason for injuries related to vehicles.

2.2.2.3 Leakage of fluids

If large amounts of fluids are leaked on to the road, it can create a slippery surface which can result in hazardous situations for other road users. Especially large leakages of oil can cause severe accidents, as in a four vehicle fatal accident in Australia in 2017 [23].

If exposed to, several of the fluids used in a vehicle, for example coolant and windshield washer fluid, can be very hazardous. Inhalation or swallowing of many of the fluids can lead to severe injuries or even death, and some of the fluids can be very irritating for the skin and the eyes. A leakage of fluids in maintenance can therefore result in injuries for the maintenance personnel. According to Health and Safety Executive Britain, 6% of fatalities in motor vehicle repair are caused by contact with harmful substance [20].

2.2.2.4 Vehicle rolling away from standstill in maintenance

According to a study by Safe Work Australia, between the years 2003-2012 approximately 40 people have been killed in Australia during repair or maintenance due to a truck unintentionally moving. The same study concludes that 44 persons have been killed due to being hit by a moving vehicle during loading/unloading. The reason for a truck moving is usually the driver/worker failed to apply brakes correctly before exciting the vehicle [24].

2.2.2.5 Fall from the vehicle

Work-related fall injuries have according to a study by Office of Industrial Relations in Queensland, Australia, resulted in 3100 serious injuries in Australia during the period 2009 to 2011. The same study shows that 14.4% of these accidents are caused by poorly designed ladders or steps, and 8% due to ladders or steps unsafely located on the trailer. The other accidents were found to be due to risk taking behaviour such as climbing at height or jumping down from trailer. A poor design can consist of parts braking or falling off, being badly placed or being slippery [25]. Even a fall from a seemingly low height (1 to 2 meters) has shown to be fatal if it involves a head injury [24].

2.2.2.6 Asphyxiation or intoxication

Historically, asphyxiation from vehicle exhaust gases has been a common method for committing suicide. Exhaust gases from older vehicles usually causes carbon monoxide asphyxiation. Old gasoline engines can produce as much as 7% carbon monoxide (CO) of the total exhaust gas, which can result in lethal concentrations of CO in a small garage within 15-30 minutes. However, the catalytic converters in modern vehicles are reported to reduce more than 99% of the concentration of carbon monoxide [26]. It is also found that diesel engines produces much less CO than gasoline or propane engines [27]. Among newer vehicles, it is more likely with asphyxia caused by carbon dioxide intoxication in combination with reduced concentration of oxygen if a person is exposed to exhaust gases [28].

Even a low concentration of carbon monoxide in the air, 0.001%, for several hours of exposure can cause death. CO remains attached to the hemoglobin for a long time which leads to accumulation even with small amounts. This reduces the bloods oxygen-carrying capacity. It can also cause headaches, drowsiness and blurred vision [29].

Both carbon monoxide and dioxide are in themselves odorless and colorless and it is therefore hard to notice if they are present. Exhaust gases do however have an odor from other components of the gas which usually should be, but cannot be guaranteed, noticed if leaked into the cab. Two other major components of exhaust gas is usually particulate matter and nitrogen. Both of these can cause long time problems, the first can cause inflammation and worsening of heart and lung diseases, and the second may aggravate respiratory infections [29].

Asphyxiation is also a problem within maintenance and repair of trucks. In Britain, around 3% of all fatal accidents in motor vehicle repair is caused by asphyxiation [20].

2.2.2.7 Electric shock

Almost every part of the human body can be injured by an electric current. The extent of the injury to any tissue will depend on many factors, for example the nature of the tissue and the duration and the amount of the electric current. The electric current can create burns by the heating of tissue, and nervous tissue has the least resistance to current flow and is therefore easily damaged [30]. Evidence from a study by Lee et al. suggests that many instances of electrical trauma is of sufficient magnitude to cause electrical breakdown of cell membranes and cell lysis. Large cells as muscle and nerve cells are in theory very vulnerable to electric breakdown [31]. Non-thermal electrical breakdown mechanisms of cell damage is most important if the contact point is brief, and heat damage is dominant if longer contact point [32].

2.2.2.8 Safety systems

The purpose of the airbag is to protect the occupants of the vehicle in case of a crash. To provide this protection, the airbag must inflate in the time between detecting the crash and the occupant beginning to move forward towards the interior of the vehicle in response to the forces induced by the crash. This time gap is very limited, which makes it necessary for the airbag to move rapidly towards the occupant with maximum speeds of around 240 km/h. The airbag is most efficient if it is fully inflated before first contact. If the occupant on the other hand is in the space where the airbag inflates, the occupant will be struck in speeds up to 240 km/h, in comparison to hitting the interior of the vehicle in speeds which could be as low as 16 km/h. The impact of an inflating airbag can therefore cause very severe injuries or even death [33]. According to NHTSA, as of June 2003, there had been 231 death in the US by airbag in collisions which otherwise would not have been fatal. The same study does however show that in 50% of these cases, the occupant was unbelted [33]. The efficiency of airbags in trucks has not been verified. However, in cars the effectiveness of the airbag alone in reducing fatalities is according to Mallaris et al. found to be 25.4%, while the same value in combination with belt is 56.2%, while efficiency of belt alone is 48.5%. The same study concludes that usage of airbag and belt reduces brain, spinal cord, facial, an abdominal injuries at the expense of minor skin and flesh wounds [34]. Several studies show that airbags are very efficient in reducing injury level in severe frontal collisions, but there is a risk that the airbag in low speed collisions can cause light injuries [35], [36].

The Electronic Stability Control (ESC) system is a combination of Yaw Stability Control (YSC), which counteracts instability in the yaw plane, and Roll Stability Control (RSC), which reduces the vehicle speed when vehicle is in risk of roll-over due to high lateral acceleration. Crash statistics for cars has shown that ESC prevents around 40% of control-loss crashes for cars. The statistics regarding ESC efficiency in crash reduction in trucks is still limited [37]. Another study by Lie et al. shows an overall positive effect of ESC in circumstances where the road has low friction. The effectiveness of ESC ranges from 13% for car occupants in crashes of all types with serious or fatal outcome, to an effectiveness of minimum 35% for single, oncoming or overtaking crashes with serious or fatal outcome on wet or icy road surface. In the same study, it was estimated that 80-100 of vehicle related deaths (out of a total of 500) could annually be saved in Sweden if all cars were equipped with ESC [38]. A study by Framer et al. based on all fatal crashes in the United States over 3 years concludes that ESC reduced the single-vehicle fatal crash involvement risk by 56%, or an estimated 34% reduction in overall fatal crash involvement risk [39]. In conclusion, it has been shown that ESC reduces the risk of driver loosing control of the vehicle and has possibly reduced the number of collisions.

2.2.2.9 Safety features

The number of safety features on the market for trucks are today limited. Volvo Trucks offers: Adaptive Cruise Control (ACC), a system that control longitudinal acceleration of the vehicle, Autonomous Emergency Braking System (AEBS), which brakes in emergency situations, Forward Collision Warning (FCW), which warns the driver if there is a risk of a forward collision, Lane Keeping Support (LKS), that warns when driver drifts out of lane, Lane Changing Support (LCS), which warns when driver initiates a lane changing with a vehicle in the blind spot, and finally Driver Alert Support (DAS), that warns if driver shows indications of for example drowsiness.

The ACC controls the longitudinal acceleration ad speed of the vehicle, with supervision from the driver. ACC in combination with FCW has shown to reduce the number of rear ending accidents with 10% [40]. However, studies have also shown an adaptive behaviour of the driver when using the ACC with higher mean speed and smaller headway, and a sudden failure can result in a rear ending collision [41]. It the ACC fails, it is, according to the product handbook, the drivers' responsibility to take over the control of the speed.

AEBS is a safety feature intended to reduce the number and the severity of rear ending collisions. According to a study by Isaksson-Hellman et al. investigating the real world efficiency of Volvo Cars emergency braking system called City Safety, the number of insurance claims for rear ending collisions was reduced by 28% [42]. This indicates that the system has lowered the number of rear ending collisions significantly. Despite this, failures in the AEBS are usually classified as a quality issue since it only is defined as a support system. However, if the vehicle in the future is autonomous, a system not braking would be seen as a very serious safety defect.

The systems LKS, LCS and DAS are warning systems which does not control lateral nor longitudinal movement of the vehicle. It is also stated in the truck handbook that the systems are *Support* systems, and that the driver should be in full control of the vehicle. There are, however, internal regulations on how many false positives are allowed during the lifetime of a truck and if these not are fulfilled, the problem is classified as a quality issue.

2.2.2.10 Restraint systems

The seat belt has a critical role in a collision. It is vital for reducing the level of injuries both in low and high speeds and studies have shown that is reduces fatalities by 45% for car occupants, 60% for occupants of light trucks an 30% for truck occupants [43], [44]. A failure of the seat belt is a very severe safety problem for heavy truck occupants in a crash and can result in ejection through the windscreen or impact against the interior [44]. An ejection of the occupant increases the risk of severe injuries and fatality significantly. In a roll-over situation, a study by Latifi et al. has found that persons ejected from the vehicle has a mortality rate of 25%, compared to 7% for persons not ejected [45].

Ejection of occupants from the vehicle is much more common for unbelted occupants than for belted occupants. According to data from the Fatality Analysis Reporting System (FARS) database from 1982 to 1996, approximately 2.5% of all fatal crashes includes a belted occupant that has been ejected. For unbelted occupants, on the other hand, the same number is approximately 29.4% [46].

A malfunction of the seat belt can also cause injuries due to too harsh tension or locking of the belt. Injuries from seat belt can consist of skeletal, soft-tissue and visceral injuries. Classic seat belt injury signs are skin abrasions to the neck, chest and abdomen. If these are present, internal injuries are present in 30% of the cases [47]. These injuries can occur even if the belt is placed properly due to the often very high forces in a collision situation. If the belt for some reason is misplaced so that wrong parts of the upper body is loaded (for example abdomen or neck), very severe injuries can occur.

The seat is the principal component of the occupant restraint system in a rear end collision. However, the seat also plays a fundamental role in restraining the occupants in roll overs, frontal and side collisions [48]. If the back of the seat fails when the rear of the vehicle is hit, there is a high risk of the occupant obtaining severe neck injuries, even in speeds below 20 km/h. However, the injury level in a low speed rear end collision between two cars is usually minor [49]. Another function of the seat is to ensure the position of the occupant in case of a collision. If the seat is out of place, the seat belt and airbag may not be able to properly protect the occupant, and might even risk hurting the occupant due to faulty contact points. In high speed collisions, there is a risk of the occupant being ejected from the vehicle if not properly restrained.

There are several parts in the vehicle that are vital for ensuring adequate survival space of the occupants during a crash. A failure of one or more of these parts can lead to unnecessary occupant injuries due to intrusion in the survival space.

The under-run protection can change the outcome of of many crash situations, including: head on collision, truck into side of car, side swipe crashes in opposing directions and rear end collisions. If there is a failure of the under-run protection system, the outcome of a possible crash might be much more severe than if the system works as intended [50].

2.2.3 Usage statistics

Volvo Group trucks are used worldwide and for many different purposes. This results in several different possible environments in which a truck can be used. Some trucks work in mining with a lot of hill driving, while other are used as garbage trucks with many start and stops. Some are used in very low temperatures, other in very high. The usage of a truck will affect which parts are most likely to fail. Therefore, there are several parameters which can be adjusted to fit the missions of the specific truck. In Volvo Group, Global Transport Application (GTA) defines these parameters. The parameters include for example Road Condition, Topography, Operating Cycle and Dirt Concentration. The most important parameters for this study are described in Appendix D.2.

The road statistics for Swedish roads is provided by Trafikverket, where the kilometers of roads with for example crash barriers or a certain speed limits can be found.

2.3 Methods for risk analysis

Risk includes both undesirable consequences and likelihood, e.g. number of people harmed and the probability of occurrence of this harm [51]. Risk analysis is the process of identifying and avoiding or reducing a risk. The more complex the system, the higher the need for a risk analysis [52]. There are several different methodologies for assessing risk, where some are developed for a certain sector of products and some are general and therefore applicable to many different products. This section will present some of the most common methods for risk assessment liked to the means of transportation.

2.3.1 Hazard Analysis - HA

Hazard Analysis (HA) is by its own not a complete risk assessment method, but a risk cannot be determined if the hazard is not understood. Therefore, HA is an important part of all risk analysis methods, even if it might not be mentioned as a separate part of the methodology. According to Ericson *"Hazard analysis is the basic key component of the system safety process"* [53]. HA is performed to identify hazards by systematically examine systems or products with consideration to surrounding factors. Hazards can be recognized by focusing on undesired outcomes or by studying known hazard-triggering mechanisms. Hazards can also be found by for example use of previous knowledge and lessons learned, or by the use of key state questions. Example of these questions can be [53]:

- Fails to operate.
- Operates incorrectly.
- Operates inadvertently.
- Operates at wrong time.
- Unable to stop operation.
- Receives erroneous data.
- Sends erroneous data.
- Conflicting data or information.

- The component is exposed to fluid/heat from external source.

The HA can be used in combination with most of the methods in this chapter to determine for example consequences and the probability of the hazard.

2.3.2 Failure Mode and Effects Analysis - FMEA

Engineers have always performed risk analyses on products and processes. The Failure Mode and Effects Analysis (FMEA) was created in 1949 by the US Armed Forces. However, FMEA first became widely spread during the 1960s. Ford Motor Company introduced FMEA in the automotive industry in the late 1970s, where it was used for safety and regulatory consideration as well as to improve production and design. The FMEA method is today used in for example semiconductor processing, food service, in the aeronautics and in the automotive industries [54].

FMEA is an analytic methodology used for recognition and evaluation of potential failures of a product or process. It is used to ensure that all potential problems have been considered through the development process. Many components and subsystems have to be reviewed to identify failure modes and the possible effects. An FMEA is also used to identify actions to prevent a potential problem from occurring [55]. According to SAE J1739, an FMEA *"is meant to be a "before-the-event" action, not an "after-the-fact" exercise"* to produce the greatest value achievable [56].

There are several purposes of performing an FMEA, for example:

- Improve product quality, reliability and safety.
- Reduce product redevelopment timing and cost.
- Document actions taken to reduce risk.
- Visualize what problems should be prioritized for corrective actions.

Different FMEAs are used during different stages in the development of a product or process. Example of FMEAs are: Concept FMEA, Design FMEA and Process FMEA, where each type of FMEA is slightly different. This section will hereafter mainly focus on Design FMEA and is based on the FMEA handbook version 4.1 if nothing else is stated [55].

The process of producing an FMEA can be divided in to three steps, which together result in a complete risk analysis with a ranking that indicates an order of prioritization for the problems.

2.3.2.1 Step 1

The first part of producing an FMEA includes the following steps:

- Identify all functions.
- Identify how each function can fail (failure mode).

- Identify a group of associated effects for each failure mode.
- Identify a severity rating for each effect group that prioritizes the failure mode.
- If possible, recommend actions to eliminate failure mode without addressing ”causes”.

A potential failure mode is according to SAE J1739 defined as *”the manner in which a component, subsystem, or system could potentially fail to meet or deliver the intended function described in the item/function column”* [56]. The failure modes can be sorted into four categories:

1. No Function: System totally non-functional/inoperative.
2. Partial/Over Function/Degraded Over Time: Degraded performance, meets some but not all requirements.
3. Intermittent Function: Complies but loses functionality or becomes inoperative.
4. Unintended Function: Interaction of several elements whose independent performance is correct adversely affects the product or process, for example unrequested operation or operation in an unintended direction.

The severity classification is associated with the most severe consequence from the failure modes. It is a relative ranking, and the ranking index can be affected only through a change in design. The severity ranking is denoted S, and the scale can be either 1-5 or 1-10 depending on company regulations. Figure 2.2 shows an example of a Design Severity Rating Table.

Effect	*Criteria: Severity of Effect*	*Ranking*
Hazardous without warning	*Very high Severity ranking when a potential Failure Mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.*	*10*
Hazardous with warning	*Very high Severity ranking when a potential Failure Mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.*	*9*
Very high	*Vehicle/item inoperable (loss of primary function).*	*8*
High	*Vehicle/item operable but at a reduced level of performance. Customer very dissatisfied.*	*7*
Moderate	*Vehicle/item operable but comfort/convenience item(s) inoperable. Customer dissatisfied.*	*6*
Low	*Vehicle/item operable but comfort/convenience item(s) operable at a reduced level of performance. Customer somewhat dissatisfied.*	*5*
Very low	*Fit and finish/squeak and rattle item does not conform. Defect noticed by most customers (greater than 75%).*	*4*
Minor	*Fit and finish/squeak and rattle item does not conform. Defect noticed by 50 percent of customers.*	*3*
Very minor	*Fit and finish/squeak and rattle item does not conform. Defect noticed by discriminating customers (less than 25 percent).*	*2*
None	*No discernible effect.*	*1*

Figure 2.2: Ford FMEA design severity rating table.

The severity rating is used to emphasize the high priority failure modes.

2.3.2.2 Step 2

In step 2, the following point should be addressed:

- Find the associated cause.
- Identify the estimated occurrence rating(s).
- Recommend actions for high severity and criticality.

The causes and its failure mode is assumed to have a one-to-one correlation, and the causes are found through a brainstorming process. Questions to help the brainstorming could for example be *"What could cause the item to fail in this manner?"* or *"What circumstance(s) could cause the item to fail to perform its function?"*.

According to SAE J1739, *"Occurrence is the likelihood that a specific Cause/Mechanism will occur during the design life"* [56]. This should be seen as a relative, not an absolute, value which can only be reduced through design change. The likelihood of occurrence of a potential failure cause is usually rated on a scale from 1 to 10. Occurrence can also be called probability depending on company requirements.

2.3.2.3 Step 3

Step 3 includes:

- Identifying current prevention controls used to establish occurrence.
- Identifying current detection controls used to establish detection rating.
- Calculating the initial RPN (Risk Priority Number).
- Recommending actions.

Prevention focuses on preventing the cause of the failure mode from occurring, and detection has a focus on detecting the cause of the failure mode.

Detection is a relative ranking associated with detection design control. The ranking can be lowered by improvement of planned design control. The affected team has to agree on an evaluation criteria and ranking system. The ranking of detection usually has a range of 1-10.

The Risk Priority Number (RPN) is a value between 1 and 1000 to rank the order of concerns in the product. This number is calculated by the product of Severity (S), Occurrence (O) and Detection (D) according to equation (2.1).

$$RPN = (S) \times (O) \times (D) \tag{2.1}$$

The failure modes with high RPN and high severity rank should be prioritized for corrective actions.

2.3.3 ISO 26262

Functional safety ensures that a device or system acts correctly to the input it receives with regards to safety. It is one aspect of the overall safety of a system. Functional safety identifies potentially hazardous situations, conditions or events that could lead to harm of person or property, and enables corrective or preventative actions to avoid or reduce the impact [57].

IEC 61508 is an international standard by the International Electrotechnical Commission (IEC) for functional safety of all electrical, electronic and software systems. The adaptation of this standard for road vehicles is called ISO 26262. The standard is applicable for development of passenger cars since 2011, and Volvo Group is expecting to expand this to trucks and buses by 2018. This section is based on the manual *ISO 26262: Road vehicles - Functional safety* if nothing else is stated [58].

The standard ISO 26262 uses risk assessment, hazard analysis and Automotive Safety Integrity Level (ASIL) determination to establish safety goals for Electrical/Electronic (E/E) components to prevent and mitigate hazardous events to reduce risk of malfunction. The ASIL rating is decided by considering the factors severity, probability of exposure and controllability.

This section will only focus on the Concept Phase adaptation of ISO 26262 (Chapter 3 in the manual).

2.3.3.1 Severity

The severity classification is a result of an evaluation of the potential harm from a hazardous situation. It is estimated for all hazardous events, which are assigned one severity class from S0 to S3 each, according to Figure 2.3. S0 denoted a consequence limited to material damage and an ASIL assignment is not required.

	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 2.3: Classes of severity in ISO 26262.

2.3.3.2 Probability of exposure

Estimation of the probability of exposure requires evaluation of scenarios with relevant environmental factors which can contribute to creating a the hazardous situation. Each hazardous event is assigned a probability class between E0 and E4 depending on the estimated probability of exposure, as can be seen in Figure 2.4. E0 can be used, but should be seen as an extremely unlikely event and has no need for follow up.

The probability of exposure can be graded based on duration of a situation or frequency of

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

Figure 2.4: Classes of probability of exposure in ISO 26262.

occurrence of a situation. The duration of a situation is estimated by the proportion of time compared to the total operating time. In some situations, the probability of exposure will be more accurate if it is estimated by the frequency of occurrence of a related driving situation. Some driving situations may have both frequency and duration, where the most appropriate exposure rank should be chosen.

2.3.3.3 Controllability

The controllability class is an estimation of the probability of the drivers ability to retain or regain the control of the vehicle in a hazardous situation. The estimation is based on assumptions with regards to for example age, driving experience, target market etc. The controllability is estimated for all hazardous events, and is ranked from C0 to C3, see Figure 2.5.

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

Figure 2.5: Classes of controllability in ISO 26262.

2.3.3.4 Automotive Safety Integrity Level - ASIL

The parameters severity, probability of exposure and controllability are used to determine an ASIL rating for each hazardous event. The ASIL should be determined in the beginning of the product development process and is an important component for ISO 26262 compliance. The ASIL ranking answers the question *"If a failure arises, what will happen to the driver and associated road users?"*.

All hazardous events are assigned an ASIL rating of QM, A, B, C or D, where D is the most severe and QM is non-hazardous. After the ASIL raking is determined, a safety improvement for the system is developed if needed. The final Table can be seen in Figure 2.6

2.3.4 Fault-Tree Analysis - FTA

Fault-Tree Analysis (FTA) was first used in the early 1960s in the US Air Force. An FTA is a structured logic diagram with a top-down approach used to analyze system failures and component faults [59].

An undesired event (system or subsystem failure) is defined and all combinations of basic events that will lead to this occurrence are analyzed. The basic events all represent causes for the undesired event, which can be for example hardware failures, human errors or environmental

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 2.6: ASIL determination in ISO 26262.

conditions. The FTA visualizes the logical relationship between undesired event and basic fault events and provides a graphical representation of the ways which a system can fail [60]. The FTA is constructed by the Boolean logic symbols AND and OR. It is used to identify how to reduce the risk of system failure. The top event (the hazardous event) of the FTA is usually found by a preliminary hazard analysis, and the FTA usually consists of five steps:

1. Define undesired event
2. Understand the system
3. Construct fault tree
4. Evaluate fault tree
5. Control hazards identified

FTA is efficient at showing how resistant a system is to potential faults, but not at finding all possible initiating faults. FMEA, on the other hand, is efficient at categorizing initiating effects and identifying their effects but not at examining several failures or their effect at system level.

2.4 Risk assessment in other sectors

Risk assessment is a vital part of product development in all sectors. In some areas, for example nuclear plants and aerospace, it is of very high importance that no issues occur, since a failure can result in many fatalities. More information regarding these risk assessment method can be found in Appendix B.

3
Method

This chapter contains the methodology used for development of the method to evaluate product defects. The chapter will present factors affecting the decision of recall, the method to identify hazardous scenarios, and the method for evaluation according to severity, probability of exposure and controllability. Furthermore, the final ASIL rating as well as application and verification of method will be described.

The current methodology for investigating potential safety related cases has several similarities to the methods for hazard analysis, risk assessment and evaluation of functional safety, described in Section 2.3. However, these methods are developed to be used in the project phase of product development, why none of them are directly applicable to safety related product defects, which mainly appear in the maintenance phase. The methods were, however, a good starting point for the development of the method for analysis of product defects.

Many risk assessment methods distinguish three steps in the analysis process: identify hazardous scenarios, likelihood of occurrence and consequence, see Section 2.3. However, this might not be sufficient to determine the severity of all possible defects, and some methods have therefore included other factors to get a result which is as comprehensive as possible. Examples of this is ISO 26262, which has included the category *Controllability*, and FMEA with the category *Detection*. The conclusion of this was that it was reasonable to assume that the likelihood/probability and the consequences/severity had to be investigated for each scenario, but this might not be sufficient to receive a complete analysis of the defect. The methods ISO 26262 were to a large extent used as base for the evaluations, since these methods are the most comprehensive of the studied hazard analysis, and already are used within Volvo. Nevertheless, the first step was to identify all hazardous scenarios.

3.1 Identifying hazardous scenarios

The system used for categorizing potential safety defects at Volvo Group today are the Customer Safety Effects, as described in Section 2.1.3. Most of these categories are very general, and do not describe a specific hazardous scenario in it self. However, it is a suitable way of categorizing similar events. From these main categories, subcategories based on possible hazardous scenarios were created, where each subcategory describes a specific scenario. These scenarios can contain defects of several different parts, which all lead to the same possible risk scenario. It is also important that the defect is categorized for the resulting effect of the defect (”*worst case scenario*”) and not for the root cause. For example, a leakage of oil leading to fire will be categorized as *Fire in vehicle* and not as *Leakage of fluid*.

