Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study

DVA501 – Thesis for the Degree of Master of Science (120 credits) in Computer Science with Specialization in Software Engineering

Mälardalen University
School of Innovation, Design and Engineering (IDT)

Volvo Construction Equipment
E&E (Electrical&Electronic) Architecture Department

May 18, 2015

Ditmar Parmeza
Student Number: 900526-P459
dpa12001@student.mdh.se

Mälardalen University: Sasikumar Punnekkat
sasikumar.punnekkat@mdh.se

Volvo Construction Equipment: Stephan Baumgart
stephan.baumgart@volvo.com
Preface and Acknowledgements

This report summarizes the industrial Master Thesis work performed at both Volvo Construction Equipment in Eskilstuna, Sweden and Mälardalen University in Västerås, Sweden in order to finalize my studies in Master of Science in Software Engineering (120 credits). I consider this work as a challenging and professional experience which not only helped me on expand significantly my knowledge and practice in Safety-Critical System Engineering but it also provided strong directions and chances for my future career in this area as well as in other Software Engineering areas.

At first place, I would like to thank my Master Thesis supervisor, Stephan Baumgart who has been very helpful, motivating and patient all the way while supervising my Master Thesis work at Volvo Construction Equipment as well as at Mälardalen University. His continuous feedback as well as the discussions in the Master Thesis meetings have been crucial throughout the whole process.

I would also like to thank Sasikumar Punnekkat, the Master Thesis examiner who provided useful guidance and feedback with respect to how the conducted studies in my thesis as well as the analysis and results should be reported. His ideas were more than helpful while improving the report.

Furthermore, I would like to express my gratitude towards all Volvo CE experts and practitioners as well as representatives from other industrial domains who gave a significant contribution and helped on providing technical information by participating in the first two conducted studies that are described in this report: the interview study and the survey study. Given that this thesis work is basically an empirical study, their industrial experience on product lines and functional safety as well as their technical feedback were of high importance to consider when working on the analysis and results of this work.

Finally, I would definitely like to thank my family and all of my friends for supporting and encouraging me while working on my Master Thesis. In such cases, moral support is also very important and much appreciated.

Abstract

Reuse processes are considered nowadays as a very advantageous and beneficial approach that is frequently used in several industrial environments. This fact has strongly motivated practitioners to rely on Software Product Line Engineering principles. Using product lines is associated with both cost savings and reduced efforts for development in industry. Moreover, many companies and domains develop products nowadays that need to be safety certified before they can be sold to customers.

In this perspective, there is industrial effort spent on addressing functional safety in product lines in industry. Different cost modeling approaches have been proposed in existing literature for providing solutions on software product line effort estimations. The main problem is that there is little evidence of cases in literature where such approaches have been applied successfully in industrial domains. In addition to that, no established product line cost model has been found in existing literature that considers functional safety efforts in its estimations.

In this thesis report, an empirical study is presented which has the main focus on the investigation of cost and efforts in industrial product lines for developing safety-critical products. Besides the literature study which highlights related work and existing cost-modeling approaches for product lines, three studies are conducted in order to provide evidence and findings for identifying cost and efforts attributed to safety-critical product line development in industrial domains.

In the first study, semi-structured interviews are performed with practitioners and industrial experts at Volvo Construction Equipment. The structure of the interview study is influenced and inspired by the findings from the literature study on expert effort estimations and established product line cost models as well as the effort and cost areas they attribute to the overall product line effort. The main purpose of the interview study is to derive results on safety effort estimation based on the feedback provided by industrial experts regarding functional safety application in the construction equipment domain. The second study consists in a survey study which gathers information on how other domains (except Volvo CE) deal with functional safety in their product lines and aims to investigate functional safety effort in their product line development process. Finally, a documentation analysis (third conducted study) is performed at Volvo CE in order to provide more evidence for supporting the findings from case study 1.