Most of the hazardous scenarios were found by analyzing data from potential safety defect cases collected at Volvo Trucks, as well as internal and external recall data. The external recall data was collected from the websites for DVSA (UK) and MLIT (Japan), where the data is easily accessible. The information regarding root cause and resulting effect for each case was studied, and the CSE was identified. All cases in each CSE were studied to find different hazardous scenarios that can occur.

However, it is likely to assume that not all possible hazardous scenarios could be found in the cases studied. Therefore, each Customer Safety Effect was studied with a Hazard Analysis approach, described in Section 2.3.1. It was thereafter found that the scenarios could be analyzed from either a top down (as in FTA) or bottom up (as in FMEA) approach. This means that the problem can be approached either by finding possible accident scenarios and from that identify what product defects that can cause the specific scenario, or by studying a product defect and identifying what possible accident scenarios this defect can result in. In this study, both methods were used to cover as many situations and defects as possible, hence making the method as comprehensive as possible. This method was especially applied in categories with few cases found in the potential safety defect cases and recall data.

When the hazardous situations were found, all possible corresponding crash scenarios were identified from the categories described in Section 2.2.1.1. For example, the hazardous scenario *Complete loss of service brakes* can result in a rear ending accident, hitting a vehicle turning off the road, hitting vehicle in intersection, hitting a pedestrian crossing the road and single accident running off road.

For hazardous scenarios not occurring during driving, there are no predefined accident situations which the scenarios had to be compared to. The possible outcomes were identified by studying data regarding accidents in maintenance and service, as well as finding available safety systems, restraints and features.

3.2 Severity

The possible severity of the injuries from a crash due to a product defect is within Volvo Group today one of the most vital components when deciding if a product should be recalled or not. It was therefore important that as many scenarios as possible were covered to be able to conclude what the worst possible outcome of a defect can be in terms of injuries.

The severity ratings of both FMEA and ISO 26262 were therefore studied. The severity rating of an FMEA is usually divided into ten steps, and the rating in ISO 26262 was divided into four steps. In both methods, the analyst of the case studies each scenario and determines a rating based on judgment and experiences. There is no way of assuring that the same value will be used in similar scenarios in future assessments. In this method, to ensure ratings with values that are as reasonable as possible, accident statistics were used as the foundations of the severity rating as far as possible. All severity ratings were gathered in tables that can be used in future evaluations, to ensure that the same values are used for similar cases.

3.2.1 Severity for scenarios occurring during driving

To determine the severity level of each crash scenario that occurs during driving, the data base STRADA was used, described in Section 2.2.1. STRADA was chosen since it is a comprehensive database covering all accidents in Sweden which are reported to the police. Furthermore, the data in STRADA is easily accessible.

The police data in STRADA was used, and the information *Type of Accident*, *Speed Restriction*, *Sub and Primary Element* and *Injury Extent* was extracted for all cases with a truck involved as either a sub or primary element. Initially, the cases were sorted according to type of accident. Thereafter, the injury level of the persons involved in the crash was studied with respect to the speed limit of the road of the accident. The injury of all road users involved in the crash is considered when studying the injury level. The injury level in STRADA is, as defined in Section 2.2.1, defined on a scale from one to four, where one is the most severe. The speed was divided into three levels: one for low speed (<=40 km/h), one for medium speed (50-70 km/h) and one for high speed (>=80 km/h). For each speed, the percentage of injuries of the different injury levels were found. For each crash scenario, described in Section 2.2.1.1, this data is presented in Appendix C.4. Depending on how large share of the crashes leading to a certain injury level, a severity rating was determined. A high number of rating levels of severity, as in FMEA, could give a very specific determination of the severity in each case. However, the risk of faulty ratings is very high. From the detail available in the STRADA police data regarding injuries, it was determined that a four-level severity rating, similar to that of ISO 26262, would be sufficient. The values for the threshold of each level were inspired by those used in ISO 26262, in combination with studying the data from the different crash scenarios. The levels of severity were divided accordingly:

- S3 - More than 15% probability of Injury level 1-2.
- S2 - More than 10% probability of Injury level 1-2.
- S1 - More than 10% probability Injury level 1-3.
- S0 - Injury level 4 and less than 10% probability of Injury level 1-3.

These values were used to create a severity table, where the severity level for all different types of accidents in the three speed intervals were gathered.

3.2.2 Severity for scenarios occurring in crash or during maintenance/service

As mentioned before, the STRADA data only covers accidents which have occurred during driving on public roads, and is therefore not applicable to accidents in maintenance, service or at standstill. Furthermore, the information regarding usage of safety systems, safety features or restraint systems during a crash is limited. Therefore, scenarios during these settings were analyzed with data found from different studies and similar cases. The data obtained covered, for example, accidents in maintenance, effectiveness of belt and airbag, and the effect of electric shock on the human body. These studies and the data used are presented in the *Result* chapter (Chapter 4), as well as in Appendix C.3. The same severity scale was used for these accidents as for the crashes occurring during driving on a public road. However, contradictory to the STRADA-data, the exact injury level is hard to determine. The data found in the studies presented, covering for example injuries in maintenance, only includes cases where injuries have occurred. This is due to the fact that incidents without personal injuries or with very modest injuries will not be reported, and therefore cannot be found in any statistics. Therefore, exact numbers of injury level have not been used in any evaluations, but the data rather gives an indication of the severity.

The scenarios found were divided into three tables; failures in maintenance/repair or at standstill, failures in crash and other failures. The category *other failures* contains cases which are not possible to categorize in any of the other categories, or can occur at any time. This table contains for example fires, failure of safety systems and asphyxiation.

3.3 Probability of exposure

If the likelihood of a defect to occur in a vehicle is very low, this method should not be applied to the case. That is, if very few cases have been reported from the market in relation to the affected fleet, a recall should usually not be issued regardless of severity. It was therefore determined that the study works with the assumption that the crash scenario does occur, and every assumption and rating was determined through this definition. For each truck model, the likelihood of this truck being exposed to a certain collision scenario was determined. For example: *if steering is lost in a Volvo truck, how likely is it that the truck will head-on collide with another vehicle in 100 km/h?*. This was an important factor in finding the most severe and probable worst case scenario and in excluding the most unlikely cases. This category was divided into different use cases depending on the truck model to determine the probability as precise as possible, but also includes one category for cases occurring in all models.

The usage environment of a truck can vary greatly depending on the intended use. The different truck models are intended to be used in certain environments, which can, depending on the specifications, be slightly modified for different usages. Factors which can be specified and can vary significantly between the different models are, for example, road usage, number of start and stops and condition of the road. The parameters that can be modified according to intended usage are in Volvo Group defined in the Global Transport Application (GTA) parameters, more information can be found in D.2. The GTA parameters and usage information of sold trucks were found in an internal database called VDA. The VDA database contains information regarding around 73 000 trucks sold in Europe, but only data from trucks sold to Sweden were used in this project. By studying the most common GTA parameters specified for each truck model in the VDA data, the most common usage scenarios were determined. The same data was also collected for all truck models combined, since many product defects affect all models.

The determined usage of the different truck models, as described above, was combined with data regarding Swedish roads, since Sweden is the defined market within the scope. This data contained the number of kilometers of road with different speed limits and crash barriers, divided into urban and rural roads, found in Appendix D.1. This enabled the possibility of evaluation of how likely it is that the specific truck drives on certain types of roads, and furthermore the probability of certain types of driving situations. However, not all driving situations needed for a comprehensive model could be deduced from this data. Therefore, certain assumptions had be made with this data as a starting point. An examples of this is: the vehicle rarely drives on low speed roads, and therefore it is assumed that it is rare with pedestrians close to the vehicle while driving. Some scenarios might be affected by the weather, and data regarding number of days with rain, snow and average temperature in Sweden was found by SMHI [61]. This data is presented in Appendix D.4. Furthermore, to ensure a reasonable evaluation, the exposure values determined were compared to values found in ISO 26262 evaluations on similar scenarios. In ISO 26262, E0 can also be used. However, in this report a category that was even more rare than E1 was found to not be necessary. The levels of probability of exposure used are defines as:

- E4 - over 10% of driving time.
- E3 - 1-10% of driving time.
- E2 - <1% of driving time.
- E1 - Not specified, very rare.

The intervals of these ratings are approximate and were based on the intervals determined in ISO 26262. However, the exposure rating described above only covers accidents that occur on public roads while driving. Failures that occur in maintenance/service or in a crash had to be evaluated separately. The different levels of exposures were in these cases defines as:

- E4 - occurs during almost every maintenance/service/crash.
- E3 - occurs often during maintenance/service/crash.
- E2 - rarely occurs during maintenance/service/crash.
- E1 - Not specified, very rare.

In maintenance, the situations are sorted based on assumptions on how regularly the different actions are performed. The exposure in crash is based on studies regarding how often the different systems are used, or different situations occur. This data is presented in Section 2.2.2 and in the respective results sections.

Since it within the scope is defined that the method should cover all cases occurring in Sweden, the method is developed with data regarding Swedish roads and weather, and specifications of trucks sold in Sweden. It is however highly applicable to similar markets such as the United States and large parts of Europe due to the similar conditions. Furthermore, if the method was to be updated with the data mentioned from another market, it could easily be applied to the respective market.

3.4 Controllability

Even if a truck is a subject to a failure of a part and is in a specific possibly hazardous location, not all the cases will lead to severe accidents. Some scenarios can be avoided by the driver, but how avoidable the accident is depends on the type of defect, the current environment, the speed and the occurrence of the situation. Therefore, it was concluded that how easily the situation could be controlled had to be taken into account. This is similar to the category *controllability* in ISO 26262, the the category will hereafter be called controllability. The controllability is in this report defined as how likely it is for the persons involved to be able to control the situation and avoid the accident situation defined in the hazard analysis.

One way to get a good estimation for this value is to perform tests with drivers, where it is recorded how many of the drivers that can avoid a certain collision. This method is in some cases used in determining controllability in ISO 26262 investigations. However, it is very expensive to perform these tests, and this is only used on rare occasions. As for the previous categories, the hazard analyses are most commonly performed by an expert estimating the outcome. Therefore, the controllability in this method had to be based on estimations as well. However, these estimations were concluded by studying previous ISO 26262 evaluations in combinations with information regarding the situation and the occurrence of the failure. For example, if the occurrence is sudden or if the speed is high, the situation is usually harder to control. For each Customer Safety Effect, all controllability evaluations were collected in a table, and this ensures that the same controllability value is used in similar case evaluations. The controllability is rated according to the following definition:

- C3 - Very hard for most drivers to avoid harm.
- C2 - Many drivers can avoid harm.
- C1 - Almost all drivers are able to avoid harm.
- C0 - Controllable in general.

The rating is based on the rating for controllability in ISO 26262.

3.5 Determine maximum ASIL for each case

Each accident situation for all hazardous scenarios found were studied and rated according to severity, probability of exposure and controllability as described above. By combining these values, an ASIL rating for each case was found by using the table found in Figure 3.1, which is as based on the ASIL table used in ISO 26262. The rating is defined as A-D and QM, where D is most severe and QM is defined as not safety related. The ASILs for the different hazardous scenarios were compared, and the highest ASIL (i.e. the ”worst case scenario”) in each scenario was determined and gathered in a table. However, note that regardless of the resulting ASIL rating, a recall might still have to be issued if, for example, not-compliance of safety regulations are fulfilled.

3.6 Verification of the method

In the recall information which can be accessed by public, the information is very limited. It is for example difficult to determine occurrence and reason behind a recall (safety or legal). When performing the analysis, more information is usually provided, to be able to perform an investigation which is as thorough as possible. Therefore, the verification of the method had to be performed on internal cases, both previous cases used to develop the method, but mainly new occurrences, since the method should be used during the decision process.

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 3.1: ASIL rating table.

4

Result

In this chapter, the results from the different stages of the development of the method will be presented. Initially, the recall decision process will be described, followed by determining the hazardous scenarios, severity, probability of exposure and controllability. Moreover, the differences between the Customer Safety Effects will be described separately in the Section 4.5, where the final worst case ASIL values will be presented.

4.1 Decision of recall and determining hazardous scenarios

The factors leading to a recall were identified by studying potential safety defects and external recalls. The total number of cases studied were 1210. The recalls from UK were issued between 1992-2017, in Japan between 2010-2017 and the internal cases were reported between 2014-2017. However, the recalls can cover truck older than the year the recall is issued.

The two most important factors in the decision process was determined to be the injury severity of the resulting accident the defect can lead to, and how probable the defect is by calculating how many defects that have occurred in the affected fleet. There are also several factors identified which leads to the defect not being classified as safety related. Some of these factors varies between the different Customer Safety Effects, but there are several factors that can be identified as common for most cases. These aspects are:

- The defect is a single case, root cause cannot be determined or root cause due to for example human error or faulty repair which does not lead to a problem occurring in a population of vehicles.

- Test of potentially defected part not showing any problem.

- No reported incidents from aftermarket.

- Misuse of product or function not within reasonable limits.

- Faulty repair.

If a potential defect can lead to very severe customer effects, an issue can be considered to be safety related even if one or several of the factors above are fulfilled. Moreover, even if the problem is not classified as safety related, a recall or service campaign can be issued if the problem is considered to be quality related or if the product does not comply with safety requirements. This method is not intended to be used in these cases, but only in cases where the decision of recall can be simplified by a rating indicating the severity.

If there is a clear notice that without a doubt, something should have been noticed by, for example, clear stepwise reduction in function, sound, movement in steering wheel, vibrations, during daily service or in maintenance/service, the case is not considered as safety related. Nevertheless, a correction of some kind (for example a quality recall or service campaign) might have to be issued. If there is any kind of slight previous notice, the hazardous situations might not avoided but the severity can usually be reduced. The occurrence described as *Previous notice* will hereafter be defined as *slight* notice, e.g. slight noise, vibrations or notice a few seconds before the failure. The notice might indicate that there is an issue, but not clearly exactly what part is defective. However, this is further analyzed in the separate CSE sections later on in this chapter.

The hazardous scenarios were determined for each of the Customer Safety Effects. These will therefore be presented in the respective CSE sections separately. The possible accident scenarios for each of the hazardous scenarios are also presented in the different CSE sections.

4.2 Severity analysis

The severity of a crash with a truck can vary greatly depending many factors, for example speed, direction of crash, location of hit, surroundings and object of impact. Each of the crash scenarios defined in the hazard analysis was compared to the corresponding category in the severity table created from the STRADA data, as described in Section 3.2. The table for crashes occurring during driving in high speed is presented in Figure 4.1. The severity tables regarding crashes during driving in low and medium speed can be found in Appendix C.5, Figures C.20 and C.21. The STRADA data used to define the tables can be found in Appendix C.4. A total of over 27 200 crashes were studied.

Defects that do not occur in a regular driving situation are not based on the data above. As described in Section 3.3, this data is based on information and reports on similar accidents, or different studies regarding the various subjects. The severity of each occurrence was gathered in three different tables; one for cases in maintenance, one for scenarios in a crash and one for other cases. These tables are found in Figures 4.2, 4.3 and 4.4 The data used is found in the respective categories and is gathered in Appendix C.3.

4.3 Probability of exposure analysis

Trucks have, as mentioned before, many different areas of usage. The most common truck model sold in Sweden was found to be the FH, the long distance truck and the flagship of Volvo trucks. Almost 80% of all trucks sold were of the model FH, compared to 17% for FE, 1% for FM and 2% for FL. The most common usages for each of these models are described in Appendix D.3. The data regarding the most common usage of the trucks was, as described in the Section 3.3, combined with the Swedish road data from Trafikverket, presented in Appendix D.1. With this data, in combination with weather data from SMHI (Appendix D.4) and data found when studying previous ISO 26262 investigations, a table for each of the truck models as well as a combined table for the average usage of the entire fleet were created. In further analysis, only

On roads >=80 km/h			
S0 Injury level 4 and less than 10% probability of Injury level 1-3	S1 More than 10% probability Injury level 1-3	S2 More than 10% probability of Injury level 1-2	S3 More than 15% probability of Injury level 1-2
	Accident with animal (small) (V1)	Vehicle reversing (V6)	Vehicle hitting parked vehicle (V5)
	Rear-ending accident (U)	Accident with animal (large) (W)	Single accident while driving straight (S 1, 3)
	Overtaking accident (O)	Accident with cycle in crossing, both driving straight (C5)	Single accident while turning (S 2, 4)
	Vehicle and cyclist in same direction, one is turning (C3)	Vehicle turning off road (A)	Meeting accident (M)
	Accident with cycle in crossing, one is turning (C6)		Accident while vehicle crossing the road (K)
			Accident with train (J5)
			Pedestrian crossing road (F 1, 2, 5, 6)
			Pedestrian walking next to road (F 3, 4)
			Meeting accident cyclist (C1)
			Accident cycle overtaking/rear ending (C2)
			Jackknifing
			Rear-ending stationary object
			Meeting accident object with no deformation zone (ex back of truck)

Figure 4.1: Severity for crashes in high speed.

the general values for the full fleet will be used for simplicity, but all variables are available for the different truck models separately. The exposure table for all truck models combined is found in Figure 4.5, and the tables for the separate truck models are presented in Appendix D.5 in the Figures D.9, D.10 and D.11.

As previously described, some product defects may occur in situations not related to driving. Therefore, probability of exposure regarding these defects were gathered in two tables; one for cases in maintenance or service and one for scenarios in a crash. However, these exposure values are assumed to be the same for all truck models. These exposure tables are presented in Figures 4.6 and 4.7.

4.4 Controllability analysis

The controllability of a hazardous situation is usually complex to asses and the results are hard to quantify. However, when studying the potential safety defects and the recall data, some factors regarding the controllability of the situation were found.

If there is a redundant system that can perform the same or similar tasks or counteract the result of the defected system, the situation is usually controllable to some extent. An example of this is if the service brakes fails, the driver can use the parking brake to reduce the speed of the vehicle.

If the defect is sudden with no previous notice, it is often hard for the driver to control the situation. If the driver, on the other hand, notices the defect before the failure, the situation

In Maintenance or at Standstill			
S0 Injury level 4 and less than 10% probability of Injury level 1-3	S1 More than 10% probability Injury level 1-3	S2 More than 10% probability of Injury level 1-2	S3 More than 15% probability of Injury level 1-2
	Superficial burn/freeze	Contact with harmful substance	Cab falling onto person
	Fall when accessing the cab (or low on the truck)	Fall when accessing a high part of the truck	Cab tilting back and crushing person
	Person hit by engine starting unexpectedly	Asphyxiation or Intoxication	Truck rolls over person (any speed)
	Engine hood unexpectedly falling hitting person	Small electric shock	Severe electric shock
			Risk of explosion
			Person underneath or very close to vehicle hit

Figure 4.2: Severity in maintenance and at standstill.

In Crash			
S0 Injury level 4 and less than 10% probability of Injury level 1-3	S1 More than 10% probability Injury level 1-3	S2 More than 10% probability of Injury level 1-2	S3 More than 15% probability of Injury level 1-2
	Too harsh tension of seat belt	Failure of seat/seat out of place	Doors/roofhatch not opening in case of crash
		Slightly reduced crash performance	Failure of seat belt all speeds
		Failure of safety system leading to increased risk of injury	Failure of airbag med-high speed
		Failure of part resulting in slightly reduced crash performance	Trapped in seat after case of crash
		Failure of airbag low	Airbag inflating too early/too harshly
			Failure of both airbag and belt
			ESC not working when needed
			Severly reduced crash performance
			Risk of explosion
			Fire after crash
			Failure of safety system leading to risk of fatalities of severe injuries
			Failure of part resulting in slightly reduced crash performance

Figure 4.3: Severity in crash.

Other failures			
S0 Injury level 4 and less than 10% probability of Injury level 1-3	S1 More than 10% probability Injury level 1-3	S2 More than 10% probability of Injury level 1-2	S3 More than 15% probability of Injury level 1-2
	ACC not braking when supposed to	Asphyxiation or Intoxication	Fire in or close to the cab
	Thermal event in cab		Fall of occupant from a vehicle in motion
	Leakage of fluids on the road		Fire in other part of truck
	AEBS not braking when supposed to		Risk of explosion

Figure 4.4: Severity, other.

	All truck models			
	E1 Not specified, very rare	E2 <1% of driving time	E3 1-10% of driving time	E4 over 10% of driving time
Road speed limit and crash barrier		Urban road low km/h with no crash barrier	Rural/highway roads high speed with crash barrier betweent the different directions	Rural/highway roads high speed with no crash barrier
			Urban roads med speed km/h with no crash barrier	Urban road high speed with crash barrier betweent the different directions
Road layout and topography	Driving through a train crossing	Urban intersections	Rural intersections	Driving in curve med speed
	Driving close to steep	Stopping at traffic light	Driving downhill with heavy load	Driving in curve high speed
	Driving on mountain road	Driving in curve low speed	Predominantely flat roads	
		Driving downhill with a curve	Medium speed crossings	
		Low speed crossing		
		High speed crossings		
Surrounding traffic	Vehicle passing parked vehicles low speed	Vehicle in front/behind low speed	Driving in a queue	Vehicle in front/behind med speed
	Vehicle passing parked vehicles med speed	Vehicle approaching in the left lane	Vehicle stopped on med speed road (about to turn)	Vehicle in front/behind high speed
		Overtaking on road with oncoming traffic	Vehicle stopped on high speed road (about to turn)	Vehicle following closely behind
		Vehicle standstill in queue	Driving downhill with vehicle in front	When parked, other parked vehicles in close proximity
		Vehicle stopped on low speed road (about to turn)	Overtaking/lane change on road without oncoming traffic med	
		Overtaking/lane change on road without oncoming traffic low speed	Overtaking/lane change on road without oncoming traffic high speed	
Surrounding VRUs	Bicyclist close to vehicle high	Right turn with cyclist approaching	Pedestrian crossing med speed	
	Pedestrian in close proximity high speed	Pedestrian passing behind vehicle	When parked, VRUs in close proximity	
		Pedestrian close to front of vehicle/passing in front of vehicle		
		Pedestrian crossing high speed		
		Pedestrian crossing low speed		
		Cyclist driving behind truck all		
		Bicyclist close to vehicle med speed		
		Bicyclist close to vehicle low speed		
		Pedestrian in close proximity med		
		Pedestrian in close proximity low		
Road surface/visibility		Ice/snow on road (slippery roads)	Wet road	
		Rough roads	Rain/snow	
		Dark, lighted	Dark, unlighted	
Maneuvering		Start and Stops		
		Vehicle parked in steep slope	Vehicle parked	
		Truck placed in a closed area with people in close proximity	Vehicle at standstill	
			Vehicle parked in slight slope	
Other	Emergency braking	Parked truck with driver sleeping		Trailer or Semitrailer attached
				Driver/occupant in vehicle during driving

Figure 4.5: Probability of exposure during driving on public roads for all truck models combined.

In Maintenance/service			
E1 Not specified, very rare	E2 rarely occurs during maintenance/service	E3 occurs often during maintenance/service	E4 occurs during almost every maintenance/service
During maintenance, service or standstill persons are never in this area	During maintenance, service or standstill persons are rarely in this area	Climbing onto high part of vehicle	Maintenance/service personnel underneath vehicle during maintenance/service
		Climbing onto low part of vehicle	When working on the engine, the probability of someone being injured if started is large
		Work behind tilted cab	When hood is open, it is very likely that a person is in the trajectory if it were to fall
		People are sometimes in this area during standstill/service/maintenance	Climbing into truck
		Changing fluids/ being close to containers of fluids	Mainenance/service personnel are frequently in contact/in close proximity with cables that could cause electric shock
		Close to heat conducting parts	During maintenance, service or standstill persons are usually in this area
		Close to containers of hot fluids	Cab tilting during maintenance and service
			People are commonly in this area during standstill/service/maintenance
			Person close to the vehicle during maintenance/service
			Vehicle parked in closed area during maintenance/service

Figure 4.6: Probability of exposure in maintenance and service.

In Crash			
E1 Not specified, very rare	E2 rarely occurs in a crash	E3 often occurs in a crash	E4 occurs in almost every crash
ESC used during good road cond	Safety system not often used in crash	Airbag deployed low speed	Airbag deployed med/high speed
	ESC used durig bad road conditions	Safety system fairly often used in crash	Safety system commonly used in crash
			Seat belt used in collision all speeds
			Driver in seat during collision
			Crash structure reducing injuries
			Occupants stuck in cab after crash

Figure 4.7: Probability of exposure in crash.

might be easier to control or the driver should have taken action to avoid a failure. However, this depends on the defect. More severe defects (as for example loss of steering or braking) may be very hard to control regardless if the driver have been notified. Furthermore, even if there are signs of the defect previous to the accident, it must be reasonable for the driver to notice it. This has to be investigated by the analyst prior to the application of the method, and if it cannot be determined, a sudden occurrence can be assumed.

Nevertheless, for all the above factors, it is also important to evaluate if the driver actually will be able to perform the action in the short time before an accident might occur. This will differ depending on surroundings, speed, driver etc. The drivers of trucks were assumed to be experienced, and therefore a higher number of situations can be properly handled and accident avoided compared to a regular car driver. The demands are also higher on the maintenance and service of the vehicle, as well as for a detection of potential failures.

Each hazardous scenario was investigated separately to ensure the most reasonable evaluation. All of the values were collected into a table for each Customer Safety Effect, which can then be applied to similar cases. These tables are presented in Appendix E.

4.5 Categories

In this section, the different Customer Safety Effects will be described in separate sections. In these sections, the identified hazardous situations and crash scenarios as well as additional information and assumptions used in the analysis will be presented. Furthermore, the worst case scenarios identified are found in a table in each section. All ratings are based on exposure for all truck models, and all crash situations are analyzed for all speeds.

4.5.1 Vehicle stability and trajectory

Vehicle stability and trajectory contains cases where steering and stability of the truck is affected. The category is divided into: loss of steering, sudden wheel lock, vehicle side pulling or unstable while driving and vehicle side pulling or unstable while braking. The controllability table for all cases regarding loss of trajectory, steering or stability is found in Figure E.1 in Appendix E.1.

4.5.1.1 Loss of steering

If a defect results in a truck losing steering, the consequences can be very severe. The hazardous situations found in this category are: complete loss of steering, blocked steering, steering wheel locked in turned position, increase in steering effort and very heavy steering. These situations can for example be caused by: steering wheel coming off, link rod not fastened correctly or broken, loose front axle, propeller shaft loosened/falling off or leakage of power steering oil.

With further analysis of the hazardous scenarios, it was found that several of the scenarios most likely would give similar outcomes and could therefore be analyzed together. The cases complete loss of steering, blocked steering and steering wheel locked in turned position were all found to lead to a complete loss of control of trajectory and where therefore assessed together. The cases increase in steering effort and very heavy steering include all cases where some steering is possible, but is limited or very heavy, and both categories can result in the same accident scenarios due to the driver not being able to change the trajectory of the vehicle. The accident scenarios analyzed for all situations were: hitting pedestrian at side of road, frontal accident and single accident. The severity rating as well as the exposure rating for each of these crash scenarios in all speeds were found, and are the same for the different hazardous scenarios. However, the controllability will vary slightly between the two scenario-categories and also depend on the occurrence of the defect.

For the first group of hazardous scenarios leading to a complete loss of control of trajectory, three different occurrences where found and analyzed; sudden loss with no previous notice, previous notice or stepwise loss or loss of both steering and braking (with or without notice). Firstly, if not steering or braking is possible, the situation is very hard to control regardless of speed. Furthermore, sudden complete loss of steering can most likely be handled to some extent, since the brake circuits still are functioning and the driver has the possibility to brake to avoid a collision. However, the higher the speed, the less time the driver have to react and brake. Therefore, the controllability is reduced the higher the relative speed between the truck and the collision object (e.g. a frontal accident in medium speed has high relative velocity and is therefore hard to control). If the defect occurs with some previous notice or stepwise loss, the situation is in most cases considered as slightly more controllable, since this acts as a warning for the truck driver, who should be able to react faster if a problem occurs. The final ASIL ratings for all these cases are high, and the values are found in Table 4.1.

For the other category of hazardous scenarios where slight steering is possible, the situations are in general slightly more controllable than the cases described above since both braking and limited steering is possible. However, it is still hard to fully avoid an accident in high speed, and the maximum ASIL found is therefore high for these scenarios as well, see Table 4.1.

Table 4.1: Worst case scenarios with ASIL for loss of steering.

Occurrence	Case	ASIL
Complete loss of steering, blocked steering or steering wheel locked in turned position		
Sudden loss, no previous notice	Single accident high speed, meeting accident med/high	D
Previous notice/ stepwise loss	Single accident high speed, meeting accident med/high	C
Loss of both steering and braking	Single accident med/high speed, meeting accident med/high	D
Increase in steering effort or very heavy steering		
Sudden loss, no previous notice	Meeting accident high speed, single accident high speed	C
Previous notice/ stepwise loss	Meeting accident med/high speed, single accident med/high speed	B

4.5.1.2 Sudden wheel lock

There are very few cases of wheel lock found in the data researched. However, by HA it was found that if one wheel suddenly is locked, the resulting accident can be very severe since the trajectory of the vehicle drastically can be changed. If both wheels suddenly are locked, the trajectory of the vehicle will usually be stable but the speed will drastically be reduced. Locking of two wheels will therefore be classified as *Unexpected braking of the vehicle*, see Section 4.5.3.2. The hazardous scenarios for wheel lock are therefore divided into: wheel lock of one steered wheel in front axle and wheel lock of one other wheel.

If wheel lock occurs on one wheel, there is a major risk that the trajectory of the vehicle change. The crash scenarios due to this situation are the same as for loss of steering, that is: hitting pedestrian at side of road, meeting accident and single accident. If the locking of brakes leads to a fire, the most severe CSE will be *Fire* and the defect will be categorized as such.

Wheel lock of a steered front wheel can cause very drastic change in trajectory of the vehicle in both medium and high speed. Therefore, the wheel lock is very hard to control even if the brakes still are functional, since the driver most likely will not have time to react before a crash. Furthermore, even if a situation with previous notice is slightly more controllable than a sudden event, the highest ASIL occurs at high speed failure, as can be seen in Table 4.2. A wheel lock on an unsteered wheel or any wheel on a rear axle of a truck usually does not result in a change in trajectory as severe as if the wheel lock is on a steered front wheel, but normally rather a side pulling. Therefore, these situations are regarded as more controllable than the case above, and a defect with previous notice is not classified as safety related. If this wheel lock on the other hand occurs on a slippery road, the same controllability as for a wheel lock on a steered front wheel is assumed. However, slippery roads are not very common and the ASIL rating is therefore not very high regardless of the less controllable situation (see Table 4.2).

Table 4.2: Worst case scenarios with ASIL for sudden wheel lock.

Occurrence	Case	ASIL
Wheel lock of one steered wheel on front axle		
Sudden occurrence, no previous notice	Single accident med/high speed, meeting accident med/high speed	D
Previous notice/ stepwise loss	Single accident high speed, meeting accident high speed	D
Wheel lock of one other wheel		
Sudden occurrence, no previous notice	Meeting accident med/high speed, single accident med/high speed	B
Previous notice/ stepwise loss	-	QM
Slippery road	Meeting accident med/high speed, single accident med/high speed	B

4.5.1.3 Vehicle side pulling or unstable while driving

Vehicle side pulling or unstable while driving includes all cases regarding lowered driving stability, both sudden events or reduced function over time. However, it does not include very sudden changes in driving conditions leading to loss of trajectory, for example tire explosions. These cases are categorized as *Sudden change of driving conditions resulting in loss of control of the vehicle*.

Situations which are classified as safety related in this category includes: sudden failure leading to side pulling and sudden failure leading to severely reduced stability. Examples leading to recalls are faulty leaf spring, radius rod disengaged from cross member, damaged V-rod, breakage of spring plates, rapid air loss in tire and stabilizer arm connecting rear axle to frame broken.

Both of the scenarios found are assumed to lead to similar accidents as loss of steering, i.e. hitting pedestrian at side of road, meeting accident and single accident. A side pulling or severely reduced stability, sudden or with previous notice, is usually very controllable in low speed, and controllable in general in medium and high speed since both steering and brakes are fully functioning. However, a sudden loss in medium and high speed still results in ASIL B, due to the high severity and exposure of the situations (see Table 4.3). As can be seen in Table 4.3, a defect with previous notice should not be classified as safety related. This also applies to cases where the process of failure is slow or if the vehicle still fulfills the requirements of stability.

Table 4.3: Worst case scenarios with ASIL for side pulling or unstable while driving.

Occurrence	Case	ASIL
Side pulling or unstable while driving		
Sudden occurrence, no previous notice	Single accident med/high speed, meeting accident med/high speed	B
Previous notice/ stepwise loss	-	QM

4.5.1.4 Vehicle side pulling or unstable while braking

There is no case found in the internal or external recall data or the potential safety related cases regarding vehicle side pulling while braking. The potential hazardous situations were therefore found by analyzing the category with HA methodology. The situations found were: imbalanced braking and inoperative brakes on one wheel. These are assumed to result in similar situations and therefore analyzed together. This can be the effect of for example software issues, uneven brake ware, stuck caliper or brake hose broken or fractured.

Vehicle unstable when braking will most likely also result in the same crash scenarios as the previous cases in this section. The occurrence and resulting situations are very similar to side pulling or unstable while driving, however, in contrast this category, the speed is usually lower due to the applied brakes. Nevertheless, the resulting ASIL ratings are the same as for side pulling or unstable while driving, as can be seen in Table 4.4.

Table 4.4: Worst case scenarios with ASIL for side pulling or unstable while braking.

Occurrence	Case	ASIL
Side pulling or unstable while braking		
Sudden occurrence, no previous notice	Single accident med/high speed, meeting accident med/high speed	B
Previous notice/ stepwise loss	-	QM

4.5.2 Thermal event

The CSE *Thermal event* contains the categories: fire in vehicle, thermal hot event and thermal cold event. The controllability table for all cases in this section is presented in Figure E.2 in Appendix E.2.

4.5.2.1 Fire in vehicle

This category describes the issues where the Customer Safety Effect is a fire or risk of fire. The defects that risk resulting in a fire usually create other problems as well, for example oil leakage leading to breakdown of another function, or brake drag leading to reduction in speed. Even if another Customer Safety Effects occurs, fire is always regarded as the most severe effect due to the high risk for injury and the high property damage costs.

Fire in a vehicle can be the result of several different problems. Some of the most common situations in a truck are identified to be: Oil spray/pressurized oil on hot surfaces, brake drag, short circuit/circuit malfunction creating sparks, chafing of unfused cables creating sparks, part in contact with hot area and overheating of part.

A common problem creating fire is long time failure of parts, either chafing of cables creating sparks or wear of hoses resulting in oil leakage. These are not considered to be safety related. Oil leakage is also a common defect for vehicles. However, it is only classified as a risk of fire if it is in spray form with risk of reaching hot surfaces. Other oil leakages might create problems with breakdown of other functions and/or oil on road leading to risk for other road users, which are classified as different CSEs. In conclusion, cases with small oil leakages, chafing of fused power cable, leakage not in spray form (not pressurized) and/or can not reach hot surfaces, dirt assembly in areas that should be cleaned regularly and long time failure are not considered safety related.

Depending on where in the vehicle the fire occurs, it can be more or less easy to control. If the fire occurs in the cab, there is a fire extinguisher which can be used to extinguish or reduce the fire. If the fire on the other hand is far from the cab, the driver will most likely have time to exit the cab before any injuries an be obtained. Nevertheless, as can be seen in Table 4.5, all sudden cases resulting in fire have the highest ASIL due to the high risk of injuries. This is largely due to the fact that vehicle fires historically have resulted in many fatalities, as described in Section 2.2.2.1. If there is a slight previous notice, such as smoke a short time before the fire, the defect and possible risk of fire could have been noticed. However, since the outcome still can be very fatal, it is regarded as safety related and rated high. Fires after a crash are considered a deadly post-crash problem, since it is common that the persons in the vehicle not are able to leave immediately after the crash. Therefore, a post-crash fire always obtain highest ASIL rating, as seen in Table 4.5.

Table 4.5: Worst case scenarios with ASIL for fire in vehicle.

Occurrence	Case	ASIL
Fire in vehicle		
Sudden occurrence, no previous notice	Fire in or close to cab	D
Previous notice/ stepwise loss	Fire in or close to cab	C
Sudden occurrence, no previous notice	Fire in other part of truck	D
Previous notice/ stepwise loss	Fire in other part of truck	C
Sudden occurrence, no previous notice	Fire after crash	D

4.5.2.2 Thermal hot event/overheating

Thermal hot event or overheating is when a thermal event is the most severe result of the malfunction. It is an overheating not leading to fire or other Customer Safety Effect, which for example can be contact with hot surfaces or sudden release of hot liquid. The possible harmful situations are risk of burn to a driver, maintenance personnel or third party. Therefore, the two situations concerned are: overheating of part or hot fluid leakage with risk of hurting driver. Examples of cases being recalled due to thermal hot event or overheating are: exhaust gas leakage and overheating of seat.

If there is some previous notice of the overheating, an injury is very easy to avoid (i.e. do not touch the surface/avoid the hot fluid). Even if there are few fatalities due to burns related to vehicles, it is a common injury in motor vehicle repair (described in Section 2.2.2.2). If sudden overheating in area where maintenance is common, the ASIL is therefore fairly high (B), see Table 4.6.

Table 4.6: Worst case scenarios with ASIL for thermal hot event.

Occurrence	Case	ASIL
Thermal hot event		
Sudden occurrence, no previous notice	Overheating of part in cab	B
Previous notice/ stepwise loss	Overheating of part in cab	QM
Sudden occurrence, no previous notice	Overheating of part in area where maintenance/service is common	B
Previous notice/ stepwise loss	Overheating of part in area where maintenance/service is common	QM
Sudden occurrence, no previous notice	Hot fluid leakage in area where maintenance/service is common	B
Previous notice/ stepwise loss	Hot fluid leakage in area where maintenance/service is common	QM
Sudden occurrence, no previous notice	Overheating of part in area where maintenance/ service not is very common	A
Previous notice/ stepwise loss	Overheating of part in area where maintenance/ service not is very common	QM
Sudden occurrence, no previous notice	Hot fluid leakage in area where maintenance/ service not is very common	A
Previous notice/ stepwise loss	Hot fluid leakage in area where maintenance/ service not is very common	QM

4.5.2.3 Thermal cold event

This category is defined in the same way as the previous category, meaning that a case is defined as thermal cold event if there is a health risk for driver, maintenance personnel or third party due to a cold part or fluid. However, there is a lack of information regarding thermal cold events within the data gathered from recalls and potential safety defects.

As in thermal hot events, it is very easy to avoid an injury if there is previous notice of the cold event. A sudden cold event can create injuries, but as described in Section 2.2.2.2, the temperature has to be very low to create a cold burn. This is most likely the reason why no recall cases have been found. However, if the cold event does occur, the ASIL rating is very similar to that of the hot events. The ASIL ratings for cold events are found in Table 4.7.

Table 4.7: Worst case scenarios with ASIL for thermal cold event.

Occurrence	Case	ASIL
	Thermal cold event	
Sudden occurrence, no previous notice	Part unexpectedly cold in cab	B
Previous notice/ stepwise loss	Part unexpectedly cold in cab	QM
Sudden occurrence, no previous notice	Part unexpectedly cold in area where maintenance/service is common	B
Previous notice/ stepwise loss	Part unexpectedly cold in area where maintenance/service is common	QM
Sudden occurrence, no previous notice	Part unexpectedly cold in area where maintenance/ service not is very common	A
Previous notice/ stepwise loss	Part unexpectedly cold in area where maintenance/ service not is very common	QM

4.5.3 Braking of the vehicle

This section contains defects regarding both loss of service brakes and unexpected braking. The controllability tables used in the evaluation in this category are found in Figures E.3 and E.4 in Appendix E.3.

4.5.3.1 Loss of service brakes

Loss of service brakes can often be a severe customer effect, and can in several situations result in very serious accidents. The situations identified as possibly safety related are: complete loss of service brakes, loss of both brake circuits and reduced brake capacity. Defects which have resulted in recall are for example: brake pedal shaft coming loose and decreased brake force due to air leakage on brake system.

U.S Department of Transportation has concluded that brake problems are found among almost 30% of the crashes with trucks in the United States during 2001 to 2003 [62]. The most likely crash scenarios identified when loosing brake capacity are: rear ending accident, hitting vehicle turning off road, hitting vehicle in crossing, hitting pedestrian crossing the road and single accident driving off road.

If both brake circuits are lost, the situation is very hard to control regardless of the speed of the vehicle and if steering still is functioning. However, if only service brakes are lost, the situation can be controllable to some extent since the speed of the vehicle can be reduced with the parking brake. Nevertheless, in higher speed it is hard for the driver to have time to react and use the parking brake instead of the service brake to reduce speed, and a crash is therefore hard to avoid. If it is possible to notice the defect prior to the failure (e.g. by slight noise or vibrations), it is more reasonable to assume that the driver will react fast and have time to use the parking brake to reduce the severity of a possible collision. As can be seen in Table 4.8, the ASIL rating for complete loss of service brakes is high in general, but slightly lower for cases with previous notice.

If brake capacity is reduced but not entirely lost, the truck can steer and brake slightly with the service brakes and fully with the parking brake. However, the truck might not be able to fully stop before a collision. Nevertheless, the collision will most likely occur in a lower speed than the cases presented above. If there is some previous notice that the brake capacity is reduced, the driver can react and apply the parking brake faster or brake harder to compensate, and the situation is therefore not considered as safety related. Reduction of brake capacity is very similar to *Deceleration not as intended* in the category *No control of vehicle speed*, see Section 4.5.5.1.

Table 4.8: Worst case scenarios with ASIL for loss of service brakes.

Occurrence	Case	ASIL
Complete loss of service brakes		
Sudden occurrence, no previous notice	Single accident while turning high speed	D
Previous notice/ stepwise loss	Single accident while turning high speed	C
Loss of both brake circuits	Single accident while turning med/high speed	D
Reduced brake capacity		
Sudden occurrence, no previous notice	Single accident while turning high speed	C
Previous notice/ stepwise loss	-	QM

4.5.3.2 Unexpected braking of the vehicle

Unexpected braking of the vehicle includes both sudden breaking of the vehicle as well as gradually locking of the brakes. The braking can last for a short duration of time or permanently until the faulty component is exchanged. Braking on one wheel is, however, categorized as side pulling since this is regarded the most severe customer effect. The hazardous scenarios found are divided into two categories: harsh braking and slight braking. The category with harsh braking contains: harsh unexpected braking, application of parking brake, harsh brake drag, unexpected locking of brakes, sudden locking of two wheels and brakes applied when accelerator pedal is pressed. The second category with slight braking contains: slight unexpected braking, application of parking brake and slight brake drag. Examples of defects leading to these problems are unintentional activation of AEBS, brake hose separation and air tank damaged.

The possible crash scenarios for both categories identified are: vehicle or cyclist behind driving into the rear of the truck (i.e. a rear ending from a vehicle or cyclist). In low speeds, the person behind the truck should keep a distance large enough to avoid a collision even during a harsh sudden braking. Furthermore, the person behind should keep a large distance even in medium and high speed to be able to brake, but might not have time to come to a complete stop before a collision if the sudden braking is harsh. If the braking occurs without brake lights, it is even harder for the person travelling behind to have time to brake. An example of a collision due to unexpected braking is an accident in Singapore in 2016 involving 13 vehicles which was caused by one car suddenly braking hard [63]. Yet, as can be seen in Figure 4.9, the ASIL for cases with harsh unexpected braking is not very high, much due to the fact that rear ending accident usually not result in severe injuries.

Slight unexpected braking, with or without brake lights, is as can be seen in Table 4.9 not considered as safety related. The person behind should keep a distance which allows slight sudden braking without collision. If over-braking on one axle occurs, there is a risk of a jackknifing situation. If a jackknifing situation arises, it is hard for the driver to control the situation. However, there are today safety systems in the truck which reduces the probability of a jackknifing situation of occurring. If a jackknifing situation does occur, the severity can be very high. Therefore, this scenario results in a an ASIL B, as can be seen in Figure 4.9. The controllability for jackknifing situations are found in Figure E.8 in Appendix E.7.

Cases with slight previous notice are only considered to be safety related if occurring without brake lights (see Table 4.9). Furthermore, stepwise loss is not considered safety related for any case in this category, since the result of a stepwise loss would be a stepwise reduction of speed. Furthermore, if locking of the wheels occurs at standstill and render the vehicle inoperable, the defect is not considered safety related since no persons are at risk of injuries.

Table 4.9: Worst case scenarios with ASIL for unexpected braking.

Occurrence	Case	ASIL
Harsh unexpected braking, application of parking brake, brake drag, unexpected locking of brakes, locking of two wheels, brakes applied when accelerator pedal is pressed		
Sudden occurrence with brake lights	Rear ending high speed, cyclist driving in to rear of vehicle high speed	A
Sudden occurrence without brake lights	Rear ending high speed	B
Previous notice with brake lights	-	QM
Previous notice without brake lights	Rear ending high speed	A
Slight unexpected braking, application of parking brake, brake drag		
Sudden occurrence with brake lights	-	QM
Sudden occurrence without brake lights	-	QM
Over-braking on one axle		
Sudden occurrence, no previous notice	Jackknifing high speed	B
Previous notice loss	-	QM

4.5.4 Integrity of the vehicle

Integrity of the vehicle contains the categories: trailer or semi-trailer uncoupling, loss of parts, sudden leakage of fluids, cab or hood falling and impaired vision and conspicuity. The controllability table used in this section is found in Figure E.5 in Section E.4.

4.5.4.1 Trailer or semi-trailer uncoupling

The trailer or semi-trailer is connected to the truck by a coupling mechanism or a fifth wheel. If there is a problem with this coupling, the trailer might come off. The only hazardous situation needed to study these defects is trailer or semi-trailer coming off. Defects found that can cause this problem are: malfunction of secondary lock, locking pin insufficient and fifth wheel coming off.

A trailer coming loose can result in very hazardous situations. The crash scenarios found are: vehicle rear ending stationary object on road and meeting accident with object without deformation zone. Both of these crash scenarios result in a high relative speed change in case of a crash. Furthermore, the rear of a trailer does not have any deformation zone, and can therefore result in more severe crashes than of those found in the category *Meeting accidents* in STRADA.

If the driver of the truck in any way has been notified of the problem prior to the failure, the situation is not classified as safety related since the driver should have investigated the problem. Furthermore, if only part of the coupling is broken or the trailer still is attached to the truck, the defect is not considered to be safety related.

In low speeds, the surrounding traffic should be able to avoid a crash with a trailer stationary on the road in the same way as a harsh unexpected braking situation. However, the meeting accident can be slightly harder to avoid, since steering away possibly can create another crash. In medium and high speed situations, the relative speed is high in both crash situations, and a crash is therefore hard to completely avoid. As can be seen in Table 4.10, ASIL D is assumed for all defects resulting in trailer uncoupling. An example of an accident where the trailer was loosened due to a faulty fifth wheel occurred in Alabama (US) in 2015, which resulted in the trailer plowing through the oncoming traffic ending up killing two persons [64].

Table 4.10: Worst case scenarios with ASIL for Trailer uncoupling.

Occurrence	Case	ASIL
Trailer uncoupling		
Sudden occurrence, no previous notice	Meeting accident with trailer med/high speed, rear ending stationary trailer high speed	D

4.5.4.2 Loss of parts

The CSE loss of parts is defined as when a part is falling off the truck, and the hazard is for other road users in risk of being hit by or driving into the part. Usually, a part coming off the vehicle results in other consequences as well, and the defect should only be placed in this category if this is the most severe customer effect.

Loosing parts can create hazardous situations if the part falling off is large and/or heavy, or if the part is located high on the truck (risk of hitting windscreen of vehicle behind). Both of these defects may cause the vehicle behind to loose control of the vehicle. Example of recalled cases are: under-run protection falling off, cross member falling off, roof hatch falling off, wrong rims fitted with risk of falling off, hydraulic pump falling off and air/fuel tank falling off.

If the vehicle behind the truck looses control of the vehicle, the following crash scenarios could occur: hitting a bicycle, hitting a parked vehicle, hitting a pedestrian, a head-on collision and a single accident. The situation is hard to control for the vehicle behind, since the situation is sudden and unusual. However, in low speeds, the road user at risk in the surrounding can possible steer and apply brakes to avoid the accident. However, the higher the speed, the harder to avoid a crash. This can be seen in Table 4.11, where it is found that the defects results in an ASIL D. According to a study by Safe Work Australia, three deaths in Australia between the years 2003-2012 have been traced back to wheels falling off a truck and hitting another vehicle [24].

It the part still to some extent is fastened to the vehicle or if there is a notice to the driver of the defect by for example sound, vibrations in steering wheel or visible during daily service, the defect should not be considered as safety related. Furthermore, to be classified as safety related, it is important that the analyst investigates how the part falls of the vehicle, and how the surrounding road users could be hit. If there is no risk of the part hitting another road user when falling off, it should not be considered as safety related.

Table 4.11: Worst case scenarios with ASIL for loss of part.

Occurrence	Case	ASIL
Loss of part leading to driver behind loosing control of vehicle		
Sudden occurrence, no previous notice	Meeting accident med/high speed, single accident high speed	D

4.5.4.3 Sudden leakage of fluids

Leakage of fluids includes leakage of all fluids in the vehicle. The fluid leakages in this category creates a hazard for third party due to fluid on the road or risk for driver or maintenance personnel. Some fuel leakages may lead to fire, and these cases are instead categorized as *Fire in vehicle*. If the loss of fluid results in loss of another function with more severe consequences, for example loss of steering or braking, it will be categorized as a this CSE.