The main contribution of this thesis work consists in the following:

1. An overall analysis of the findings and results derived from the three conducted studies was provided in order to identify and explain the cost areas that contribute in the overall functional safety effort attested in industrial product lines. Moreover, several functional safety-related issues and challenges are identified while analyzing the three studies. Highest focus during this analysis regards their impact on cost in the functional safety perspective. Finally, we provide solutions on how to reduce this impact on cost by explaining the interdependencies between different safety-related cost areas, as well.

The most important contribution of the analysis consists in the conclusions drawn from the investigation of functional safety effort estimation in product...
lines in industry. Previously, performing the literature study did not bring to the identification of any cost-modelling technique or estimation approach that is considering functional safety effort estimation in industry. For this reason, the results derived based on the findings in our empirical study are crucial in this perspective.

2. In addition, we propose guidelines on proposing a new estimation approach in the future which would combine principles from both formal cost-modelling techniques as well as expert-based estimation methods which rely on the industrial expertise and human experience. We derive different components for the total functional safety effort in product lines from the findings in our empirical study. Moreover, different safety-related scenarios in industry and include safety effort estimations for each of them. The biggest contribution is however on the directions given on how to estimate in practice each of the functional safety effort components. Such directions are currently missing in existing effort estimation methods.

3. Finally, proposals on how to improve further our analysis on product line safety effort estimation are given. Furthermore, we explain what is needed in addition in order to propose and design a relevant safety-related product line effort estimation approach in the future.
LIST OF FIGURES ............................................................................................................. 1
LIST OF TABLES .............................................................................................................. 2

1. INTRODUCTION ........................................................................................................... 3
   1.1 PROBLEM DESCRIPTION ..................................................................................... 3
   1.2 RESEARCH QUESTIONS ....................................................................................... 3
   1.3 CONTRIBUTION ..................................................................................................... 4
   1.4 REPORT OVERVIEW .............................................................................................. 5

2. BACKGROUND .............................................................................................................. 6
   2.1 THE PRODUCT LINE APPROACH ....................................................................... 6
       2.1.1 Benefits of the Product Line Approach in comparison to Single-Product Development ............... 8
       2.1.2 Drawbacks and Challenges associated to the Product Line Approach .............................................. 9
       2.1.3 Effort in Product Line Development and Single Development ......................................................... 9
   2.2 FUNCTIONAL SAFETY ............................................................................................ 10
       2.2.1 Basic Concepts ............................................................................................... 10
       2.2.2 Functional Safety Standards ........................................................................... 11
       2.2.3 Risk Assessment Techniques .......................................................................... 14
       2.2.4 Safety Cases .................................................................................................... 18
   2.3 CONSIDERING FUNCTIONAL SAFETY IN PRODUCT LINES ......................................... 19

3. RESEARCH METHOD .................................................................................................... 20
   3.1 LITERATURE STUDY ............................................................................................ 20
       3.1.1 Literature Search ............................................................................................. 20
       3.1.2 Literature Evaluation and Selection ................................................................ 20
       3.1.3 Literature Search Results ................................................................................ 21
   3.2 CONDUCTED STUDIES ......................................................................................... 22
       3.2.1 Interview Study ............................................................................................... 23
       3.2.2 Survey Study .................................................................................................... 25
       3.2.3 Documentation Analysis .................................................................................. 26

4. RELATED WORK .......................................................................................................... 28
   4.1 SOFTWARE PRODUCT LINE COST MODELS ..................................................... 28
       4.1.1 COCOMO II ...................................................................................................... 29
       4.1.2 COPLIMO ........................................................................................................ 31
       4.1.3 qCOPLIMO ...................................................................................................... 33
       4.1.4 Poulin’s Model .................................................................................................. 35
       4.1.5 SoCoEMo-PLE ................................................................................................. 36
       4.1.6 Withey’s Model ................................................................................................. 38
       4.1.7 Schmid’s Model ............................................................................................... 40
       4.1.8 Boeckle’s Model (A Cost Model for Software Product Lines) .............................................. 42
       4.1.9 SIMPLE ........................................................................................................... 44
       4.1.10 InCoMe .......................................................................................................... 48
       4.1.11 Discussion ...................................................................................................... 50
   4.2 EXPERT ESTIMATION METHODS FOR PRODUCT LINES ........................................ 53
5. CONDUCTED STUDY 1: INTERVIEW STUDY .................................................. 59
   5.1 INTRODUCTION .............................................................................. 59
   5.1.1 Problem Area 1: Managing safety in product lines in industry ............... 59
   5.1.2 Problem Area 2: Efforts related to functional safety in industry .................. 59
   5.1.3 Problem Area 3: Identification of activities and approaches that can affect the cost related specifically to safety aspects ................................................................. 59
   5.2 COST ANALYSIS IN PRODUCT DEVELOPMENT ............................... 60
   5.3 INTERVIEW STUDY - RESULTS ...................................................... 62
   5.3.1 General Background .................................................................. 63
   5.3.2 Key Findings .............................................................................. 64
   5.4 DISCUSSION ............................................................................... 77