Hazardous situations found are: large leakage of fluids on the road and leakage of harmful substance in maintenance with risk for surrounding personnel. These situations can for example be caused by oil hose strength not sufficient, defective fuel pump, injection pipe loosened, faulty fuel filter, oil cooler hose loosened, crack on fuel pipe, fuel tank not fastened correctly, oil leak power steering and cracks on oil hose.

As described in Section 2.2.2.3, large amounts of oil on the road has lead to severe crashes. However, most commonly, the vehicles on the road should get a previous notice from seeing the oil on the road. However, as can be seen in Table 4.12, the defect is still classified as safety related with an ASIL rating of B.

In Section 2.2.2.3 it is also described that around 6% of the fatalities in motor vehicle repair in the UK every year are caused by leakages of fluids. A sudden leakage is very hard to control and avoid, and if the leakage of fluids occurs in an area where maintenance or driver commonly are located in, the risk of injury is high (and so is the ASIL rating, see Table 4.12). Fluid leakage both on road and in maintenance is only considered to be safety related if it is sudden and if the leakage is large.

Table 4.12: Worst case scenarios with ASIL for leakage of fluids.

Occurrence	Case	ASIL
	Large leakage of fluids on the road	
Previous notice	Meeting accident med/high speed, single accident high	B
	Fluid leakage in maintenance	
Sudden occurrence, no previous notice	Leakage of harmful substance in area where maintenance personnel or driver often is located in	C
Sudden occurrence, no previous notice	Leakage of harmful substance in area where maintenance personnel or driver rarely is located in	A
Sudden occurrence, no previous notice	Leakage of harmful substance in area where maintenance personnel or driver never is located in	QM

4.5.4.4 Cab falling

If there is a problem with the attachment of the cab, it may fall into the floor while tilted. This creates a risk of the cab falling onto the driver or maintenance personnel, which most likely would result in very severe injuries due to its large weight. The hazardous scenarios identified are: cab falling into the floor and cab tilting back to original position which can result in crushing a person located in this area. Defects that have found to cause these situations are: stretched attachment bolt, pull chamber oil leakage, cab tilt torsion bar broken and faulty cab mount bracket.

The scenario of the cab falling can only happen when the cab is tilted, which is common when the vehicle is in maintenance or repair. Even if the safety procedure includes not going under a tilted cabin, this is determined to be a misuse within reasonable limits. If a fall of the cab occurs, it is not possible to control the situation and avoid possible injuries. If there is a risk of the cab falling in to the floor, the resulting effect of the accident is determined to be severe enough to always classify it as safety related. This also applies to cases with prior notice by for example hard tilting.

If a defect causes the cab to fall back to upright position during the tilting, there is a risk that someone might be in the the area behind and get injured or even killed, as in an accident during maintenance in Australia. This accident was however due to a locking pin being dislodged or not being inserted and not a product defect [65]. In the same way as for a cab falling into the floor, the situation is not controllable and is considered as very severe both with and without notice. However, it is not not as common for people to be behind the tilted cab than close in front of a tilted cab, why the ASIL is found to be slightly lower.

4.5.4.5 Impaired vision and conspicuity

This category contains all cases regarding ”see and be seen” for the truck driver and the surrounding traffic. Many cases of recalls due to impaired vision and conspicuity are quality related or due to the vehicle not fulfilling safety regulations. It rarely creates large safety hazards, due to the fact that the driver still is in control of the vehicle and can stop the vehicle if a problem occurs. However, several hazardous situations have been found: sudden activation of the high beam, failure of both headlights, severely impaired vision for driver, malfunction of all brake lights and malfunction of all indicator lamps. Recalls have been issued for automatic leveling of

Table 4.13: Worst case scenarios with ASIL for cab falling.

Occurrence	Case	ASIL
	Cab falling	
Sudden occurrence, no previous notice	Cab falling onto person	D
Previous notice/ stepwise loss	Cab falling onto person	C
Sudden occurrence, no previous notice	Cab tilting back and crushing person	C
Previous notice/ stepwise loss	Cab tilting back and crushing person	B

headlights not working and faulty placement of mirrors. Both these cases are regarding vehicles not fulfilling safety regulations. If there is any kind of previous notice (e.g. one of two lamps not working, warning lamp in dashboard) the defect will not be classified as safety related.

The situations sudden activation of high beams, failure of both headlights and impaired vision for driver can all cause head-on collisions or single accidents driving off road, which can lead to severe injuries. However, all of these problems are easily noticed and the driver can control the situation by coming to a safe stop before a collision occurs. As can be seen in Table 4.14, none of these situations are considered as safety related.

If all brake lamps fail to work as intended, this could possibly lead to a vehicle or cyclist hitting the rear of the vehicle if a reduction in speed is not noticed in time to come to a complete stop. The vehicle behind should keep a distance large enough to be able to avoid a crash if the lead vehicle starts braking, but might in lack of brake lights start braking too late to avoid a collision completely. However, as seen in Table 4.14, this case is not considered safety related.

If the indicator lamps on one or both sides of the truck fail to work as intended, it will not be clear for surrounding road users what the intended path is. The crash situations possible were therefore found to be: hitting vehicle turning off the road, hitting vehicle overtaking, hitting vehicle in intersection and hitting pedestrian crossing the road while truck is turning. However, all of these cases are considered as easy to control since both brake and steering systems are fully functioning. Furthermore, the indicator lamps should be checked every day, and if there is a malfunction, the vehicle should not be driven. Table 4.14 shows that all cases regarding failure of indicator lamps not are safety related.

4.5.5 Start and operation of vehicle

Start and operation of vehicle contains the following categories: no control of vehicle speed, unexpected movement of vehicle from standstill and unexpected moving of parts/components. The different sections uses different controllability tables, and these will therefore be presented separately in each section.

Table 4.14: Worst case scenarios with ASIL for impaired vision.

Occurrence	Case	ASIL
Impaired vision		
Sudden occurrence, no previous notice	Sudden activation of high beam	QM
Sudden occurrence, no previous notice	Failure of both headlights	QM
Sudden occurrence, no previous notice	Impaired vision for driver	QM
Sudden occurrence, no previous notice	Malfunction of all brake lights	QM
Sudden occurrence, no previous notice	Malfunction of all indicator lamps	QM

4.5.5.1 No control of vehicle speed

No control of vehicle speed includes situations regarding not being able to control vehicle speed not covered by loss of service brakes and sudden change of driving condition resulting in loss of control of the vehicle. The hazardous scenarios are found to be: unintentional acceleration, deceleration not as intended (too high), deceleration not as intended (too low), not possible to accelerate and not possible to accelerate or decelerate. Examples of defects are: brake pedal not behaving as intended, cruise control disengaged without notifying driver, water intrusion into engine, insufficient intensity of turbine blades and engine valves broken. All controllability values used in this section are found in Figures E.3 and E.4 in Appendix E.3.

Unintentional acceleration leads to a higher speed than the driver has intended, and has been found to lead to the following situations: a rear ending collision, hitting vehicle turning off the road, hitting vehicle in intersection, hitting pedestrian in crossing and single accident while turning. If there still is a possibility to brake, the situation is usually controllable even if the occurrence is sudden. If the acceleration on the other hand is sudden and the braking power is lost at the same time, it is very hard to control the situation, even at low speeds. There has historically been several recalls due to this issue. One example is a Toyota recall from 2009 because of an uncontrollable acceleration leading to crashes in high speed resulting in 52 deaths [66].

If the deceleration is lower than expected, the same crash scenarios as for unintentional acceleration are possible. The parking brake is still fully functioning, and can be used to increase the brake force. It is however harder to fully avoid a collision the higher the speed is. As can be seen in Table 4.15, this scenario is considered as safety related if the occurrence is sudden. If there is previous notice of some kind, the driver should apply more brake force or use the parking brake.

If too high deceleration occurs, the possible crash situations are identified as: rear ending from vehicle or cyclist. This is very similar to cases of *Unexpected braking* (see Section 4.5.3.2). In the same way as in this section, the situation is usually controllable, since the vehicle behind should keep a distance long enough to be able to brake and avoid a crash. Therefore, as can be seen in Table 4.15, the scenario is not considered as safety related.

A vehicle not being able to accelerate is in most situations not considered a safety related problem, but most likely a quality issue. However, if the defect occurs in one of the following situations, it can cause severe injuries: collision in intersection, head on collision (while overtaking) and truck struck by train. The first two collisions are often quite easy to control; if the truck not is able to drive out of a crossing, the warning lamps should be started to warn other drivers, and an overtaking situation should be aborted as soon as the problem is identified. If the truck cannot move from a train crossing, on the other hand, this situation is not possible to control. However, train crossings are not very common. Therefore, as can be seen in 4.15, not being possible to accelerate is considered to be safety related, but is not considered very severe.

Not possible to accelerate or decelerate can cause the same crash scenarios as too low deceleration. If both brake circuits are lost at the same time as acceleration is lost, the situation is very hard to control. It is possible to steer, but this is usually not sufficient to avoid a collision completely. This is therefore considered as safety related, and is rated as ASIL D (4.15). If the parking brake on the other hand is functioning, it can be used to reduced the speed of the vehicle. However, the higher the speed, the harder it gets to completely avoid an accident. Furthermore, even if there has been prior notice to the driver, the situation is considered as severe and hard to control, and is therefore rated as safety related. However, the driver has the possibility to engage the parking brake faster and by that is more likely to avoid the accident. This results in a slightly lower ASIL value, see 4.15.

Table 4.15: Worst case scenarios with ASIL for no control of vehicle speed.

Occurrence	Case	ASIL
Unintentional acceleration		
Sudden occurrence, no previous notice	Single accident while turning high speed	B
Previous notice	-	QM
Sudden occurrence, no previous notice	Single accident while turning med speed	D
Deceleration not as intended (too high)		
Sudden occurrence, no previous notice, with brake lights	-	QM
Deceleration not as intended (too low)		
Sudden occurrence, no previous notice	Single accident while turning med/high speed	C
Not possible to accelerate		
Sudden occurrence, no previous notice	Train crossing all speeds	A
Not possible to accelerate or decelerate		
Sudden occurrence, no previous notice, parking brake still functioning	Single accident while turning med/high speed	D
Previous notice, parking brake still functioning	Single accident while turning med/high speed	C
Loss of both brake circuits	Single accident while turning med speed	D

4.5.5.2 Unexpected movement of the vehicle from standstill

This section contains situations where the truck due to a defect unintentionally rolls away from standstill. The hazardous scenarios identified are: rolling away from standstill during normal parking and during maintenance/service. The malfunctions causing the rolling away from standstill can for example be air leakage on brake system, position of gear undetectable, delayed response in activation of parking brake, vehicle able to start with gear engaged and brake wire cut. The controllability values used in this section are found in Figures E.3 and E.4 in Appendix E.3 for cases in normal parking, and in Figure E.6 in Appendix E.5 for situations in maintenance.

If the vehicle rolls away when parked, the following crash scenarios can occur: hitting pedestrian, hitting parked vehicle and rolling away from parking in slope hitting vehicle in opposite direction. These scenarios occur in low speed, since the vehicle starts rolling from standstill, except if the vehicle starts rolling from a slope, where the speed can reach up to medium level (depending on slope). If the movement of the vehicle can not be noticed shortly after the stop, there is a risk that the driver has left the cab. In this case, the situation is not controllable for the truck driver. However, since the speed is low, the surrounding road users will probably have time to move out of the trajectory of the vehicle. If the movement occurs very shortly after the stop and the driver still is in the vehicle, the situation is usually quite controllable. Furthermore, if the defect in any way can be noted prior to the failure, the situation is usually considered controllable. However, if the driver has time to leave the vehicle, hazardous situations can occur and the situation is classified as safety related, as can be seen in Table 4.16.

If the vehicle is in maintenance or service, personnel are often in front or underneath the vehicle, which creates a large risk for someone being run over if the vehicle suddenly starts to move. As described in Section 2.2.2.4, several persons are killed in maintenance in Australia each year due to vehicles unexpectedly moving. If there, however, is a previous notice of the movement, maintenance personnel should have taking the correct measures to avoid an accident. As can be seen in Table 4.16, a sudden movement is classified as safety related with the highest ASIL possible.

Table 4.16: Worst case scenarios with ASIL for unexpected moving from standstill.

Occurrence	Case	ASIL
Unexpected movement from standstill (normal parking)		
Sudden occurrence, no previous notice, driver in vehicle	Rolling away forward from parking hitting pedestrian	A
Sudden occurrence, no previous notice, driver not in vehicle	Rolling away forward from parking hitting pedestrian	C
Previous notice/reduced function, driver in vehicle	-	QM
Previous notice/reduced function, driver not in vehicle	Rolling away forward from parking hitting pedestrian	A
Unexpected movement from standstill (maintenance)		
Sudden occurrence, no previous notice	Rolling away in maintenance	D
Previous notice/ reduced function	Rolling away in maintenance	QM

4.5.5.3 Unexpected moving of parts/components or auxiliary equipment during use, intervention, maintenance or repair

There are no cases regarding unexpected moving of parts found in the data studied. However, two hazardous scenarios were found with a HA analysis of the category: engine starting during maintenance/service, and engine hood falling down during maintenance/service. The controllability table used in this section are found in Figure E.6 in Appendix E.5.

If the engine starts or the hood falls during maintenance, the risk of someone being injured is large, but the severity of these injuries is usually quite low. As can be seen in Table 4.17, the situations are both considered to be safety related. However, only sudden cases are considered safety related, since proper measures to avoid injury should have been taken by the maintenance personnel if the defect could have been noticed prior to the failure.

Table 4.17: Worst case scenarios with ASIL for unexpected moving of parts.

Occurrence	Case	ASIL
Unexpected moving of parts		
Sudden occurrence, no previous notice	Engine starting unexpectedly during maintenance/service	B
Sudden occurrence, no previous notice	Engine hood unexpectedly falling during maintenance/service	B

4.5.6 Effects on the driver, passenger and maintenance personnel

This section contains quite varied categories, both defects that occur in maintenance and during driving. The categories presented are: fall from the vehicle during access, fall of occupants during driving, people trapped in vehicle, asphyxiation or intoxication, sudden change of driving condition, electric shock and misleading information. Since the scenarios are very varied, different controllability tables are used in the evaluations. The controllability table used will be presented in each section.

4.5.6.1 Fall from the vehicle during cab access, back of cab access, windshield access or similar

Within the studied data, there are no reported cases or recalls regarding fall from the vehicle during cab access. However, through a HA analysis of the category, the following hazardous scenarios are found: fall from low height (e.g. during cab access) and fall from medium to high height (e.g. top of cab). The controllability table used in this section can be found in Figure E.6 in Appendix E.5.

As described in Section 2.2.2.5, many serious injuries due to falling occur in work-related accidents each year in Australia. Around 22% of the cases reported (in total 3100) where due to poor design or placement of steps and ladders. If the step or ladder brakes when used, the situation is very hard to control and the person will most likely fall into the ground. Therefore, both fall from a low and a high height are found to be safety related and both rates with ASIL B (see Table 4.18). This is due to the fact that the higher fall has a higher severity rating compared to a lower fall, but it is less common with climbing on high parts of the truck. Furthermore, only sudden failures are considered as safety related. If the failure in some way can be noticed, the step or ladder should not be used or another grip can be secured.

Table 4.18: Worst case scenarios with ASIL for fall from vehicle during access.

Occurrence	Case	ASIL
Fall from vehicle		
Sudden occurrence, no previous notice	Fall from low height	B
Sudden occurrence, no previous notice	Fall from med/high height	B

4.5.6.2 Fall of occupants from the vehicle

Fall of occupants from the vehicle contains all defects where there is a risk for the occupant of a truck of falling from the vehicle while in motion. This section uses the controllability table found in Figure E.8 in Appendix E.7. The only case found that can lead to this situation is doors opening while driving. If an occupant of the vehicle falls out of the vehicle while in motion, the severity of the injuries can be very high. However, the situation is regarded to be very easy to control, since the driver will notice the problem as soon as it occurs and come to a safe stop. As can be seen in Table 4.19, the scenario found is not considered safety related.

Table 4.19: Worst case scenarios with ASIL for fall of occupants from vehicle.

Occurrence	Case	ASIL
Fall of occupants		
Sudden occurrence, no previous notice	Fall of occupant from vehicle when moving due to doors opening	QM

4.5.6.3 People trapped in vehicle

During normal driving, it is not considered hazardous if a door or roof hatch does not open. If a collision on the other hand occurs, it is vital for the driver to be able to exit the cab. The hazardous scenarios found are: both doors or the roof hatch does not open after crash, one door does not open after crash and occupant trapped in seat after crash. It is assumed that a crash has occurred in the assessment in this section, and the controllability table found in Figure E.7 in Appendix E.6 is used.

If at least one of the doors can be opened after a crash, the situation is usually controllable, since occupants can exit the cab or people can enter the cab to help. However, if the driver is stuck in the seat or both doors or the roof hatch cannot be opened when needed, the situation is very hard to control and can lead to fatalities if the occupants cannot get help in time. Therefore, the ASIL rating for these scenarios are found to be high (see 4.20). However, if there is any kind of previous notice, the defect is not considered as safety related.

Table 4.20: Worst case scenarios with ASIL for people trapped in vehicle.

Occurrence	Case	ASIL
People trapped in vehicle		
Sudden occurrence, no previous notice	Both doors or the roof hatch does not open after crash	D
Sudden occurrence, no previous notice	One door does not open after crash	B
Sudden occurrence, no previous notice	Trapped in seat after crash	D

4.5.6.4 Asphyxiation or intoxication

Sudden asphyxiation or intoxication is very rare with modern vehicles, due to a reduction of carbon monoxide with usage of catalytic converters, as described in Section 2.2.2.6. Therefore, the recalls within the data studied are mainly non-compliance with safety regulations due to for example problem with urea injection, faulty fuel injectors or faulty wiring of EGR. However, the following hazardous situations have been found: gases leaking into the cab and unintentional release of exhaust gases at standstill. The controllability table used in this section is found in Figure E.8 in Appendix E.7.

If exhaust gases leak into the cabin, the smell would most likely alarm the driver before any injuries can be obtained, and the situation is therefore considered as controllable in general. However, since carbon monoxide (CO), which is the component in exhaust gases that usually causes fatalities, is odorless in itself, it cannot be guarantied. If the gas is hard to notice by smell, the situation is hard to control and can lead to accumulation of CO in the body. Both CO and the other large component of exhaust gases called carbon dioxide can also cause long time problems such as inflammation and worsening of heart and lung disease. Therefore, these scenarios are seen as safety related, as can be seen in Table 4.21.

If there is an unintentional release of exhaust gases during standstill in a enclosed area (e.g. in maintenance or in a parking garage), the surrounding persons can obtain severe injuries. If the driver is not close to the truck, the problem is not noticed and cannot be controlled. This has been found to be a problem in maintenance, where several fatalities occur in the UK every year, as described in Section 2.2.2.6. As can be seen in Table 4.21, this scenario is considered safety related.

Table 4.21: Worst case scenarios with ASIL for asphyxiation or intoxication.

Occurrence	Case	ASIL
Asphyxiation or intoxication		
Sudden, easy to notice	Gases leaking into the cab	A
Sudden, hard to notice	Gases leaking into the cab	C
Sudden occurrence, no previous notice	Unintentional release of exhaust gases at standstill in limited area	A

4.5.6.5 Sudden change of driving condition resulting in loss of control of the vehicle

This category contains sudden changes of driving conditions resulting in the driver not being able to control the trajectory and possibly the speed of the vehicle. The category does not contain defects concerning engine failure, loss of steering or loss of brake systems. This is a very wide category which can contain for example: parts inside the cab falling onto the driver, sudden rupture of airbag and tire explosion or blow-out. The hazardous scenarios found when analyzing the category are: abrupt failure of part or function in cab resulting in driver distracted and not able to control vehicle, abrupt failure of part or function suddenly affecting trajectory of vehicle and steering suddenly not working as intended (less/more/opposite direction than intended). The controllability table used is found in Figure E.1 in Appendix E.1.

The crash scenarios found for these defects are: bicycle collision, hitting parked vehicle, hitting pedestrian, head-on collision and single accident. To be classified as safety related, the occurrence for the scenarios with sudden change of driving conditions has to be sudden/abrupt or hard to notice. These scenarios are hard to control, even in low speed, and the ASIL is determined to be high (see Table 4.22).

For cases where steering fails to work as intended, the situation is still regarded as fairly controllable, since the driver still has control over some parts of steering as well as braking. The situation is very similar to heavy steering found in the category *Loss of steering* (Section 4.5.1.1). If there is slight previous notice, the driver can possibly counteract the failure but might not be able to completely avoid an accident. The situation is therefore slightly controllable, but still considered safety related, see 4.22.

Table 4.22: Worst case scenarios with ASIL for sudden change of driving condition.

Occurrence	Case	ASIL
Abrupt failure of part or function in cab, driver distracted and not able to control vehicle/ Abrupt failure of part or function, suddenly affecting trajectory of vehicle.		
Sudden occurrence, no previous notice	Single accident high speed	D
Previous notice	Single accident high speed	C
Steering not working as intended (less/more/opposite direction than intended)		
Sudden occurrence, no previous notice	Meeting accident med/high speed, single accident high speed	C
Previous notice/ stepwise loss	Meeting accident med/high speed, single accident med/high speed	B

4.5.6.6 Electric shock

There are no cases regarding electric shock found in the studied data. However, defects such as chafing of unfused power cable, exposed wiring or incorrect battery wiring could possibly lead to electric shock. It is also possible that these defects can result in other Customer Safety Effects, for example fire, regarded more severe and would therefore be placed in a different category. The controllability table used is found in Figure E.6 in Appendix E.5.

The hazardous scenarios identified are: severe electric shock and small electric shock. As described in Section 2.2.2.7, almost every part of the body can be injured from electric shock. This has been found to be a large cause of mortality in workplace accidents. The final ASIL rating can be found in Table 4.23, where it is clear that both scenarios are considered safety related. However, several of the causes, such as chafed cables, are easy to notice and are therefore not regarded as safety related.

Table 4.23: Worst case scenarios with ASIL for electric shock.

Occurrence	Case	ASIL
Electric shock		
Sudden occurrence, no previous notice	Small electric shock	C
Sudden occurrence, no previous notice	Severe electric shock	D

4.5.6.7 Misleading information for drivers, passengers or maintenance personnel

The vehicle has several functions that informs the driver or maintenance personnel regarding status and problems of the vehicle and its functions and systems. This category contains all defects where the vehicle gives faulty information that can lead to accidents. Examples of recalls issued due to misleading information are: faulty indication lamp for ESP, inadequate color on lamp lenses for indicator lamp and speedometer indicating lower speed than the actual vehicle speed. However, all these recalls are due to non-compliance of safety requirements. The hazardous situations found are: no information at engine failure and faulty information gear. The controllability tables used are found in Figures E.3 and E.4 in Appendix E.3.

The possible crash scenarios if the engine fails are the same as if the vehicle cannot accelerate, see Section 4.5.5.1. The scenarios are: collision in intersection, head-on collision while overtaking and train hitting the truck. If the engine fails, it will be noticed by a reduction in speed and possibly noise or smoke. The information about this breakdown is therefore usually delivered to the driver regardless of if the lamps on dashboard are lit, and a hazardous situation will most likely not occur. However, if the driver for some reason is not able notice the failure, it is considered as safety related and rated with ASIL A, see Table 4.24.

Faulty information about which gear is engaged will while driving usually does not result in any hazardous situations. However, if a gear is engaged when the truck indicates parked position, this can result in the vehicle unintentionally moving from standstill. This would possibly result in the same accidents as for *Involuntary movement of the vehicle from standstill* in Section 4.5.5.2. The final ASIL determined can be seen in Table 4.24.

It is worth noticing that all hazardous situations found in this section also could be covered by the other sections mentioned above. This category mainly covers cases with non-compliance of safety requirements where no severe accidents usually occurs. However, since the cases described above are analyzed in the same way as the cases placed in the categories describing the resulting accidents, the resulting ASIL will be the same. Therefore, to simplify the categorizing for the analyst, this section is kept. Furthermore, new hazardous scenarios might be identified that should be categorized as misleading information.

Table 4.24: Worst case scenarios with ASIL for misleading information.

Occurrence	Case	ASIL
No information at engine failure		
Sudden occurrence, no previous notice	Train crossing all speeds/ Meeting accident high speed	A
Faulty information gear (normal parking)		
Sudden occurrence, no previous notice, driver in vehicle	Rolling forward from parking hitting pedestrian	A
Sudden occurrence, no previous notice, driver not in vehicle	Rolling forward from parking hitting pedestrian	C
Previous notice/reduced function, driver in vehicle	-	QM
Previous notice/reduced function, driver not in vehicle	Rolling forward from parking hitting pedestrian	A
Faulty information gear (maintenance)		
Sudden occurrence, no previous notice, driver not in vehicle	Rolling away in maintenance	D
Previous notice/ reduced function	Rolling away in maintenance	QM

4.5.7 Safety features

This section contains defects to all system that increases the safety of the vehicle. The cases are divided into three categories: failures in safety systems, failures in safety features and restraints not working. All hazardous situations described in these sections occur during or after a crash. The analysis is therefore based on the assumption that a crash has occurred, or is occurring. The controllability table found in Figure E.7 in Appendix E.6 is used for all evaluations.

4.5.7.1 Failures in safety systems leading to an unsafe operation of the vehicle

Safety systems are in this report defined as legally required safety systems, excluding restraint systems. A failure in a safety system will naturally result in a non-compliance of safety regulations and a recall or campaign is usually demanded. However, a failure in safety system can also lead to severe injuries, and the hazardous situations identified are: failure of airbag, failure of ESC and failure of other safety systems leading to unsafe driving conditions.

The first scenario, failure of airbag, can be divided into two parts: airbag not inflating when supposed in crash and airbag inflating falsely in crash (too early/late/quickly). Since the information, as described in Section 2.2.2.8, regarding airbags in trucks is limited, the same efficiency as in cars is assumed in the evaluation. If the failure of the airbag cannot be noted prior to the failure, it is not possible to control the situation. If the airbag is inflated suddenly when not in a crash, the situation is defined as *Sudden change in driving condition* as described previously. As described in Section 2.2.2.8, it has been found that the airbag reduces the number of fatalities by around 25%. It is however, slightly less efficient in low speeds than in medium to high speeds. Furthermore, it has also been shown that an impact of an inflating airbag can cause severe and fatal injuries. The final ASIL rating of an airbag failure is therefore found to be high, as can be seen in Table 4.25

As described in Section 2.2.2.8, ESC is most efficient in situations with a wet or icy road surface, even if the effectiveness in trucks not has been shown. If the ESC fails to work when intended, there is a large risk of the driver loosing control of the vehicle. The final ASIL for ESC failures can be seen in Table 4.25.

There are, as seen in Table 4.25, a few categories where the specific safety system not is defined. These are added to cover as many safety systems as possible, where the analyst has the chose the category most applicable to the current defect. This does, however, create a possibility of different analysts coming to different conclusions, and it is therefore reasonable to assume that the hazardous scenarios in the future has to updated with new safety systems, improvements or findings in studies.

Table 4.25: Worst case scenarios with ASIL for failure of safety system.

Occurrence	Case	ASIL
	Failure of safety systems	
Sudden occurrence, no previous notice	Airbag failure (i.e. not inflated during crash) high speed	D
Sudden occurrence, no previous notice	Airbag inflating too early/late/ too quickly high speed	D
Sudden occurrence, no previous notice	Failure of ESC, bad road condition	B
Sudden occurrence, no previous notice	Failure of ESC, good road condition	A
Sudden occurrence, no previous notice	Failure of other safety system leading to increased risk of fatality (commonly used/activated in crash)	D
Sudden occurrence, no previous notice	Failure of other safety system leading to increased risk injury (commonly used/activated in crash)	C
Sudden occurrence, no previous notice	Failure of other safety system leading to increased risk of fatality (fairly commonly used/activated in crash)	C
Sudden occurrence, no previous notice	Failure of other safety system leading to increased risk of fatality (fairly commonly used/activated in crash)	B
Sudden occurrence, no previous notice	Failure of other safety system leading to increased risk of fatality (not commonly used/activated in crash)	B
Sudden occurrence, no previous notice	Failure of other safety system leading to increased risk of fatality (not commonly used/activated in crash)	A

4.5.7.2 Failures in safety features leading to an unsafe operation of the vehicle

Safety features are in this report defined as non-regulatory systems to increase safety in a vehicle. A failure in one of these systems does not usually create a hazardous situation in driving.

Therefore, it is rare to issue a recall regarding failures in safety features, more commonly quality related service campaigns are demanded. For example, a faulty warning from lane change support will not create a hazardous situation. The potential safety related situations that can occur in this category are found to be: failure of ACC, failure of AEBS and failure of other safety feature.

If the ACC fails to reduce the speed of the vehicle when intended, the driver might end up in a rear ending collision. It is, however, according the product handbook, the drivers' responsibility to take over the control of the longitudinal acceleration if ACC fails. Yet, there is a risk that the driver in higher speeds does not have time to fully avoid an accident if the failure is noticed too late. Since the severity of a rear ending collision is low, the situation was found to not be safety related, as seen in Table 4.26. If the ACC unintentionally accelerates and the acceleration not is ended by applying the brakes, the problem is classified as *Unintentional acceleration*, see Section 4.5.5.1. If ACC or AEBS on the other hand suddenly brakes, the situation is classified as *Sudden braking*, Section 4.5.3.2. If the AEBS fails to brake when intended, a crash which possibly could have been avoided might occur. That is, it does not create a hazardous situation, it simply cannot avoid a hazardous situation. Since the AEBS system is not mandatory and cannot create a hazardous situation when malfunctioning, the defect is not classified as safety related (see Table 4.26). However, since the customers expect the system, it will most likely be classified as a quality problem and a service campaign issued.

The number of safety features in the vehicles are increasing fast. This might result in an increasing number of potential failures within this category. Many of these will most likely be software related, and these problems are supposed to be handled in the project work with ISO 26262. However, it is very likely that several scenarios will have to be added to this category in the future.

Table 4.26: Worst case scenarios with ASIL for failure of safety feature.

Occurrence	Case	ASIL
Failure of safety feature		
Sudden occurrence, no previous notice	ACC not braking when supposed to	QM
Sudden occurrence, no previous notice	AEBS not braking when supposed to	QM

4.5.7.3 Restraint or supplemental restraint system not working

The restraint systems of a truck are in this report defined as belts, seats and frame/collision structure, i.e. all systems ensuring the position and survival space of the occupants in a collision. These are vital for limiting the severity of the injuries in an accident. The hazardous scenarios has therefore been found to be: failure of seat belt, failure of part resulting in reduced crash performance and seat out of place.

If the occurrence of all scenarios above is sudden, there is no way for the driver to control the situation and reduce the severity of a collision. As described in Section 2.2.2.10, the seat belt has reduced fatalities of truck occupants with around 30% (up to 60% in light trucks). A failure of seat belt is therefore considered as a very severe safety related defect, as can be seen in Table 4.27. A too harsh tension of the seat belt can also cause injuries in case of crash, even if the risk of severe injuries is quite low. The problem is considered as safety related, but rated slightly lower than for a complete malfunction of the belt.

The seat is an important component of the restraint system. One of the functions is to ensure the position of an occupant in case of a collision, so that the airbags and seat belt can be as efficient as possible in reducing injuries. If the seat is out of place, there can for example be a risk for the driver getting a faulty contact point with the airbag. Therefore, the ASIL rating is found to be high, see Table 4.27.

Other components considered as restraint system are parts added to increase the crash performance of the vehicle, both for the occupants of the vehicle as well as occupants of other vehicles. These are all covered by the categories containing *Failure of part resulting in reduced crash performance* in Table 4.27. It is here the analysts who has to decide which category that bests describes the possible outcome of the defect, in the same way as in the category *safety systems*. There is a large probability that more scenarios will have to be added to this category in the future.

Table 4.27: Worst case scenarios with ASIL for failure of restraint system.

Occurrence	Case	ASIL
	Failure of restraint system	
Sudden occurrence, no previous notice	Failure of seat belt in crash	D
Sudden occurrence, no previous notice	Too harsh tension of seat belt in crash	B
Sudden occurrence, no previous notice	Seat out of place/seat failure in crash	C
Sudden occurrence, no previous notice	Failure of part resulting in slightly reduced crash performance (injuring truck occupant).	C
Sudden occurrence, no previous notice	Failure of part resulting in severely reduced crash performance (injuring truck occupant).	D
Sudden occurrence, no previous notice	Failure of part resulting in slightly reduced crash performance (injuring other road user), ex. underrun protection	C
Sudden occurrence, no previous notice	Failure of part resulting in severely reduced crash performance (injuring other road user), ex. underrun protection	D

4.6 Verification and usage of method

This section will shortly describe how to verify and apply the method to a potential safety related case.

As mentioned in Section 3.6 in the method chapter, it is hard to verify the model on recall cases, since the information is limited. Therefore, the method was applied to internal potential safety related cases. However, the method is intended to be applied during the process in decision of recall, and can only serve as a lessons learned when applied to old cases. Therefore, it is vital that the method is tested on new cases reported to Volvo Group in the future. If a value in one of the severity, exposure och controllability tables is changed, the affected tables for worst cases ASIL should be updated as well.

When a case is reported, the current analyst has to start with analyzing if the method should be applied, that is if the problem could be reoccurring in several vehicles, and if there are reported cases from the market and so on. When determined that this defect potentially is safety related, the analyst categorizes the defect into the most applicable CSE category, as well as the most applicable hazardous scenario. The occurrence of the defect is investigated, and the respective ASIL value is chosen. If no hazardous scenario could be applied to the defect, the analysts has to find all possible accident scenarios and determine the severity, exposure and controllability for these by using the tables for the affected truck model/s. The highest ASIL is found, and the table with the worst case ASIL-values is updated with the new hazardous scenario. All these tables for rating should be kept on an internal web page for easy access, and ensuring that all analysts within the company uses the same ratings. This process is described below:

If applicable hazardous scenario exist:

- Ensure that the method should be applied by studying root cause.
- Determine the affected fleet.
- Determine the occurrence of the defect.
- Find Customer Safety Effect
- Find applicable hazardous scenario.
- Find the worst case ASIL value for the scenario and occurrence in table for the specific Customer Safety Effect.

If applicable hazardous scenario does not exist:

- Ensure that the method should be applied by studying root cause.
- Determine the affected fleet.
- Determine the occurrence of the defect.
- Find Customer Safety Effect
- Determine a new hazardous scenario.
- Find the possible accident/crash scenarios. Use evaluations of similar hazardous scenarios as a guide.
- Use the tables for severity, exposure and controllability and find the respective values for each crash scenario.
- Determine the worst case ASIL value and save in the table with all ASIL ratings for the specific Customer Safety Effect.

A flow chart describing this procedure is available in Appendix F.

As for now, all ASIL values calculated are based on exposure for all truck models combined.

Before starting to use the method, the same calculations should be performed for all other truck models as well. However, this is easily done by finding the corresponding exposure value in the table for the different models as used in the evaluations for the models combined.

5

Discussion and conclusion

The final result of the research is a method to easily and quickly evaluate product defects. It is likely that more hazardous scenarios have to be added in the future, however since a large number of cases have been studied in the development of this method, it should be able to cover most possible cases occurring. The application of the method also results in a rating of the defects, which can be used in allocation of resources as well as serve as a motivation of decision.

The previous research within product safety is limited, due to the fact that most companies are reluctant to share the recall decision process and detailed recall information since this information can damage the brand. Therefore, there is to the author's knowledge no similar method used to address product defects. Due to the lack of research within the product defect area, the method is to a large extent based on the methods of ISO 26262 and FMEA. These methods were chosen mainly since both already are used within Volvo Group, and are more comprehensive than many other hazard analysis methods.

The method can be applied to any other truck brand by simply exchanging the data for usage of trucks, and to other markets by changing the road data. The injury data is assumed to be applicable to most European countries, as well as other similar markets such as the United States. It is also likely to assume that the usage and roads are quite similar for similar sized trucks, nevertheless, the exposure values might not be as precise for other markets or brands.

As described in Section 2.1, an increase in number of product defects has lead to product safety and liability being a growing focus area for many companies. The Swedish government has adopted a vision of zero fatalities in traffic, which naturally leads to stricter requirements. Volvo also has a vision of zero accidents with Volvo Group products. To achieve this, accidents due to product defects have to be minimized or extinguished. Furthermore, a large number of products recalled can be considered a sustainability issue. Taking for example the Takata airbag recall, were over 50 million faulty airbag components had to be exchanged [67]. This lead to an additional 50 million airbags that had to be produced due to a defect, which would not have been needed if the airbags were properly designed when first produced. The more recalls necessary, the more parts have to be produced (if not software related). Therefore, it is also important that the decisions and rating found in each evaluation are used as a lessons learned, to avoid similar defects in the future.

The database used for injuries on road was STRADA, which in itself contains several limitations. For example, there is a risk of missing some possible crash cases, since only police reported cases will be present in the data used. This can lead to for example single accidents not being reported if no personal injuries occur, which can lead to a skew in the severity of single accidents (i.e. the resulting injuries of single accidents seem more severe than they in reality are). It could therefore be beneficial to combine the police data with the hospital STRADA data as well as data from an insurance company, where all accidents leading to property damage and/or personal injuries can be found. However, these types of databases are very hard to access. Furthermore, the police reporting of injury level only accounts for the survivability of the patient, i.e. how life threatening the injuries obtained in the crash are. This is not always a good indication of how injured a person is in an accident. In for example rear ending crashes, it is found that the severity of the accidents are S1 in all speeds, which is very low. However, many of the occupants who have been in a rear ending crash obtain life long neck injuries, most commonly called whiplash injuries. A more suitable approach for defining the severity of the different crash types would have been to use the lifelong cost of the injury. This type of data is however not accessible today.

The injury data for maintenance/service is based on various studies from different countries, and also contains a problem with under reporting (e.g. if someone falls and is not injured, the accident will not be reported). Therefore a lot of assumptions had to be drawn to determine the severity of these accidents. If new studies covering more maintenance/service accidents were to be performed, the severity table should be updated. The severity in crash could be improved with more information regarding efficiency of safety systems, restraints and features, especially in trucks. Furthermore, the exposure in maintenance/service could also be updated if a more thorough study of how often the various tasks are performed. It could also be beneficial to divide the exposure into categories with the usage rather than the model, i.e. long haul, distribution and construction.

It is for some product defects hard to determine the most severe Customer Safety Effect. For example, if the vehicle faulty indicated that the parking brake is applied which leads to the vehicle rolling away, is this classified as misleading information or unexpected moving from standstill? As previously defined, the outcome of the defect and not the root cause should be used to determine the CSE. However, in cases where this is hard to determine (as the example above) the scenario can be found in both CSEs to avoid any mistakes when using the method. It has in these cases of course been verified that the same result will be achieved regardless of CSE used. Furthermore, if there is an uncertainty of which CSE to classify a certain defect as, the Section 4.5 in this report can serve as a guide.

The method has been hard to verify, since the information accessible in external recall cases is limited. Therefore, the method should be additionally verified by application on new potential defects reported to Volvo Trucks. The method should also give the same results when used by different analysts. However, this has not been tested within the scope of this project. This test would be beneficial to perform before starting to use the method. Furthermore, the method can only be used by someone with knowledge regarding the recall process as well as the effect of defects of certain parts is required, since some factors (e.g. applicable CSE and occurrence) has to be identified. However, it is assumed that all analysts at Volvo has this knowledge. Furthermore, there will always be uncommon cases that can not be covered by a generalized method. In these cases, the analyst has to evaluate the defect manually, but can use the method as support.

As stated above, the method should be updated if new hazardous scenarios are found, as well as if new data regarding severity, exposure or controllability is found. To ensure that all analysts uses the same tables, the latest updated version should always be kept on an internal website. Furthermore, all evaluated defects should be accessible for all analysts using the method to enable future comparing.

The level of automation in vehicles is increasing fast. This will most likely create new hazardous scenarios, as well as increase the exposure and reduce the controllability of several of the scenarios found in this report. It is therefore important that the method is updated with each added system and feature, especially systems controlling longitudinal and lateral acceleration of the vehicle.

In conclusion, the method developed fulfills the objective of simplifying the evaluation of product defects, as well as creating a rating for highlighting the level of issue for a potential recall. However, the method should be tested on new cases and possibly by several analysts before adapted into the recall process. Furthermore, it is important to keep in mind that the method and its rating only serve as a support in the recall process. A part can be recalled due to quality or safety regulations even if it is not classified as safety related. Furthermore, a part does not have to be recalled even if it is classified as safety related, but this rather serve as a recommendation to the decision makers. However, not only classifying a defect as safety related but also giving it a rating could enforce the recommendation further.

Finally, to simplify referring to the model, the name *Evaluation of Safety Defect Method* (ESDM) is proposed.

Bibliography

[1] Volvo Trucks, *Volvo FH - mediegalleri för FH*, http://www.volvotrucks.se/sv-se/trucks/volvo-fh-series/media-gallery.html.

[2] *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*, National Highway Traffic Administration (NHTSA), 2015.

[3] R. Schoenburg and T. Breitling, "Enhancement of active and passive safety by future pre-safe systems", in *19th ESV Conference*, National Highway Traffic Safety Administration (NHTSA), 2005.

[4] M. Distner, M. Bengtsson, T. Broberg, and L. Jakobsson, "City safety — a system addressing rear-end collisions at low speeds", in *Proc. 21th International Technical Conference on the Enhanced Safety of Vehicles*, National Highway Traffic Safety Administration (NHTSA), 2009.

[5] M. Avery and A. Weekes, "Autonomous braking systems and their potential effect on whiplash injury reduction", in *Conf. Neck Injuries in Road Traffic and Prevention Strategies*, National Highway Traffic Safety Administration (NHTSA), 2008.

[6] *European Accident Research and Safety Report 2013*, Volvo Trucks, 2013.

[7] S. Haefele and E. Westkämper, "Identification of Product Safety-relevant Tasks for Global Automotive Manufacturers", *Procedia CIRP*, vol. 17, pp. 326–331, 2014.

[8] H. Bates, M. Holweg, M. Lewis, and N. Oliver, "Motor vehicle recalls: Trends, patterns and emerging issues", *Omega*, vol. 35, no. 2, pp. 202–210, 2007.

[9] M. Eilert, S. Jayachandran, K. Kalaignanam, and T. A. Swartz, "Does it pay to recall your product early? An empirical investigation in the automobile industry", *Journal of Marketing*, vol. 81, no. 3, pp. 111–129, 2017.

[10] National Highway Traffic and Safety Adminstration (NHTSA), *Regulations*, https://www.nhtsa.gov/laws-regulations/fmvss.

[11] European Commission (EC), *Motor Vehicle Defects and Safety Recalls: What Every Vehicle Owner Should Know*, https://ec.europa.eu/growth/sectors/automotive/safety_en, 2017.

[12] FindLaw, *Auto Recalls: The Basics*, 2013. [Online]. Available: http://injury.findlaw.com/product-liability/car-defects-and-recalls-basics.html.

[13] National Highway Traffic and Safety Adminstration (NHTSA), *Safety in the automotive sector*, https://www-odi.nhtsa.dot.gov/recalls/recallprocess.cfm, 2011.

[14] The Vision Zero Initiative, *Vision zero*, http://www.visionzeroinitiative.com.

[15] *STRADA - Transportstyrelsens Olycksdatabas*, Regeringskansliet, Näringsdepatrementet, 2009.

[16] U. Björnstig, J. Björnstig, and A. Eriksson, "Passenger car collision fatalities", *Accident Analysis and Prevention*, vol. 40, pp. 158–166, 2008.

[17] P. Capella, "35 die, 1 Briton missing in Mont Blanc tunnel fire", *The Guardian*, 1999, https://www.theguardian.com/world/1999/mar/27/6.

[18] K. H. Digges, R. G. Gann, S. J. Grayson, M. M. Hirschler, R. E. Lyon, D. A. Purser, J. G. Quintiere, R. R. Stephenson, and ArchieTewarson, "Improving survivability in motor vehicle fires", in *Proceedings of INTERFLAM*, vol. 7, 2007, pp. 135–143.

[19] Å. Viklund, J. Björnstig, M. Larsson, and U. Björnstig, "Car crash fatalities associated with fire in sweden", *Traffic injury prevention*, vol. 14, no. 8, pp. 823–827, 2013.

[20] Health and Safety Executive Britain, *Injury statistics*, `http://www.hse.gov.uk/mvr/resources/statistics/injurystats.htm`, 1995.

[21] M. S. O'mara, D. G. Greenhalgh, and T. L. Palmieri, "Burn injury caused by motor vehicle use and repair", *Journal of burn care & research*, vol. 27, no. 6, pp. 901–904, 2006.

[22] A. López-Arquillos and J. C. Rubio-Romero, "Analysis of workplace accidents in automotive repair workshops in Spain", *Safety and health at work*, vol. 7, no. 3, pp. 231–236, 2016.

[23] ABC News Australia, *Bruce highway crash: Fatal four-vehicle collision closes major road near Maryborough*, `http://www.abc.net.au/news/2017-04-17/bruce-highway-fatal-traffic-crash/8448078`, 2017.

[24] "Work-related fatalities involving trucks, Australia 2003 to 2012", Safe Work Australia, Tech. Rep., 2014.

[25] *Preventing workers falling from trucks*, Office of Industrial Relations, Queensland Government, Queensland Australia, 2015.

[26] M. Vevelstad and I. Morild, "Lethal methemoglobinemia and automobile exhaust inhalation", *Forensic science international*, vol. 187, no. 1, e1–e5, 2009.

[27] M. A. Elliott, G. J. Nebel, and F. G. Rounds, "The composition of exhaust gases from diesel, gasoline and propane powered motor coaches", *Journal of the Air Pollution Control Association*, vol. 5, no. 2, pp. 103–108, 1955.

[28] G. A. Schmunk and J. A. Kaplan, "Asphyxial deaths caused by automobile exhaust inhalation not attributable to carbon monoxide toxicity: Study of 2 cases", *The American journal of forensic medicine and pathology*, vol. 23, no. 22, pp. 123–126, 2002.

[29] N. A. B. Mabahwi, O. L. H. Leh, and D. Omar, "Human health and wellbeing: Human health effect of air pollution", *Procedia-Social and Behavioral Sciences*, vol. 153, pp. 221–229, 2014.

[30] R. Fish, "Electric shock, part ii: Nature and mechanisms of injury", *The Journal of emergency medicine*, vol. 11, no. 4, pp. 457–462, 1993.

[31] R. C. Lee and M. S. Kolodney, "Electrical injury mechanisms: Electrical breakdown of cell membranes", *Plastic and Reconstructive Surgery*, vol. 80, no. 52, pp. 672–679, 1987.

[32] M. Capelli-Schellpfeffer, M. Toner, R. C. Lee, and R. D. Astumian, "Advances in the evaluation and treatment of electrical and thermal injury emergencies", *IEEE Transactions on Industry Applications*, vol. 31, no. 5, pp. 1147–1152, 1995.

[33] L. Evans, *Traffic safety.* 2004.

[34] A. Malliaris, J. DeBlois, and K. Digges, "Air bag field performance and injury patterns", SAE Technical Paper, Tech. Rep., 1996.

[35] J.-F. Huère, J.-Y. Foret-Bruno, G. Faverjon, *et al.*, "Airbag efficiency in frontal real world accidents", in *Proceedings: International Technical Conference on the Enhanced Safety of Vehicles*, National Highway Traffic Safety Administration, vol. 2001, 2001.

[36] M. Segui-Gomez, "Driver air bag effectiveness by severity of the crash", *American Journal of Public Health*, vol. 90, no. 10, p. 1575, 2000.

[37] G. Markkula, O. Benderius, K. Wolff, and M. Wahde, "Effects of experience and electronic stability control on low friction collision avoidance in a truck driving simulator", *Accident Analysis & Prevention*, vol. 50, pp. 1266–1277, 2013.

[38] A. Lie, C. Tingvall, M. Krafft, and A. Kullgren, "The effectiveness of electronic stability control (ESC) in reducing real life crashes and injuries", *Traffic injury prevention*, vol. 7, no. 1, pp. 38–43, 2006.

[39] C. M. Farmer, "Effect of electronic stability control on automobile crash risk", *Traffic injury prevention*, vol. 5, no. 4, pp. 317–325, 2004.

[40] W. G. Najm, M. D. Stearns, H. Howarth, J. Koopmann, and J. Hitz, "Evaluation of an automotive rear-end collision avoidance system", National Highway Traffic Safety Administration (NHTSA), Tech. Rep., 2006.

[41] M. Hoedemaeker and K. A. Brookhuis, "Behavioural adaptation to driving with an adaptive cruise control (ACC)", *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 1, no. 2, pp. 95–106, 1998.

[42] I. Isaksson-Hellman and M. Lindman, "Real-world performance of city safety based on Swedish insurance data", in *Vortrag gehalten auf der 24th International Technical Conference on the Enhanced Safety of Vehicles (ESV)*, vol. 8, 2015.

[43] M. Clayton, B. Helms, and C. Simpson, "Active prompting to decrease cell phone use and increase seat belt use while driving", *Journal of applied behavior analysis*, vol. 39, no. 3, pp. 341–9, 2006.

[44] A. Goudswaard, J. Nieboer, and E. Janssen, "Truck front underrun protection", *TNO Road-Vehicles Research Institute, Netherlands. IRCOBI*, 1991.