6. CONDUCTED STUDY 2: SURVEY STUDY ................................................. 80
   6.1 INTRODUCTION .............................................................................. 80
   6.2 SURVEY RESULTS ...................................................................... 81
       6.2.1 General Background ................................................................. 81
       6.2.2 Scenarios and Organizational Effort ............................................. 82
       6.2.3 Core Asset Base Effort ............................................................... 84
       6.2.4 Effort for Unique Parts ............................................................... 85
       6.2.5 Reuse Effort ........................................................................... 86
       6.2.6 Evolutional Effort .................................................................... 88
       6.2.7 Maintenance Effort ................................................................. 89
   6.3 DISCUSSION ............................................................................... 90

7. CONDUCTED STUDY 3: DOCUMENTATION ANALYSIS .......................... 92
   7.1 INTRODUCTION .............................................................................. 92
   7.2 EVIDENCE FOR ISSUES AND SCENARIOS RELATED TO CHANGES FROM PREVIOUS GENERATIONS ................................................................. 92
   7.3 EVIDENCE FOR ISSUES AND SCENARIOS RELATED TO THE ORGANIZATIONAL EFFORT ................................................................. 93
   7.4 EVIDENCE AND ISSUES RELATED TO THE CORE ASSET BASE, REUSE AND UNIQUE EFFORTS ................................................................. 94
   7.5 EVIDENCE AND ISSUES RELATED TO THE EVOLUTIONAL EFFORT ................................................................. 95
   7.6 EVIDENCE AND ISSUES RELATED TO THE MAINTENANCE EFFORT ................................................................. 97
   7.7 SUMMARY ............................................................................... 98

8. ANALYSIS ................................................................................................... 99
   8.1 CONDUCTED STUDIES 1 AND 3 ..................................................... 99
       8.1.1 Areas for improvement related to issue 1 ...................................... 99
       8.1.2 Areas for improvement related to issue 2 ...................................... 101
       8.1.3 Areas for improvement related to issue 3 ...................................... 101
       8.1.4 Areas for improvement related to issue 4 ...................................... 102
       8.1.5 Areas for improvement related to issue 5 ...................................... 103
       8.1.6 Areas for improvement related to issue 6 ...................................... 104
8.2 CONDUCTED STUDY 2 ........................................................................................................ 105
8.3 DISCUSSION ..................................................................................................................... 108
8.3.1 Identifying Functional Safety Effort ............................................................................. 108
8.3.2 Challenges for Functional Safety Effort Estimation .................................................. 109
8.3.3 Possible Solution and Improvements for Functional Safety Effort Estimation in Industry .... 110
8.4 VALIDATION .................................................................................................................... 110
8.4.1 Construct Validity ......................................................................................................... 110
8.4.2 Internal Validity ............................................................................................................ 111
8.4.3 External Validity .......................................................................................................... 111
8.4.4 Reliability .................................................................................................................... 112
8.4.5 Limitations .................................................................................................................. 112
9. PROPOSAL FOR A NEW APPROACH ............................................................................. 113
9.1 TOWARDS A NEW COMBINED ESTIMATION APPROACH .............................................. 113
9.1.1 Safety Cost Areas ........................................................................................................ 114
9.1.2 Directions for Industrial Safety-Related Scenarios ..................................................... 116
9.1.3 Guidelines on estimating input values for safety cost areas ...................................... 119
9.2 SAFETY COST INTERDEPENDENCIES ....................................................................... 122
9.3 AREAS FOR IMPROVEMENT AND FUTURE CONSIDERATION .................................. 125
10. SUMMARY AND CONCLUSIONS .................................................................................. 126
10.1 SUMMARY ...................................................................................................................... 126
10.2 CONCLUSIONS .............................................................................................................. 127
11. FUTURE WORK .............................................................................................................. 129
REFERENCES ...................................................................................................................... 130
APPENDIX A: INTERVIEW QUESTIONNAIRE .................................................................. 134
APPENDIX B: SURVEY QUESTIONS .................................................................................. 146
List of Figures