[45] R. Latifi, A. El-Menyar, H. El-Hennawy, and H. Al-Thani, "Rollover car crashes with ejection: A deadly combination—an analysis of 719 patients", *The Scientific World Journal*, vol. 2014, 2014.

[46] U.S. Roads, *Ejection from Vehicles Involved in Fatal Crashes Is Increasing*, http://www.usroads.com/journals/p/rilj/9808/ri980804.htm, 1998.

[47] C. Hayes, W. Conway, J. Walsh, L. Coppage, and A. Gervin, "Seat belt injuries: Radiologic findings and clinical correlation", *Radiographics*, vol. 11, no. 1, pp. 23–36, 1991.

[48] K. H. Digges, J. H. Morris, and A. C. Malliaris, "Safety performance of motor vehicle seats", SAE Technical Paper, Tech. Rep. 930348, 1993.

[49] K. Alhaifi, N. Alhaifi, and J. Alazemi, "Sled Damping Seat to Decrease Neck Injury in Rear-end Accident Experimental and Modelling", *Journal of Mechanical Engineering and Automation*, vol. 7, no. 1, pp. 16–22, 2017.

[50] J. Lambert and G. Rechnitzer, *Review of truck safety: Stage 1: Frontal, side and rear underrun protection*, 194. Monash University Accident Research Centre, 2002.

[51] M. Stamatelatos and H. Dezfuli, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Second Edition, National Aeronautics and Space Administration, Hanover, MD, 2011.

[52] M. Modarres, *Risk Analysis in Engineering - Techniques, Tools, and Trends*. Taylor and Francis Group, 2006.

[53] C. A. Ericson, *Hazard Analysis Techniques for System Safety*, Second Edition. Fredericksburg, Virginia: John Wiley and Sons Inc., 2016.

[54] C. S. Carlson, "Annual reliability and maintainability symposium", in *Understanding and Applying the Fundamentals of FMEAs*, 2014.

[55] *FMEA Handbook Version 4.1*, Fourth Edition, Ford Motor Company, Dearborn, MI, 2004.

[56] *Potential Failure Mode and Effects Analysis in Design*, Society of Automotive Engineers (SAE), 2002.

[57] *Functional safety - Essential to overall safety*, International Electrotechnical Commission (IEC), Geneva, Switzerland, 2015.

[58] *ISO 26262: Road vehicles - Functional Safety*, ISO, Geneva, Switzerland, 2011.

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

[60] L. Xing and S. V. Amari, *Fault Tree Analysis - Handbook of Performability Engineering*. Springer, 2008.

[61] SMHI, *Klimatdata*, https://www.smhi.se/klimatdata.

[62] "Report to congress on the large truck crash causation study", U.S. Department of Transportation, Tech. Rep., 2006.

[63] The Straits Times, *13-vehicle collision on SLE due to sudden braking by one driver*, `http://www.straitstimes.com/singapore/13-vehicle-collision-on-sle-due-to-sudden-braking-by-one-driver`, 2016.

[64] Today's Trucking, *Fifth wheels recalled following deadly crash*, `todaystrucking.com/fifth-wheels-recalled-following-deadly-crash`, 2015.

[65] "Safety alert: Securing raised tilt cabs", NT WorkSafe, Tech. Rep., 2013.

[66] S. M. Kirchhoff, *Unintended acceleration in passenger vehicles*. DIANE Publishing, 2010.

[67] National Highway Traffic and Safety Adminstration (NHTSA), *Takata recall spotlight*, `https://www.nhtsa.gov/equipment/takata-recall-spotlight`.

[68] T. Bedford and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge, UK: Cambridge University Press, 2001.

[69] United States Nuclear Regulatory Commission, *Probabilistic Risk Assessment (PRA)*, `https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html`, 2016.

[70] M. Stamatelatos, *Probabilistic Risk Assessment (PRA)*, National Aeronautics and Space Administration, 2000.

[71] *FAA System Safety Handbook*, Federal Aviation Administration, 2000.

[72] Z. Penga, Y. Lyub, A. Miller, C. Johnson, and T. Zhao, "Risk Assessment of Railway Transportation Systems using Timed Fault trees", *The Open Transportation Journal*, vol. 5, pp. 34–44, 2011.

[73] A. Berrado, E.-M. El-Koursi, A. Cherkaoui, and M. Khaddour, "A Framework for Risk Management in Railway Sector: Application to Road-Rail Level Crossings", *Quality and Reliability Engineering*, vol. 32, no. 1, pp. 181–194, 2016.

[74] *Department of Defense Standard Practice - System Safety*, Fifth Edition, Department of Defense, 2012.

[75] "Factors related to fatal single-vehicle run-off-road crashes", National Highway Traffic Safety Administration (NHTSA), Tech. Rep., 2009.

[76] U. Björnstig, J. Björnstig, and A. Eriksson, "Passenger car collision fatalities-with special emphasis on collisions with heavy vehicles", *Accident Analysis & Prevention*, vol. 40, no. 1, pp. 158–166, 2008.

[77] A. Krusper, *Structural interaction between vehicles. An investigation of crash compatibility between cars and heavy goods vehicles*. Chalmers University of Technology, 2014.

[78] M. Distner, M. Bengtsson, T. Broberg, and L. Jakobsson, "City safety - a system addressing rear-end collisions at low speeds", in *Proc. 21st International Technical Conference on the Enhanced Safety of Vehicles*, 2009.

[79] M. Shin, K. Park, and G. Park, "Occupant analysis and seat design to reduce neck injury from rear end impact", *International journal of crashworthiness*, vol. 8, no. 6, pp. 573–581, 2003.

[80] L. Jakobsson, T. Broberg, H. Karlsson, A. Fredriksson, N. Gråberg, C. Gullander, and M. Lindman, "Pedestrian airbag technology–a production system", in *23rd International Technical Conference on the Enhanced Safety of Vehicles (ESV) National Highway Traffic Safety Administration*, 2013.

A

Customer Safety Effects

This appendix contains a figure of all customer safety effects and the respective subcategories, see Figure A.1.

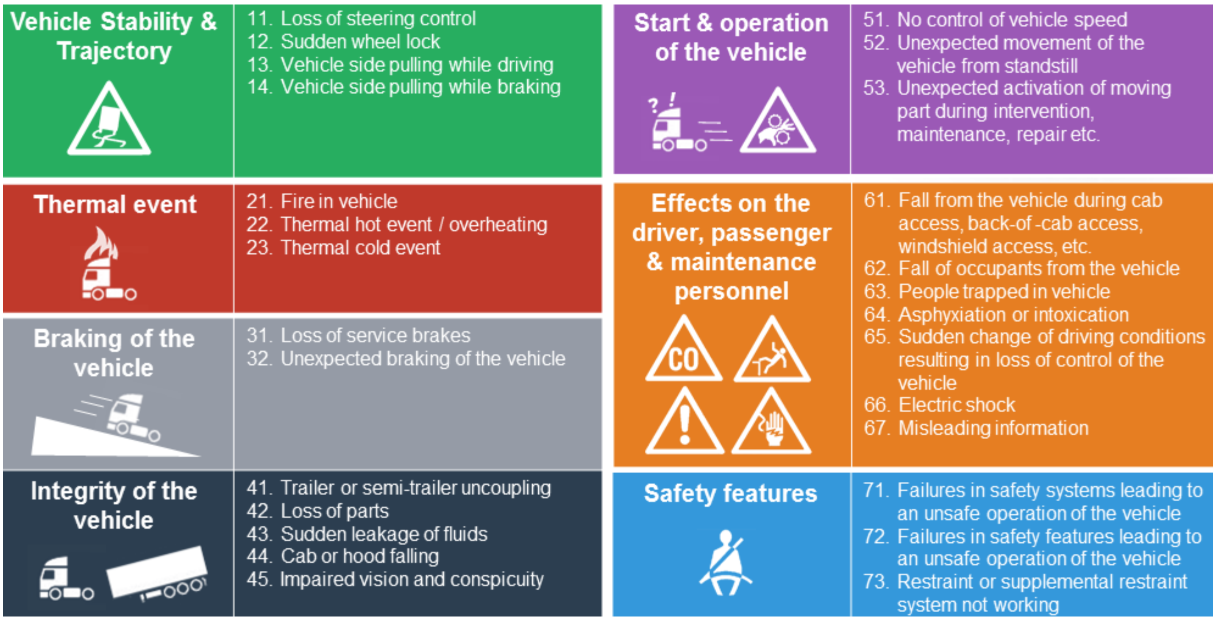


Figure A.1: Customer Safety Effects as defined within Volvo Trucks.

B

Risk analysis in other sectors

Risk analysis is, as described before, a vital part of all product development processes. In this section, the method for risk analysis in the sectors nuclear, aerospace, aviation, railway and military will be described.

B.1 Probabilistic Risk Assessment - PRA

Probabilistic Risk Assessment (PRA) is an analysis method to evaluate risks regarding complex technological systems. PRA is used in many fields, for example the chemical process sector, the nuclear sector and the aerospace sector [68]. Risk according to PRA is divided into two quantities:

1. Magnitude/severity.

2. Likelihood/probability

Probabilistic Risk Assessment usually answers three basic questions:

- What are the initiating events?

- How severe are the potential consequences?

- What is the probability of the consequence to occur?

According to Bedford and Cooke, risk can be defined as a set of scenarios which each has a probability and a consequence [68]. The PRA can be solved using for example a Fault Tree Analysis.

B.1.1 PRA in the nuclear sector

The Nuclear Regulatory Commission (NRC) has since 1974 used PRA to identify risks and their respective consequences and likelihood of occurrence. The assessment determines strengths and weaknesses of the design and operation of a nuclear power plant. The PRA in the nuclear sector can estimate three levels of risk [69]:

- Level 1 - Estimates frequency of accident causing damage to the nuclear reactor core.
- Level 2 - Estimates frequency of accidents that releases radioactivity from nuclear power plant.
- Level 3 - Estimates the possible consequences regarding injury for the public and damage to the environment.

B.1.2 PRA in the aerospace sector

Early in the Apollo program, National Aeronautics and Space Administration (NASA) relied on Hazard Analysis and FMEA for system safety assessment, while the nuclear industry adopted the PRA. However, after the Challenger accident in 1986, criticism was directed towards the work with HA and FMEA, and PRA gained significant momentum at NASA [51].

PRA quantifies ”risk metrics”, which are the measures in a decision model, for example the frequency of occurrence or probability of consequences. For NASA, these risk metrics can be probability of loss of crew or probability of mission failure etc. [51].

A typical PRA process within NASA can be:

- Define and select the objective and consequences of the risk assessment.
- Familiarization of the system.
- Identify initiating events.
- Model the accident scenario using for example FTA.
- Perform uncertainty and sensitivity analyses.

When the PRA is completed, the lead contributors to risks are identified and an importance ranking is created [70].

B.2 Risk analysis in the aviation sector

The aviation sector uses the standard FAA System Safety, determined by Federal Aviation Administration (FAA). The standard consists of a five step approach for risk analysis; planning, hazard identification, analysis, assessment and decision. Both elements of risk, hazard severity and likelihood of occurrence are investigated according to Figure B.1 and B.2. The values from these evaluations are combined in a table similar to that of the ASIL classification in ISO 26262. The result from this table is the assessed risk, also referred to as Hazard Risk Index (HRI) [71].

Catastrophic	Results in multiple fatalities and/or loss of the system
Hazardous	Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: Large reduction in safety margin or functional capability Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (1) Serious or fatal injury to small number of occupants of aircraft (except operators) Fatal injury to ground personnel and/or general public
Major	Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be – Significant reduction in safety margin or functional capability Significant increase in operator workload Conditions impairing operator efficiency or creating significant discomfort Physical distress to occupants of aircraft (except operator) including injuries Major occupational illness and/or major environmental damage, and/or major property damage
Minor	Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Include Slight reduction in safety margin or functional capabilities Slight increase in workload such as routine flight plan changes Some physical discomfort to occupants or aircraft (except operators) Minor occupational illness and/or minor environmental damage, and/or minor property damage
No Safety Effect	Has no effect on safety

Figure B.1: Severity definitions for FAA process.

Probable	Qualitative: Anticipated to occur one or more times during the entire system/operational life of an item. Quantitative: Probability of occurrence per operational hour is greater that 1 x 10^{-5}
Remote	Qualitative: Unlikely to occur to each item during its total life. May occur several time in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1 x 10^{-5}, but greater than 1 x 10^{-7}
Extremely Remote	Qualitative: Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1 x 10^{-7} but greater than 1 x 10^{-9}
Extremely Improbable	Qualitative: So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1 x 10^{-9}

Figure B.2: Likelihood of occurrence definitions for FAA process.

B.3 Risk analysis in the railway sector

Safe systems are an essential requirement of a railway transportation system. Risks in the railway system can be derailment, collision and fire [72]. The most common risk analysis method in railway transportation engineering is FMEA, and uses for example FTA for hazard identification. The risk analysis consist of estimation of frequency and consequence of the event [73].

B.4 Risk analysis in the military sector

The Department of Defence (DoD) has created a standard for system safety named MIL-STD-882E used in the military in the US [74]. The system safety process of this standard contains eight elements, presented in logic sequence in Figure B.3.

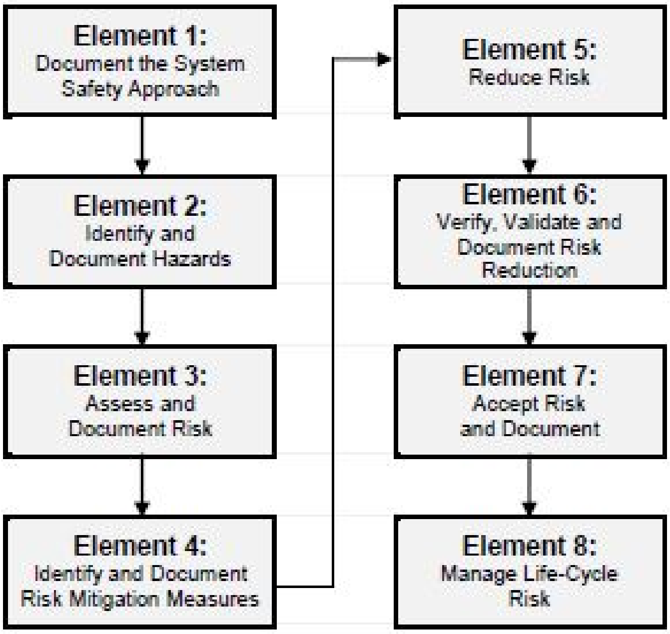


Figure B.3: Eight elements of the system safety process in the military sector.

Element three focuses on the methodology of analyzing the risks. The severity is determined for a given hazard at a given point in time and is ranked on a scale from 1-4, where 1 is Catastrophic and 4 is Negligible.

The probability at the same point in time is determined by assessing the likelihood of occurrence of a mishap. It is graded on a scale from A-F, where A is Frequent and F is Eliminated.

If possible, quantitative data is used to define the rate of occurrence. The probability level cannot be lowered by training, warning or caution but only design changes. A Risk Assessment Matrix is formed, where probability and severity together creates a Risk Assessment Code (RAC). The Risk Assessment Matrix is seen in Figure B.4.

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure B.4: Risk Assessment Matrix.

C

Data for severity

C.1 Relations between police and hospital data in STRADA

There are two databases in STRADA; one collected by the police and one collected by the hospitals. The two databases are separate, but a case can be found in both databases by identification numbers. The relation between the two databases can be found in Figure C.1

C.2 Crash categories

To be able to study different mechanisms and injuries in crashes, the crashes are usually divided into different categories according to occurrence or road users involved. This section aims to describe the categories used in STRADA (with one addition), to clarify some decisions and conclusions in the creation of the method. Most of the crashes are described according to the authors definition.

C.2.1 Single vehicle crashes (S)

A single vehicle crash is a collision with only one vehicle involved. This category includes running off road, roll-overs, hitting stationary objects or hitting moving objects (not vehicles or humans). If another person, not occupant in the truck, is in risk of being injured during the crash, it will not be considered a single vehicle collision, even if the person is not in a vehicle. A common cause for vehicle running off road is operator error, for example in form of intoxication, fatigue, inattention or distraction. Other factors contributing to the risk of a driver running off road can be related to weather, roadway and vehicle [75]. The single vehicle crashes are in this report divided into driving on a straight road and driving off road (S 1, 3), and driving off road while turning (S 2, 4).

C.2.2 Meeting accident/head-on collision (M)

A head-on collision is a collision where two vehicles collide front to front, with more or less overlap. Head-on collision is a frequent multi-vehicle collision type [76]. Even if frontal collisions between heavy duty vehicles and cars are rare compared to frontal crashes between two cars, the outcome is usually much more severe. This is due to the crash incompatibility, which depends on mass, stiffness and geometry [77]. If a passenger car collides head on with a 65-ton truck when both are travelling in 70 km/h, the car will be exposed to a theoretical change of velocity of 137 km/h. This leads to the occupants of the vehicle being exposed to an extremely high deceleration force, equivalent to a fall from 70 m, an impact which is almost impossible to survive [76]. Another issue which have been a result of head-on collisions between a truck and a car is the car under-running the truck, which can lead to very severe injuries. Therefore, the Front Underrun Protection (FUP), which reduces the risk of this scenario, is now a mandatory equipment for heavy duty trucks in many countries [77].

Sideswipe collisions are where the side of vehicles from two opposing directions touch. The difference from a full frontal collision is that the impact mainly is in the side of the vehicles. However, there is no difference between sideswipe collisions or head-on collisions in STRADA. Both head on collisions and sideswipe collisions are commonly caused by one of the vehicles drifting out of its lane and on to the opposing vehicles side of the road.

C.2.3 Rear-end collision (U)

A rear-end collision is a crash where a vehicle drives in to the rear of the vehicle in front. Rear-end collisions account for a large amount of crashes every year. Most rear-end collisions occur at low speeds, up to 30km/h, in city traffic. A common injury from rear-end collisions is soft-tissue neck injury for occupants of both vehicles [78]. Rear-ending accidents at all speeds does not usually result in severe or fatal injuries, nevertheless, the neck injury can create lifelong suffering for the patient in the form of a so called *Whiplash* injury [79].

C.2.4 Collision while overtaking (O)

Collision while overtaking includes both the side of the truck hitting the side of another vehicle, as well as the side of another vehicle hitting the side of the truck. However, it does not contain overtaking accident resulting in a head-on collision. If the truck hits the side of another vehicle, there is a risk that one of the vehicles is pushed either off the road or in to the center of the road (crash barrier or over to the lanes in the opposing direction). If a small vehicle hits the side of a truck, there is a risk for so called under-riding, where the vehicle fully or partly is stuck underneath the trailer of the truck. This type of collision usually leads to very severe injuries an possibly even fatality. It is becoming more common with underrun protections to reduce the severity of the side collisions, and most overtaking collisions will today not result in fatal injuries.

C.2.5 Crash with vehicle in intersection (K)

A crash in an intersection is a collision between two or more vehicles in any kind of intersection or crossing. Intersections are most common in urban areas, but does also occur in rural areas to some extent. Since vehicles in the intersection are turning, driving straight and meeting vehicles from several different directions, the point of contact between the vehicles can be almost anywhere on the vehicle. Therefore, the injury outcome of the crash can be very varied depending on the scenario. However, the speed in a crossing, especially without traffic lights, should be lowered compared to the rest of the current road.

C.2.6 Crash with vehicle about to turn off the road (A)

On urban and rural roads, vehicle about to turn left might be at standstill in the center of the lane. This can lead to a vehicle behind hitting this vehicle. The category also contains crashes with a vehicle turning over the opposing lane being hit by a vehicle travelling in the opposite direction.

C.2.7 Collision with unprotected road user (F, C)

This section is in STRADA divided into accidents with pedestrians and accidents with cyclists, however here described together called Vulnerable Road User (VRU). VRUs are unprotected and usually travels in a lower speed than other road users. This makes them much more vulnerable than occupants of another vehicle, even in very low speeds. However, many new innovations and systems have been implemented in cars to improve especially pedestrian safety during the last decade. For example, improvements of the front of the vehicle and pedestrian airbags have been added to many new vehicles [80]. However, none of these have been implemented in trucks.

C.2.8 Collision animal (W, V1)

Collision with animal contains accidents with all different types of animals. Depending on the animal, the resulting severity can be very varied. A collision with for example an elk or a wild boar can result in very severe personal injuries. A collision with a rabbit on the other hand, will most likely not result in any injuries. Furthermore, cases with accidents with small animals which does not cause any injuries or property damage will most likely not be reported.

C.2.9 Crash with parked vehicle and crash during reversing (V5, V6)

Crashes occurring during reversing are common in parking areas and usually occurs in very low speed. Pedestrians and cyclists hit by a reversing vehicle are not covered by this section, but is included in the category *Collision with unprotected road user*. Crashes with parked vehicle are most common in urban areas, where parked vehicles are common. Most of the time, there is no occupant in a parked vehicle, but this situation can of course occur.

C.2.10 Crash with tram or train (J5, J8)

A crash with a tram is any collision between a truck and a tram. This collision can only occur in the few cities in Sweden that actually have trams, for example Göteborg, Norrköping and Stockholm. The speed of the trams is usually relatively low, and trams often driven in a separate road section not occupied by vehicles.

A crash with a train can occur in any train crossing. However, the risk of accidents with trains is today lowered by traffic lights and/or a bar before the crossing. A train hitting a truck usually leads to very severe injuries to the truck occupants, since the weight and speed of the train is high, and the possibility to brake is very limited.

C.2.11 Jackknifing (Not a category in STRADA)

When an articulated vehicle folds, the event is called *jackknifing*. Jackknifing usually occurs when different amounts of braking occurs on the different axles. A jackknifing event can have several outcomes; it can cause an accidents with other road users, as well as cause the occupants of the truck to be crushed if the cab is pushed towards the trailer. It can be caused by for example bad road conditions and improper braking. Jackknifing is becoming less common due to several safety systems which reduces the risk of an uncontrollable situation.

C.3 Severity data for accidents not occurring during driving

Since the STRADA data not is applicable to accidents which does not occur during driving on public roads, data to base the severity rating regarding the other situations had to be collected. This section contains data additional to the data presented earlier in the report used to determine this rating. However, as mentioned before, the difference between this data and the data found in STRADA is that minor or no injuries are not reported and therefore not found in this statistics. Therefore, these exact numbers have not been used in any evaluations, but rather serves as an indication of severity as well as occurrence.

Figure C.2 contains information regarding causes of fatalities and injuries in motor vehicle repair (MVR) in the UK. The study was performed by the *Health and Safety Executive*, which is a governmental initiative in the UK. The study contains statistics from MVR accidents over ten respective three years [20].

Figure C.3 describes the injuries obtained by falling from a truck. The data was collected by *WorkSafe*, a governmental initiative in Australia in an attempt to *"provide information [...] to enable businesses to better manage their own fall risks"* [25].

Ejection of a occupant can be a severe result of a crash. The risk of ejection it 15.38 times greater for unbelted persons than for those who have fastened their seat belt. Ejection have been found to occur 1.44 times more often in a truck than in a car. Number of fatalities during crashes involving ejections can be seen in Figure C.4. All information regarding ejection is collected by *Road Injury Prevention and Litigation Journal* in the US [46].

Safe work Australia is a governmental initiative in Australia who have gathered information regarding work-related fatalities involving trucks in Australia between the years 2003 to 2012 [24]. This data is gathered in Figures C.5, C.6 and C.7.

C.4 Severity data from STRADA

In this section, all data used from STRADA will be presented. The data is divided by the previously mentioned crash categories, and each table will show the level of injury in percentage divided between the different speed limits.

C.5 Tables of Severity divided by speed

In this section, the final severity tables for low and medium speeds are presented. The severity table for high speed is presented in Figure 4.1 in Section 4.2.

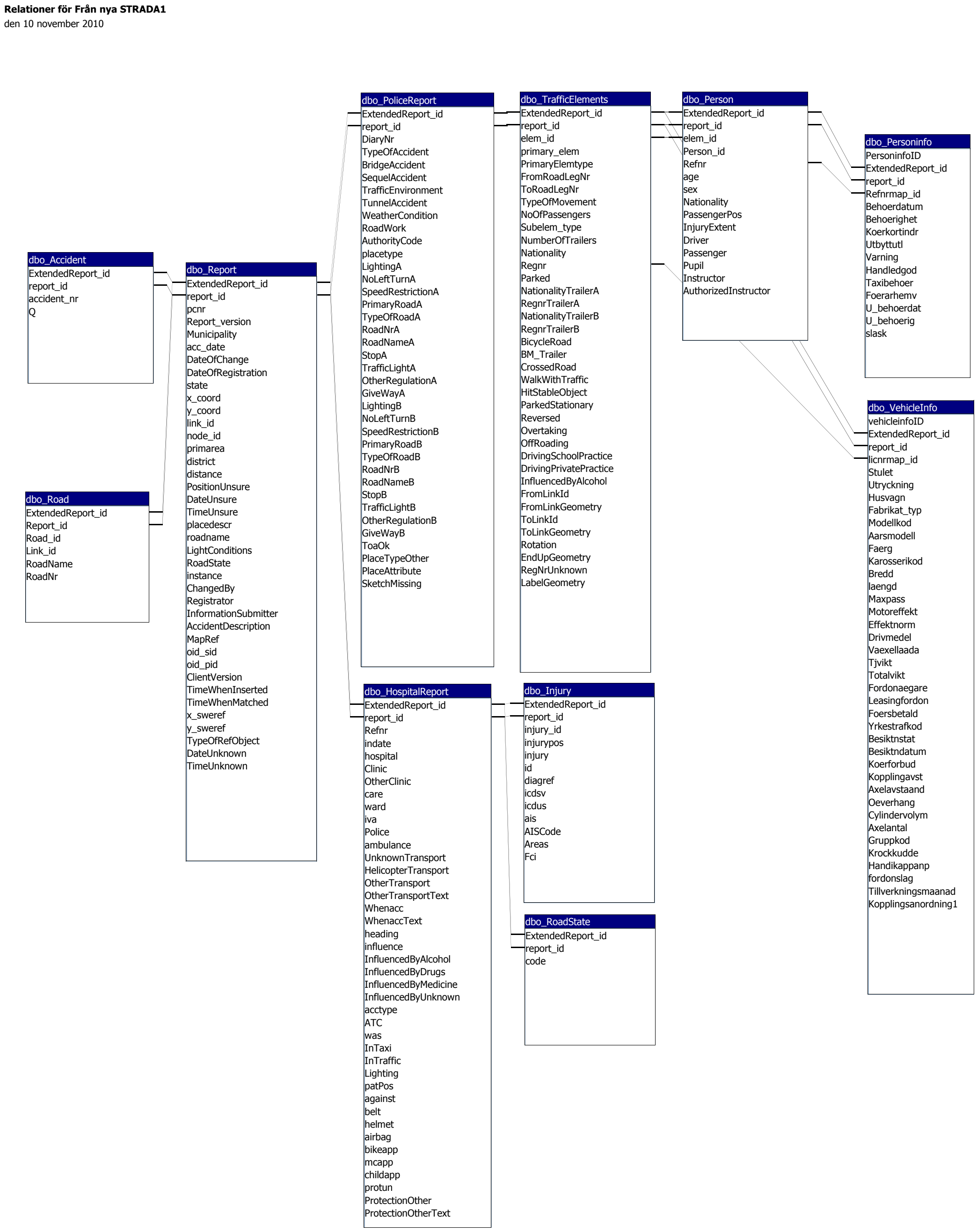


Figure C.1: Relations between police data and hospital data in STRADA.

Type of fatal injury to workers in MVR uk 10 years	
Hit by moving object/collapsing/overturning	24%
Hit by moving vehicle	20%
Fall from height	8%
Fire / explosion	8%
Contact with harmful substance	6%
Other known kind	13%
Unspecified or unknown kind	8%
Electricity	3%
Slip or trip	3%
Hit against a fixed object	3%
Drowned or asphyxiated	3%
Contact with moving machinery	1%
Non-fatal injury 3 years	
Lifting and handling injuries	33%
Slip, trip, fall same level	21%
Struck by object	16%
Fall from height	7%
Struck against	4%
Struck by moving vehicle	3%
Contact with machinery	3%
Exposure to harmful substance	2%
Exposed to fire	1%
Trapped by something collapsing	1%
All other kinds and unknown	8%

Figure C.2: Types of injuries in Motor Vehicle Repair in the UK.

Injuries from falling from truck Australia	
Poorly designed ladders or steps	14.4%
Climbing at height onto the trailer to secure loads	13%
Climbing on the top of the trailer where there are unprotected openings	10%
Ladders or steps unsafely located on the	8%
Climbing at height up or between ramps and crates on the trailer access loads	8%
Climbing at height onto the trailer or carrier to load or unload	6.5%
Jumping down from the trailer	6.5%
Using tyres as steps to climb onto the trailer/walking in trailers that have become slippery with contaminants	5%

Figure C.3: Reasons behind injuries obtained from falling from a truck in Australia.

Ejection of occupant in fatal crashes US	Ejected	Not Ejected
Belted	2.5%	97.5%
Unbelted	29.4%	70.6%

Figure C.4: Ejection of occupants during fatal crashes in the US.

Fatalities for truck drivers in Australia	
Vehicle collision	72%
Being hit by moving objects	11%
Being trapped between stationary and moving objects	6%
Being hit by falling objects	4%
Falls from a height	4%
Other	4%

Figure C.5: Cause for fatalities for truck drivers in Australia.

Truck related worker fatalites in repair/maintenance Australia	
Truck occupants	**58%**
Vehicle collision	2%
Being hit by moving objects	24%
Being trapped between stationary and moving objects	13%
Being hit by falling objects	7%
Falls from a height	9%
Other type of incident	4%
Workers in other vehicles	**7%**
Vehicle collision	0%
Being hit by moving objects	7%
Other type of incident	0%
Worker on foot	**35%**
Being hit by moving objects	15%
Being trapped between stationary and moving objects	13%
Being hit by falling objects	4%
Other type of incident	4%

Figure C.6: Cause for fatalities for truck drivers in maintenance/repair in Australia, divided by occurrence.

Truck-related fatalities involving loading/unloading	
Hit by moving vehicle	37%
Hit by own vehicle	13%
Pedestrian worker hit by truck	13%
Truck driver hit by other vehicle	11%
Hit by falling cargo	17%
Fall from vehicle	13%
Loading plant onto tray of truck	8%
Vehicle overbalanced	6%
Trapped in lifting eqipment	5%
Hitting overhead power lines	4%
Hit by falling ramp	3%
Explosion	3%
Other	5%
Truck-related worker fatalities involving repair/maintenance	
Working on truck when it moved	25%
Crushed while inside truck body	24%
Working on truck when hit by another truck	16%
Tyre incidents	9%
Working on cars when hit by a truck	7%
Falls from trucks	5%
Crushed when jack failed	5%
Other	7%

Figure C.7: Cause for fatalities for truck drivers in maintenance/repair and during loading/unloading in Australia.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	2,6%	53,8%	39,3%	4,3%
50-70 km/h	0,8%	8,4%	52,2%	31,5%	7,1%
>=80 km/h	2,8%	12,3%	51,6%	24,5%	8,8%

(a) Category A, vehicle hit while turning off road.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	4,4%	48,1%	43,0%	4,4%
50-70 km/h	1,8%	10,4%	40,4%	37,9%	9,5%
>=80 km/h	18,2%	13,6%	18,2%	31,8%	18,2%

(b) Category C1, meeting accident between bicycle and truck.

Figure C.8: STRADA data: injury level vs. speed limit category A and C1.

Injury speed %	1	2	3	4	9
<=40 km/h	0,4%	5,9%	45,1%	39,7%	8,9%
50-70 km/h	3,2%	9,9%	39,0%	36,1%	11,8%
>=80 km/h	7,2%	11,2%	36,8%	32,8%	12,0%

(a) Category C2, overtaking or rear ending accident between bicycle and truck.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	5,0%	50,0%	40,0%	5,0%
50-70 km/h	2,5%	12,0%	39,0%	36,5%	10,0%
>=80 km/h	0,0%	6,7%	46,7%	33,3%	13,3%

(b) Category C3, accident between bicycle and truck driving in the same direction, one is turning.

Figure C.9: STRADA data: injury level vs. speed limit category C2 and C3.

Injury speed %	1	2	3	4	9
<= 40 km/h	0,0%	20,0%	40,0%	30,0%	10,0%
50-70 km/h	0,6%	13,6%	38,3%	35,2%	12,3%
>= 80 km/h	0,0%	0,0%	0,0%	0,0%	0,0%

(a) Category C4, accident between bicycle and truck driving in opposite direction, one is turning.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	0,0%	61,5%	15,4%	23,1%
50-70 km/h	2,7%	13,4%	37,2%	34,9%	11,7%
>=80 km/h	0,0%	50,0%	0,0%	50,0%	0,0%

(b) Category C5, accident in crossing, both bicycle and truck driving straight.

Figure C.10: STRADA data: injury level vs. speed limit category C4 and C5.

Injury speed %	1	2	3	4	9
<=40 km/h	1,8%	14,0%	36,8%	33,3%	14,0%
50-70 km/h	1,8%	13,4%	38,9%	35,7%	10,3%
>=80 km/h	0,0%	6,7%	46,7%	40,0%	6,7%

(a) Category C6, accident in crossing, one of the bicycle or the truck is turning.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	0,0%	50,0%	0,0%	50,0%
50-70 km/h	0,0%	0,0%	40,0%	10,0%	50,0%
>=80 km/h	0,0%	0,0%	0,0%	0,0%	0,0%

(b) Category C7, truck hits bicycle at standstill.

Figure C.11: STRADA data: injury level vs. speed limit category C6 and C7.

Injury speed %	1	2	3	4	9
<=40 km/h	2,0%	15,9%	33,8%	41,7%	6,6%
50-70 km/h	5,2%	13,9%	33,3%	36,2%	11,4%
>=80 km/h	13,2%	19,1%	7,4%	48,5%	11,8%

(a) Category F1256, pedestrian crossing the road when hit by a truck driving straight.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	10,0%	40,0%	30,0%	20,0%
50-70 km/h	4,9%	15,9%	35,4%	30,5%	13,4%
>=80 km/h	14,3%	14,3%	21,4%	42,9%	7,1%

(b) Category F34, pedestrian walking next to the road when hit by a truck.

Figure C.12: STRADA data: injury level vs. speed limit category F1256 and F34.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	18,2%	36,4%	45,5%	0,0%
50-70 km/h	4,0%	11,0%	44,0%	38,0%	3,0%
>=80 km/h	0,0%	0,0%	0,0%	0,0%	0,0%

(a) Category F78, pedestrian crossing the road when hit by a truck turning.

Injury speed %	1	2	3	4	9
<=40 km/h	6,7%	6,7%	33,3%	46,7%	6,7%
50-70 km/h	6,9%	5,6%	41,7%	27,8%	18,1%
>=80 km/h	36,4%	9,1%	13,6%	18,2%	22,7%

(b) Category F9, pedestrian at standstill hit by a truck.

Figure C.13: STRADA data: injury level vs. speed limit category F78 and F9.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	0,0%	50,0%	50,0%	0,0%
50-70 km/h	0,0%	0,0%	72,4%	20,7%	6,9%
>=80 km/h	0,0%	0,0%	0,0%	0,0%	0,0%

(a) Category J5, collision between tram and truck.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	7,9%	84,2%	5,3%	2,6%
50-70 km/h	4,4%	17,8%	37,8%	35,6%	4,4%
>=80 km/h	0,0%	28,6%	28,6%	28,6%	14,3%

(b) Category J8, collision between train and truck.

Figure C.14: STRADA data: injury level vs. speed limit category J5 and J8.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	4,5%	53,8%	36,3%	5,5%
50-70 km/h	1,2%	9,6%	51,0%	30,9%	7,2%
>=80 km/h	4,0%	13,8%	49,1%	23,4%	9,7%

(a) Category K, collision in intersection.

Injury speed %	1	2	3	4	9
<= 40km/h	3,1%	5,2%	50,5%	33,0%	8,2%
50-70 km/h	3,9%	13,7%	48,9%	26,2%	7,3%
>= 80 km/h	13,1%	15,2%	40,1%	23,0%	8,6%

(b) Category M, meeting/head-on collision.

Figure C.15: STRADA data: injury level vs. speed limit category K and M.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	0,0%	50,0%	37,5%	12,5%
50-70 km/h	0,3%	5,9%	45,4%	44,9%	3,6%
>=80 km/h	0,4%	7,1%	47,7%	36,4%	8,4%

(a) Category O, collision while overtaking.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	2,8%	50,0%	41,3%	5,9%
50-70 km/h	0,1%	4,3%	51,0%	37,9%	6,7%
>=80 km/h	0,6%	7,0%	49,5%	35,0%	7,9%

(b) Category U, rear ending accident.

Figure C.16: STRADA data: injury level vs. speed limit category O and U.

Injury speed %	1	2	3	4	9
<=40km/h	0,0%	10,0%	85,0%	5,0%	0,0%
50-70 km/h	1,4%	16,2%	78,6%	1,7%	2,2%
>=80km/h	2,0%	14,0%	78,9%	2,7%	2,3%

(a) Category S13, single accident, truck is driving straight.

Injury speed %	1	2	3	4	9
<=40 km/h	20,0%	0,0%	80,0%	0,0%	0,0%
50-70 km/h	4,5%	15,9%	72,6%	4,5%	2,5%
>=80 km/h	2,0%	22,0%	70,0%	4,0%	2,0%

(b) Category S24, single accident, truck turning.

Figure C.17: STRADA data: injury level vs. speed limit category S13 and S24.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	0,0%	0,0%	0,0%	0,0%
50-70 km/h	0,0%	4,8%	50,0%	31,0%	14,3%
>=80 km/h	0,0%	5,0%	60,0%	20,0%	15,0%

(a) Category V1, truck collision with animal (not large wild animals).

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	9,4%	59,4%	21,9%	9,4%
50-70 km/h	0,6%	10,0%	50,3%	19,3%	19,8%
>=80 km/h	2,7%	13,7%	45,6%	26,2%	11,8%

(b) Category V5, collision with parked vehicle.

Figure C.18: STRADA data: injury level vs. speed limit category V1 and V5.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	1,6%	49,2%	44,3%	4,9%
50-70 km/h	0,4%	6,7%	51,4%	32,6%	8,9%
>=80 km/h	2,6%	10,8%	49,1%	26,4%	11,1%

(a) Category V6, collision while reversing.

Injury speed %	1	2	3	4	9
<=40 km/h	0,0%	0,0%	0,0%	0,0%	0,0%
50-70 km/h	1,7%	10,3%	77,6%	8,6%	1,7%
>=80 km/h	0,4%	10,6%	68,9%	15,4%	4,8%

(b) Category W, accident with large wild animals.

Figure C.19: STRADA data: injury level vs. speed limit category V6 and W.

On roads 50-70 km/h			
S0 Injury level 4 and less than 10% probability of Injury level 1-3	S1 More than 10% probability Injury level 1-3	S2 More than 10% probability of Injury level 1-2	S3 More than 15% probability of Injury level 1-2
	Accident with animal (small) (V1)	Vehicle hitting parked vehicle (V5)	Single accident while driving straight (S 1, 3)
	Vehicle reversing (V6)	Accident with animal (large) (W)	Single accident while turning (S 2, 4)
	Rear-ending accident (U)	Accident while vehicle crossing the road (K)	Meeting accident (M)
	Overtaking accident (O)	Meeting accident cyclist (C1)	Accident with train (J5)
	Accident with tram (J5)	Accident cycle overtaking/rear ending (C2)	Pedestrian crossing road (F 1, 2, 5, 6)
	Vehicle turning off road (A)	Vehicle and cyclist in same direction, one is turning (C3)	Pedestrian walking next to road (F 3, 4)
		Vehicles in opposing directions, one is turning (C4)	Pedestrian crossing road, vehicle turning (F 7, 8)
		Accident with cycle in crossing, both driving straight (C5)	Meeting accident object with no deformation zone (ex back of truck)
		Cyclist standstill (C7)	
		Jackknifing	
		Rear-ending stationary object	

Figure C.20: Severity in medium speed.

On roads <=40 km/h			
S0 Injury level 4 and less than 10% probability of Injury level 1-3	S1 More than 10% probability Injury level 1-3	S2 More than 10% probability of Injury level 1-2	S3 More than 15% probability of Injury level 1-2
Accident with tram (J5)	Vehicle hitting parked vehicle (V5)	Single accident while driving straight (S 1, 3)	Pedestrian crossing road (F 1, 2, 5, 6)
Accident with animal (small) (V1)	Vehicle reversing (V6)	Single accident while turning (S 2, 4)	Pedestrian crossing road, vehicle turning (F 7, 8)
	Rear-ending accident (U)	Pedestrian walking next to road (F 3, 4)	Accident with cycle in crossing, one is turning (C6)
	Overtaking accident (O)	Meeting accident object with no deformation zone (ex back of truck)	Accident with train (J5)
	Meeting accident (M)		
	Accident while vehicle crossing the road (K)		
	Meeting accident cyclist (C1)		
	Accident cycle overtaking/rear ending (C2)		
	Vehicle and cyclist in same direction, one is turning (C3)		
	Vehicles in opposing directions, one is turning (C4)		
	Accident with cycle in crossing, both driving straight (C5)		
	Vehicle turning off road (A)		
	Jackknifing		
	Rear-ending stationary object		

Figure C.21: Severity in low speed.

D

Data for probability of exposure

D.1 Road data from Trafikverket

In the road data from *Trafikverket*, the most common roads in Sweden in terms of speed limits and crash barriers were found. In urban areas, the most common speed limits are between 30 - 50 km/h, and speed limits above these are rare. Information regarding crash barriers is limited in urban areas, since most urban roads are municipal and the information given from Trafikverket is only available for governmental roads. It is however visible that the majority of the governmental roads in urban areas at 100 km/h or over have a crash barrier dividing the two directions. In rural or highway areas, it can be seen that a majority of roads with a speed limit of 100 km/h and above have a crash barrier separating the two directions. Figure D.1 contains data for all roads combined, Figure D.2 contains data for urban roads and Figure D.3 contain information regarding rural roads and highways.

All	Vägräcke mitten	Vägräcke höger	Ej vägräcke	Tot	% mitten	% höger	% inget	km roads	% km roads
Gångfart	0	0	1	1	0%	0%	100%	225	0.0%
20 Km/h	0	0	0	0	25%	22%	67%	17	0.0%
30 Km/h	6	4	293	301	2%	1%	97%	20 079	3.3%
40 Km/h	20	19	1 406	1 438	1%	1%	98%	13 546	2.2%
50 Km/h	151	132	5 956	6 181	2%	2%	96%	34 428	5.7%
60 Km/h	93	60	1 453	1 576	6%	4%	92%	2 664	0.4%
70 Km/h	1 199	806	57 335	58 973	2%	1%	97%	504 710	83.2%
80 Km/h	730	402	14 145	15 047	5%	3%	94%	14 884	2.5%
90 Km/h	871	502	8 391	9 460	9%	5%	89%	9 266	1.5%
100 Km/h	4 441	1 006	2 243	6 771	66%	15%	33%	4 491	0.7%
110 Km/h	3 342	735	222	3 606	93%	20%	6%	1 821	0.3%
120 Km/h	629	138	43	682	92%	20%	6%	341	0.1%
Tot	11 481	3 805	91 490	104 036				606 472	

Figure D.1: Road data from Trafikverket, all roads combined.

Urban	Vägräcke mitten	Vägräcke höger	Ej vägräcke	Tot	% mitten	% höger	% inget	km roads	% km roads
Gångfart	0	0	1	1	0.0%	0.0%	100.0%	223	0.4%
20 Km/h	0	0	0	0	0.0%	0.0%	100.0%	11	0.0%
30 Km/h	3	2	228	233	1.4%	0.9%	97.7%	18 588	30.4%
40 Km/h	16	17	1 123	1 156	1.4%	1.4%	97.1%	12 815	21.0%
50 Km/h	73	64	2 385	2 522	2.9%	2.5%	94.6%	26 987	44.2%
60 Km/h	38	19	314	370	10.3%	5.0%	84.7%	1 174	1.9%
70 Km/h	59	27	313	399	14.9%	6.7%	78.5%	1 134	1.9%
80 Km/h	34	13	59	106	31.9%	12.2%	55.9%	93	0.2%
90 Km/h	12	4	17	33	36.9%	11.0%	52.1%	51	0.1%
100 Km/h	32	13	1	46	70.7%	28.1%	1.2%	26	0.0%
110 Km/h	27	4	2	33	83.0%	10.8%	6.2%	18	0.0%
120 Km/h	0	0	0	0	100.0%	0.0%	0.0%	0	0.0%
Tot	296	161	4 442	4 898				61 120	

Figure D.2: Road data from Trafikverket, urban roads.

Rural	Vägräcke mitten	Vägräcke höger	Ej vägräcke	Tot	% mitten	% höger	% inget	km roads	% km roads
Gångfart	0	0	0	0	0.0%	0.0%	0.0%	2	0.0%
20 Km/h	0	0	0	0	29.0%	25.3%	45.6%	6	0.0%
30 Km/h	3	2	65	70	4.0%	3.1%	92.9%	1 491	0.3%
40 Km/h	3	2	283	289	1.1%	0.8%	98.1%	731	0.1%
50 Km/h	78	68	3 572	3 718	2.1%	1.8%	96.1%	7 441	1.4%
60 Km/h	55	42	1 140	1 236	4.4%	3.4%	92.2%	1 490	0.3%
70 Km/h	1 139	779	57 022	58 940	1.9%	1.3%	96.7%	503 575	92.3%
80 Km/h	696	390	14 086	15 171	4.6%	2.6%	92.8%	14 791	2.7%
90 Km/h	859	499	8 374	9 732	8.8%	5.1%	86.0%	9 215	1.7%
100 Km/h	4 409	993	2 242	7 644	57.7%	13.0%	29.3%	4 465	0.8%
110 Km/h	3 315	731	220	4 266	77.7%	17.1%	5.2%	1 803	0.3%
120 Km/h	629	138	43	810	77.6%	17.1%	5.3%	341	0.1%
Tot	11 186	3 644	87 048	101 878				545 352	

Figure D.3: Road data from Trafikverket, rural roads.

D.2 Usage data from GTA

As described before, there are many parameters that can be adjusted for a truck based on the intended usage. These parameters are within Volvo Group defined in GTA, and the statistics regarding the different parameters in sold trucks are found in LDA. In this section, the different parameters will be presented together with statistics over how common the different specifications are in the sold vehicles.

Volvo Trucks produces four different truck models today. The *FH* is a long haul truck, an is the flagship of Volvo Trucks. The *FM* has varied usages, both distribution, long haul and construction. The truck models FE and FL are almost exclusively used in distribution. A more detailed description of the usage of the different models based on the data found in LDA can be found in Appendix D.3.

Model	
FH	80%
FM	17%
FE	1%
FL	2%

Figure D.4: Percentage of vehicles of different models.

One of the most important parameters defined in GTA is the *operating cycle*, which reflects how often the vehicle stops to load or unload goods. This parameter is divided into four levels with increasing distance between stops: stop and go (<0.5km), local (0.5-5km), regional (5-50 km) and long distance (>50km). The number of vehicle sold with specifications of the different cycles is found in Figure D.5.

Cycle	Long Distance	Construction	Distribution
FH	89%	5%	6%
FM	19%	17%	64%
FE	0%	0%	100%
FL	0%	0%	100%
Total	58%	8%	33%

Figure D.5: Percentage of vehicles sold with the different cycles.

Road condition defines the roughness of the road, varying from smooth to very rough. Smooth is defined as at least 95% of the total distance is covered on properly surfaced roads of good quality. A road is assessed as rough if the road surface is of poor quality an up to 5% of the total distance is covered on extremely poor roads or off-roads. The specification of the sold trucks regarding road condition can be found in D.6.

RoadCond	Smooth	Rough	Very Rough
FH	70%	30%	0%
FM	54%	46%	0%
FE	100%	0%	0%
FL	100%	0%	0%
Total	68%	32%	0%

Figure D.6: Percentage of vehicles adjusted for the different road conditions.

Depending of the intended usage and market of the truck, the topography the truck will be exposed to can vary greatly. The parameter *Topography* ranges between flat, predominantly flat and hilly. Flat is defined as slopes with a gradient of <3% which occurs >99% of the driving distance, with a maximum gradient of 8%. Flat conditions usually occurs on highways. Predominantly flat is assessed as slopes with a gradient of <6% which occurs during >98% of the driving distance, and a maximum gradient of 16%. Hilly is defined as slopes with gradients <9% that occurs during >98% of the driving distance and maximum gradient of 20%. Hilly conditions does not usually occur on public roads, but mainly on construction sites or in mining. The data regarding topography specifications in LDA can be found in D.7

Topography	Flat	Predominan tely flat	Hilly
FH	39%	60.50%	0.50%
FM	25%	71%	4%
FE	8%	93%	0%
FL	8.60%	91%	0.50%
Total	31%	67%	2%

Figure D.7: Percentage of vehicles adjusted for different topography.

The parameter *yearly usage* defines the distance in kilometers for each year of the truck, and this is a good indication of the intended usage of the truck. Long distance vehicles usually cover significantly larger distances, from 80 000 - 400 000 km/year, each year than for stop and go and local trucks, typically 15 000 - 40 000 km/h. The data from LDA regarding yearly usage specification can be found in D.8.

Usage	0-20 000	20 000-40 000	40 000-60 000	60 000-80 000	80 000-100 000	100 000-150 000	150 000-200 000	>200 000
FH	3%	7%	10%	11%	11%	31%	17%	10%
FM	16%	0%	46%	21%	7%	7%	2%	1%
FE	16.50%	50%	16.50%	11%	3%	3%	0%	0%
FL	2%	11%	6%	1%	80%	0%	0%	0%
Total	6%	6%	18%	12%	15%	23%	12%	7%

Figure D.8: Percentage of vehicles adjusted for different usage in kilometers driven.