Figure 1: Development Phases in SPLE [1].................................................................7
Figure 2: Graphical presentation of product line benefits in the economical perspective [4]..............10
Figure 3: The V-model according to ISO 26262 standard – Part 6 [10]........................................12
Figure 4: Example of a FTA where two components fail because of an event..............................17
Figure 5: General template for GSN argumentation [17].......................................................18
Figure 6: Distribution of digital sources used as references......................................................22
Figure 7: Distribution of types of sources used as references....................................................22
Figure 8: Triple Case Design ..................................................................................................23
Figure 9: Interview Study Structure.......................................................................................24
Figure 10: Survey Study Structure..........................................................................................26
Figure 11: Method for Documentation Analysis .........................................................................27
Figure 12: Overview of proposed cost models in chronological order.......................................28
Figure 13: General Design of qCOPLIMO model [30]................................................................33
Figure 14: Comparison of ROI in COPLIMO and qCOPLIMO [30]...........................................34
Figure 15: Decision tree illustration used in Withey’s model [38]..............................................39
Figure 16: Product line strategy performed by Schmid’s model [39]..........................................41
Figure 17: Structure of the InCoMe Model [44]..........................................................................48
Figure 18: Relation between cost and product development ....................................................60
Figure 19: Interdependencies between issues identified in the interview study .........................79
Figure 20: Changes from previous generations .........................................................................83
Figure 21: Activities with impact on the organization..................................................................84
Figure 22: Common artifacts used by survey respondents ........................................................85
Figure 23: Number of domains that reuse different types of common development artifacts ....86
Figure 24: Highest integration effort when reusing from the common artifacts .........................87
Figure 25: Number of domains that reuse risk assessment documentation ..................................87
Figure 26: Extra functional safety effort for added products in the domains included in the survey ....89
Figure 27: Number of domains for identified maintenance activities with highest effort on product line maintenance in general and in the functional safety perspective.......................................................89
Figure 28: High level design of the combined approach ..........................................................114
Figure 29: Identified safety cost components in all three studies ..............................................115
List of Tables