D.3 Defined usage for different truck models

This section contains a description of the usage of each truck model produced by Volvo Trucks, based on the data found in Appendix D.2.

D.3.1 FH

The truck model *FH* is mainly intended for long distance usage, which also is what 89% of all sold FH trucks are designed for. Less than 6% respective 5% are intended for construction or distribution. The FH is mainly used on highways, which usually are in good condition, and 70% of all FH trucks are specified to drive on smooth roads. Sweden, as well as many other countries in Europe, has a varied topography and 60.5% of the FH trucks are therefore specified to drive on predominately flat roads, and 39% are specified for flat roads. FH trucks usually covers high mileage, and 58% have a yearly average over 100 000 km.

D.3.2 FM

The truck model *FM* includes both the regular FM and the FMX, which is specially adapted to construction. The usage of the FM is therefore varied, with 64% used in distribution, 19% in long distance and 19% in construction. This creates problems in identifying a common usage scenario for the model. Since many of the trucks are used in construction or on rural roads, the rate of trucks intended to be used on rough roads is high, almost 46%, and 75% are specified to drive on predominately flat or hilly roads. The mileage covered each year also varies greatly, most commonly between 40 000-80 000 km/year.

D.3.3 FE and FL

The usage of the truck models *FE* and *FL* have very similar usages. For both models, 100% are specified to be used within distribution. Trucks used in distribution mainly drives short distances in urban areas, where roads are well maintained. Therefore, 100% of the the FE and FL trucks are defined to drive on smooth roads. However, the topography can be very varied within cities, why over 91% of the trucks of these models are defined as to be used in predominantly flat areas. The FL trucks have a higher yearly average mileage than FE, with 80% at 80 000-100 000 km/year compared to 83% between 0-60 000 km/year for the FE.

D.3.4 All models

If the product defect can occur in all models, the most common usage for the entire population has to be studied. From all truck models, the most common use cycle (58% of all vehicles) is defined as long distance, while 33% are used in distribution and 8% in construction. 68% of the vehicles are defined to be driven on smooth roads, and 67% are used in predominantly flat areas. The yearly average in driven kilometers is spread out, but the majority is defines as between 40 000-150 000 km/year. Since 80% of the trucks in the studied population are FH, these variables are very similar to those of the FH.

D.4 Weather data from SMHI

The following data regarding weather in Sweden is from Sveriges Meteorologiska Hydrologiska Institut (SMHI) [61].

- Average temperature: -8 to +10°C.
- Average value days with more than 1 cm snow: 100.
- Highest temperature reached: +38°C.
- Lowest temperature reached: -52.6°C.
- Average number of days with precipitation: 80-160.

D.5 Tables of probability of exposure divided by model

This section contains the final tables for probability of exposure, divided by the different models. The table for FH is presented in Figure D.9, FM is presented in Figure D.10 and FE and FL are presented in Figure D.11. The table for all models combined is presented in Section 4.3.

	FH			
	E1 Not specified, very rare	E2 <1% of driving time	E3 1-10% of driving time	E4 over 10% of driving time
Road speed limit and crash barrier		Urban road low km/h with no crash barrier	Rural roads high speed with crash barrier betweent the different directions	Rural/highway roads high speed with no crash barrier
			Urban roads med speed km/h with no crash barrier	Urban/highway road high speed with crash barrier betweent the different directions
Road layout and topography	Driving through a train crossing	Stopping at traffic light	Driving downhill with heavy load	Driving in curve med speed
	Driving close to steep	Driving in curve low speed	Predominantely flat roads	
	Driving on mountain road	Driving downhill with a curve	Medium speed crossings	
		Low speed crossing	Driving in curve high speed	
		High speed crossings		
Surrounding traffic	Vehicle passing parked vehicles low speed	Vehicle in front/behind low speed	Driving in a queue	Vehicle in front/behind med speed
	Vehicle passing parked vehicles med speed	Overtaking on road with oncoming traffic	Vehicle stopped on med speed road (about to turn)	Vehicle in front/behind high speed
		Vehicle standstill in queue	Vehicle stopped on high speed road (about to turn)	Vehicle following closely behind
		Vehicle stopped on low speed road (about to turn)	Driving downhill with vehicle in front	When parked, other parked vehicles in close proximity
		Overtaking/lane change on road without oncoming traffic low speed	Overtaking/lane change on road without oncoming traffic med speed	
			Overtaking/lane change on road without oncoming traffic high speed	
			Vehicle approaching in the left lane	
Surrounding VRUs	Bicyclist close to vehicle high speed	Right turn with cyclist approaching	Pedestrian crossing med speed	
	Pedestrian in close proximity high speed	Pedestrian passing behind vehicle	When parked, VRUs in close proximity	
		Pedestrian close to front of vehicle/passing in front of vehicle		
		Pedestrian crossing high speed		
		Pedestrian crossing low speed		
		Cyclist driving behind truck all speeds		
		Bicyclist close to vehicle med speed		
		Bicyclist close to vehicle low speed		
		Pedestrian in close proximity med speed		
		Pedestrian in close proximity low speed		
Road surface/visibility		Ice/snow on road (slippery roads)	Wet road	
		Rough roads	Rain/snow	
		Dark, lighted	Dark, unlighted	
Maneuvering		Start and Stops	Vehicle parked	
		Vehicle parked in steep slope	Vehicle at standstill	
		Truck placed in a closed area with people in close proximity	Vehicle parked in slight slope	
Other	Emergency braking	Parked truck with driver sleeping inside		Trailer or Semitrailer attached driving

Figure D.9: Probability of exposure during driving on public roads for model FH.

	FM			
	E1 Not specified, very rare	E2 <1% of driving time	E3 1-10% of driving time	E4 over 10% of driving time
Road speed limit and crash barrier			Rural roads high speed with crash barrier betweent the different directions	Rural/highway roads high speed with no crash barrier
			Urban road low speed with no crash barrier	Urban roads med speed with no crash barrier
				Urban/highway road high speed with crash barrier betweent the different
Road layout and topography	Driving through a train crossing	Driving downhill with a curve	Stopping at traffic light	Driving in curve med speed
	Driving close to steep	High speed crossings	Driving downhill with heavy load	Predominantely flat roads
	Driving on mountain road	Driving in curve high speed	Medium speed crossings	
			Driving in curve low speed	
			Low speed crossing	
Surrounding traffic		Vehicle approaching in the left lane	Driving in a queue	Vehicle in front/behind med speed
		Overtaking on road with oncoming traffic	Vehicle stopped on med speed road (about to turn)	Vehicle following closely behind
		Vehicle passing parked vehicles low speed with people inside	Vehicle stopped on high speed road (about to turn)	Vehicle in front/behind low speed
		Vehicle passing parked vehicles med speed with people inside	Driving downhill with vehicle in front	When parked, other parked vehicles in close proximity
			Vehicle in front/behind high speed	
			Vehicle standstill in queue	
			Vehicle stopped on low speed road (about to turn)	
			Overtaking/lane change on road without oncoming traffic low speed	
			Overtaking/lane change on road without oncoming traffic med speed	
			Overtaking/lane change on road without oncoming traffic high speed	
Surrounding VRUs	Bicyclist close to vehicle high speed	Right turn with cyclist approaching	Pedestrian crossing med speed	
	Pedestrian in close proximity high speed	Pedestrian passing behind vehicle	Pedestrian crossing low speed	
	Pedestrian crossing high speed	Pedestrian close to front of vehicle/passing in front of vehicle	Pedestrian in close proximity med speed	
		Cyclist driving behind truck all speeds	Pedestrian in close proximity low speed	
			Bicyclist close to vehicle med speed	
			Bicyclist close to vehicle low speed	
Road surface/visibilit y		Ice/snow on road (slippery roads)	Wet road	
		Rough roads	Rain/snow	
		Dark, lighted		
		Dark, unlighted		
Maneuvering		Vehicle parked in steep slope	Vehicle parked	
		Truck placed in a closed area with people in close proximity	Vehicle at standstill	
			Start and Stops	
			Vehicle parked in slight slope	
Other	Emergency braking	Parked truck with driver sleeping inside	Trailer or Semitrailer attached	Driver/occupant in vehicle during driving

Figure D.10: Probability of exposure during driving on public roads for model FM.

	FE/FL			
	E1 Not specified, very rare	E2 <1% of driving time	E3 1-10% of driving time	E4 over 10% of driving time
Road speed limit and crash barrier		Rural/highway roads high speed with crash barrier betweent the different directions	Urban road med speed with crash barrier betweent the different directions	Urban road low km/h with no crash barrier
		Rural/highway roads high speed with no crash barrier		Urban roads med speed km/h with no crash barrier
Road layout and topography	Driving through a train crossing	Driving in left lane on highway	Predominantely flat roads	Low speed crossing
	Driving close to steep	Driving downhill with heavy load	Medium speed crossings	Driving in curve low speed
	Driving on mountain road	Driving downhill with a curve	Stopping at traffic light	
		High speed crossings	Driving in curve med speed	
		Driving in curve high speed		
Surrounding traffic	Overtaking on road with oncoming traffic	Vehicle approaching in the left lane	Driving in a queue	Vehicle in front/behind med speed
		Vehicle standstill in queue	Vehicle stopped on med speed road (about to turn)	Vehicle in front/behind low speed
		Vehicle in front/behind high speed	Driving downhill with vehicle in front	Vehicle following closely behind
		Vehicle passing parked vehicles with people inside low speed	Overtaking/lane change on road without oncoming traffic	Vehicle stopped on low speed road (about to turn)
		Vehicle passing parked vehicles with people inside med speed	Overtaking/lane change on road without oncoming traffic low speed	When parked, other parked vehicles in close proximity
		Vehicle standstill in queue	Overtaking/lane change on road without oncoming traffic med speed	
		Vehicle stopped on high speed road (about to turn)		
		Overtaking/lane change on road without oncoming traffic high speed		
Surrounding VRUs	Bicyclist close to vehicle high speed	Right turn with cyclist approaching	Pedestrian crossing med speed	Pedestrian in close proximity low speed
	Pedestrian in close proximity high speed	Cyclist driving behind truck all speeds	Pedestrian crossing low speed	
	Pedestrian crossing high speed		Pedestrian passing behind vehicle	
			Pedestrian close to front of vehicle/passing in front of vehicle	
			Bicyclist close to vehicle med speed	
			Bicyclist close to vehicle low speed	
			Pedestrian in close proximity med speed	
			When parked, VRUs in close proximity	
Road surface/visibilit y	Dark, unlighted	Ice/snow on road (slippery roads)	Wet road	
		Rough roads	Rain/snow	
		Dark, lighted		
Maneuvering		Vehicle parked in steep slope		
		Truck placed in a closed area with people in close proximity	Vehicle parked	Start and Stops
			Vehicle at standstill	
			Vehicle parked in slight slope	
Other	Emergency braking	Trailer or Semitrailer attached		Driver/occupant in vehicle during driving
	Parked truck with driver sleeping inside			

Figure D.11: Probability of exposure during driving on public roads for model FE and FL.

E

Tables for controllability

This chapter will present all tables for controllability, divided into eight tables. Each table will be presented in the respective sections below.

E.1 Loss of trajectory, steering and stability

This controllability table (Figure E.1) covers all defects resulting in loss of trajectory, steering or stability of the vehicle.

E.2 Thermal event and fire

The controllability table for thermal event, Figure E.2, should be used in all situations resulting in thermal hot or cold events as well as fires.

E.3 Not possible to control vehicle speed (deceleration, acceleration not working as intended)

The controllability for cases regarding vehicle speed is gathered in Figures E.3 and E.4. This table divided into several sections describing the different situations.

E.4 Vision, conspicuity, loss of part and road condition

This table, see Figure E.5 contains controllability for various cases, with the common factor that they mainly affects other road users rather than the truck driver (with the exception of vision).

Controllability Loss of trajectory/steering/stability			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
Increase in steering effort/heavy steering/not working as intended low speed with notice	Increase in steering effort/heavy steering/not working as intended low/med speed without notice	Abrubt failure of part leading to loss of trajectory low speed without notice	Abrubt failure of part leading to loss of trajectory med/high speed without notice
Vehicle side pulling or unstable all speeds with notice	Increase in steering effort/heavy steering/not working as intended med/high speed with notice	Increase in steering effort/heavy steering/not working as intended high speed (and high relative speed) without notice	Loss of both steering and braking all speeds with or without notice
Vehicle side pulling or unstable low speed without notice	Vehicle side pulling or unstable med/high speed without notice	Complete loss of steering med speeds (and med relative speed) without notice	Complete loss of steering in high speeds (and high relative speed) without notice
Wheel lock unsteered wheel low speed without notice	Complete loss of steering in low speeds without notice	Complete loss of steering high speed with notice	Wheel lock on steered front wheel med/high speed without notice
Wheel lock unsteered wheel all speeds with notice	Complete loss of steering med speed with notice	Wheel lock on steered front wheel low speed without notice	Wheel lock on steered front wheel high speed with previous notice
Complete loss of steering low speed with notice	Slight steering and braking possible in med and high speed with notice	Wheel lock on steered front wheel med speed with notice	Wheel lock on unsteered wheel on slippery road med/high speed with or without notice
Abrubt failure of part leading to loss of trajectory low speed with notice	Slight steering and braking possible in low and med speed without notice	Wheel lock on unsteered wheel on slippery road low speed with or without notice	
	Wheel lock on steered front wheel low speed with notice	Abrubt failure of part leading to loss of trajectory high speed with notice	
	Wheel lock unsteered wheel med/high speed without notice		
	Abrubt failure of part leading to loss of trajectory med speed with notice		

Figure E.1: Controllability for loss of trajectory.

E.5 Maintenance, service or standstill

The table found in Figure E.6 contains controllability for all situations found occurring in maintenance, service or at standstill. As can be seen, most situations occurring in maintenance are very hard to control.

E.6 In crash

Figure E.7 contains the table for controllability in crash. That is, cases which only occurs after the crash. In general, these situation are very hard to control, as can be seen.

Controllability fire, thermal event			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
Thermal hot/cold in cab with notice		Fire in cab with notice	Fire in cab without notice
Thermal hot event /thermal cold event/leakage of hot fluids in other area with notice		Fire close to cab with notice	Fire close to cab without notice
		Fire in other area with notice	Fire in other area without notice
			Thermal hot/cold event in cab without notice
			Thermal hot event /thermal cold event/leakage of hot fluids in other area without notice
			Fire after crash

Figure E.2: Controllability for fire and thermal events.

E.7 Other

This controllability table, shown in Figure E.8, contains all cases which could not be placed in any of the other tables. It contains asphyxiation, jackknifing and doors opening while driving.

Controllability Braking/vehicle rolling away/vehicle speed			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
Unintentional deceleration/too harsh deceleration			
Harsh braking with brake lights low speed without notice	Harsh braking with brake lights med speed without notice	Harsh braking with brake lights high speed without notice	Harsh braking on one axle without brake lights high speed without notice
Harsh braking with brake lights all speeds with notice	Harsh braking without brake lights low speed without notice	Harsh braking without brake lights med speed without notice	Harsh braking with cyclist behind vehicle without brake lights med/high speed without notice
Harsh braking without brake lights low speed with notice	Harsh braking without brake lights med speed with notice	Harsh braking without brake lights high speed with notice	Harsh braking with cyclist behind vehicle with brake lights high speed without notice
Slight braking with brake lights all speeds without notice	Harsh braking with cyclist behind vehicle without brake lights low speed without notice	Harsh braking with cyclist behind vehicle with brake lights med speed without notice	Wheel lock on one axle without brake lights high speed without notice
Slight braking without brake lights low speed without notice	Slight braking without brake lights med/high speed without notice	Wheel lock on one axle without brake lights med speed without notice	Wheel lock on one axle with brake lights high speed without notice
Wheel lock on one axle with brake lights low speed without notice	Wheel lock on one axle with brake lights med speed without notice	Too high deceleration high speed with cyclist behind vehicle without notice	Harsh braking without brake lights high speed without notice
Harsh braking with cyclist behind vehicle with brake lights low speed without notice	Wheel lock on one axle without brake lights low speed without notice		
Too high deceleration low/med speed without notice	Too high deceleration high speed without notice		
Too high deceleration low speed with cyclist behind vehicle without notice	Too high deceleration med speed with cyclist behind vehicle without notice		
Deceleration not as intended/loss of brakes			
Loss of service brakes low speed with notice	Loss of service brakes low speed without notice	Loss of service brakes med speed without notice	Loss of both brake circuits all speeds with or without notice
Reduced brake performance low speed without notice	Loss of service brakes med speed with notice	Loss of service brakes high speed with notice	Loss of service brakes high speed without notice
Too low deceleration low speed without notice	Too low deceleration med speed without notice	Too low deceleration high speed without notice	
Too low deceleration all speeds with notice			

Figure E.3: Controllability regarding vehicle speed part 1.

Controllability Braking/vehicle rolling away/vehicle speed			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
Unintentional acc/not possible to acc/not possible to acc or dec			
Possible to brake during unintentional acceleration low/med speed, with or without notice	Possible to brake during unintentional acceleration high speed without notice	Not possible to accelerate and decelerate med speed without notice	Unintentional acc not possible to brake all speeds without notice
Not possible to accelerate and decelerate low speed with notice	Not possible to accelerate high speed without notice	Not possible to accelerate and decelerate high speed with notice	Not possible to accelerate in train crossing all speeds without notice
Not possible to accelerate low/med speed without notice	Not possible to accelerate and decelerate low speed without notice		Not possible to accelerate and decelerate high speed without notice
Possible to brake during unintentional acceleration high speed, with notice	Not possible to accelerate and decelerate med speed with notice		Loss of both brake circuits and not possible to accelerate all speeds without notice
Vehicle rolling away from standstill			
Vehicle rolling away from standstill, driver in vehicle with notice	Vehicle rolling away from standstill, driver in vehicle without notice		Vehicle rolling away from standstill driver not in vehicle without notice
	Vehicle rolling away from standstill, driver not in vehicle with notice		
Failure of safety system			
Failure of AEBS with or without notice	Failure of ACC med/high speed without notice		
Failure of ACC low speed without notice			
Failure of ACC all speed with notice			

Figure E.4: Controllability regarding vehicle speed part 2.

Controllability Vision/conspicuity/loss of part or trailer/road condition			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
Activation of high beams without notice	Trailer stationary on road low speed	Trailer stationary on road med speed	Trailer stationary on road high speed
Failure of both headlights with or without notice	Loss of part leading to loss of control of vehicle behind low speed	Trailer moving in opposite direction of traffic low speed	Trailer moving in opposite direction to traffic med/high speed
Impaired vision for driver with or without notice	Large leagake of fluids on roads med/high speed	Loss of part leading to loss of control of vehicle behind med speed	Loss of part leading to loss of control of vehicle behind high speed
Malfunction of all brake lights low speed without notice	Malfunction of all brake lights med/high speed without notice		
Malfunction of all indicator lamps with or without notice			
Large leagake of fluids on roads low speed			

Figure E.5: Controllability for cases regarding vision, conspicuity, loss of part and road condition.

Controllability in maintenance, service or at standstill			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
Vehicle rolling away from standstill in maintenance with notice		Cab falling/tilting back with notice	Failure of part leading to fall of person without notice
Failure of part leading to fall of person with notice			Unintentional release of exhaust gases at standstill in limited area
Leakage of hazardous substance in maintenance with notice			Electric shock
Engine starting during service/maintenance with notice			Vehicle rolling away from standstill in maintenance without notice
Engine hood falling during maintenance/service with notice			Leakage of hazardous substance in maintenance without notice
			Cab falling/tilting back without notice
			Engine starting during service/maintenance without notice
			Engine hood falling during maintenance/service without notice

Figure E.6: Controllability in maintenance, service or at standstill.

Controllability in crash			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
	One door not opening after crash		Doors and/or roofhatch not opening after crash
			Trapped in seat after crash
			Failure of safety system/restraint system used in crash without notice
			Airbag failure/inflating too quickly
			Failure of ESC when needed

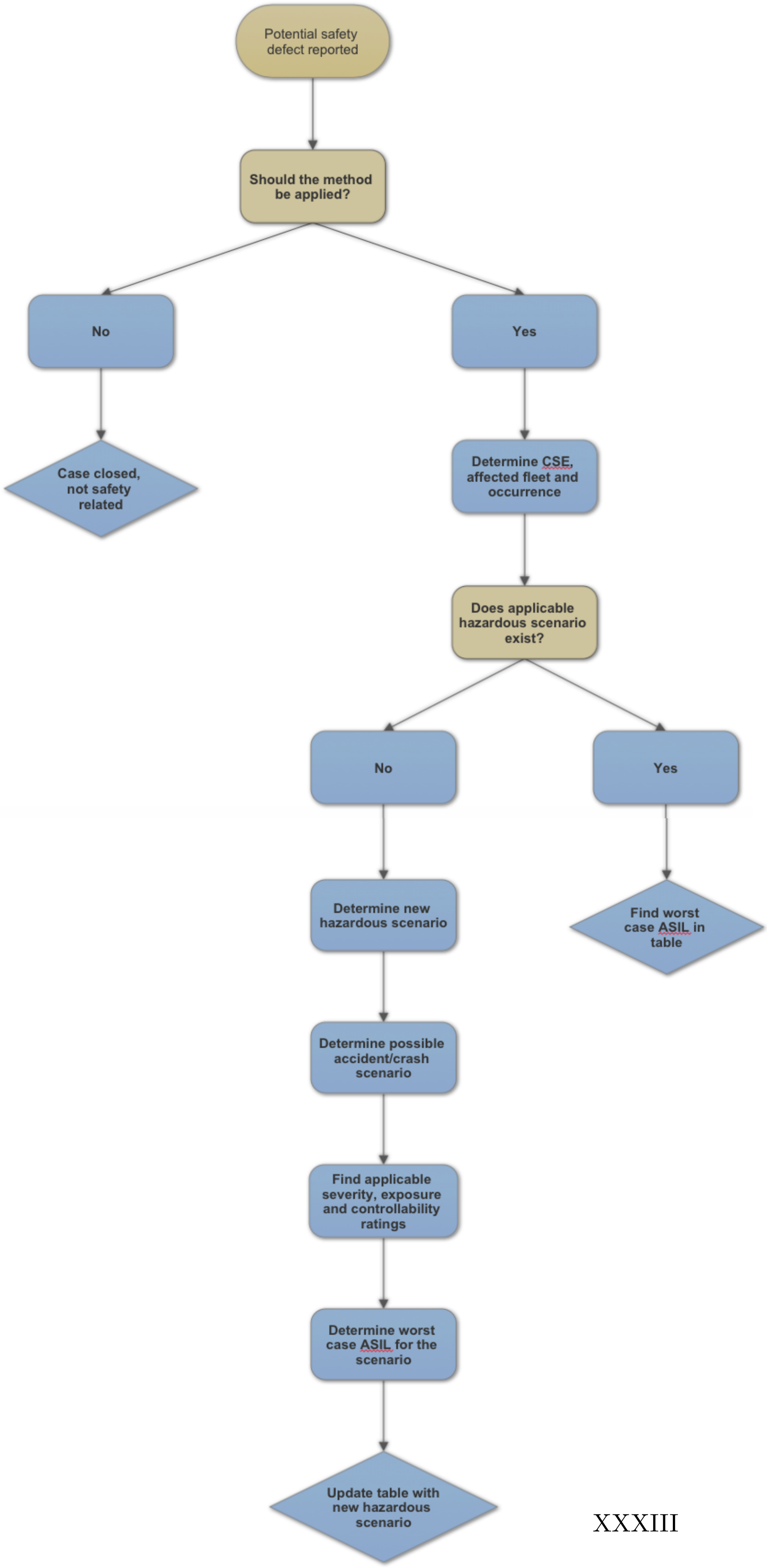
Figure E.7: Controllability for crash.

Controllability Other			
C0 Controllable in general	C1 Almost all drivers are able to avoid harm	C2 Many drivers can avoid harm	C3 Very hard for most drivers to avoid harm
A faulty HMI message is controllable in general	Gas noticed by smell leaking into the cab		Gas not easily noticed leaking into cab
Doors opening and driver fasten in seat with seat belt with or without notice	Jackknifing med/high speed without notice		Gas leaking when driver not close to vehicle
Jackknifing all speeds with notice			
Jackknifing low speed without notice			

Figure E.8: Controllability for other cases.

F

Flow chart describing usage of method


Potential safety defect reported
Should the method be applied?
No
Yes
Case closed, not safety related
Determine CSE, affected fleet and occurrence
Does applicable hazardous scenario exist?
No
Yes
Determine new hazardous scenario
Find worst case ASIL in table
Determine possible accident/crash scenario
Find applicable severity, exposure and controllability ratings
Determine worst case ASIL for the scenario
Update table with new hazardous scenario