Table 1: ASIL definition based on S, E and C ................................................................. 13
Table 2: Hazard evaluation in the analysis ................................................................. 15
Table 3: Template for performing and reporting FMECA ........................................... 16
Table 4: Severity ranking for the failures ................................................................. 17
Table 5: Reference selection based on the criteria .................................................... 21
Table 6: Evaluation of software product line cost models .......................................... 50
Table 7: General overview of the interviewees .......................................................... 63
Table 8: Significant changes from previous generation(s) attested by each interviewee .................................................................................................................. 64
Table 9: Cost impact of issues and scenarios of changes from previous generations .......... 67
Table 10: Issues observed on the organizational side ................................................. 70
Table 11: Cost impact of issues and scenarios related to organizational effort ................. 70
Table 12: Issues related to core asset base, reuse and unique efforts ............................. 71
Table 13: Cost impact of scenarios from issue 4 ......................................................... 73
Table 14: Issues related to evolulutional effort ......................................................... 74
Table 15: Cost impact of scenarios related to evolulutional effort ................................. 75
Table 16: Issues related to maintenance effort ......................................................... 76
Table 17: Cost-related issues and key findings ........................................................... 78
Table 18: General overview of the survey respondents ............................................... 81
Table 19: Survey responses on functional safety and cost modelling ............................. 82
Table 20: Evidence for issues 1 and 2 ....................................................................... 92
Table 21: Evidence for issue 3 .................................................................................. 93
Table 22: Evidence for issue 4 .................................................................................. 94
Table 23: Evidence for issue 5 .................................................................................. 96
Table 24: Evidence for issue 6 .................................................................................. 97
Table 25: Increase of Ccab in issue 1 and impact on other cost factors ......................... 100
Table 26: Increase of Ccab in issue 2 and impact on other cost factors ......................... 101
Table 27: Increase of Corg (D) and Ccab in issue 3 and impact on other cost factors .......... 102
Table 28: Increase of Corg (D) and Ccab in issue 4 and impact on other cost factors .......... 102
Table 29: Increase of Cevo in issue 5 and impact on other cost factors .......................... 104
Table 30: Increase of Cmaintenance in issue 6 and impact on other cost factors ............. 105
Table 31: Identified cost areas in study 2 and the similarity level with the context of the corresponding cost areas in study 1 ........................................................................ 106
Table 32: Identified cost dependencies based on the analysis of findings from studies 1 and 3 .... 123
1. Introduction

1.1 Problem Description

Software product line engineering represents nowadays an approach that is embraced by a wide range of industrial domains. Developing several products as a product line brings to many advantages compared to the situation when they are developed as single products. A well known advantage of the product line is the possibility to prepare the products for the targeted market in a significant shorter time. Of course, developing each product in a single way would generally require extra time, effort and resources. Moreover, the overall quality would increase when the products are developed in series and share many commonalities. If there is some defect detected at one product, then it will be automatically detected at the other product line members, as well. Maintaining the products as a product line requires less effort than providing specific maintenance support for each product developed in single mode.

Regardless, there are different situations and scenarios that need to be considered in a real industrial environment. Hence, the above product line advantages cannot be generalized for each situation or scenario in an industrial domain. When passing from single development to product line development, an analysis should take place in order to estimate and compare the effort of developing the products in a product line with the effort needed for developing them as single products. Comparing the results from the estimations brings to a more safe approach for evaluating if using product lines really pays off and when it is expected to pay off. Today, there are several cost-modeling approaches that provide solutions for product line effort estimation.

The number of domains that are considering functional safety for their products lines is significantly increasing. Different systems and environments are exposed always to several threats which may cause often the system to fail, and in some cases, accidents can happen. In order to avoid such consequences, functional safety is applied for a wide range of industrial product lines. This is the case also for Volvo Construction Equipment (Volvo CE) where different functional safety standards are applied for different product lines: wheel loaders, articulated haulers, excavators and so on.

As the interest on applying functional safety increases significantly, the effort put is increasing substantially as well. For this reason, the effort put on functional safety in industrial product lines needs to be investigated. The problem is that there is currently no established approach that is considering safety estimation in industry. Moreover, capturing the effort related to functional safety represents a complex task and it cannot be achieved by using formal estimation models.

1.2 Research Questions

We identified the following research questions we aim to answer in this work.

(1) RQ1: Which studies consider both cost models and product lines?

RQ1.1: Which cost models deal with both cost issues and software product lines?
RQ1.2: Which cost models have been successfully applied in industrial environments?

RQ1.3: Which cost models consider the efforts for functional safety in product lines?

(2) RQ2: Which efforts relate to functional safety in industrial product lines?

RQ2.1: Which cost factors can be identified as main components that contribute in the total safety-related effort in product lines??

RQ2.2: Which efforts are related to safety-related activities?

In order to answer the first research question RQ1 and its sub-questions (RQ1.1-RQ1.3), a literature study is performed in chapter 4. In this literature study, existing product line cost models as well as expert-based estimation methods are investigated. We investigate and summarize how each existing cost model deals with product line effort estimations. Furthermore, we identify cases when such models are applied in practice as well as the possibility if any of them is taking functional safety in consideration.

Regarding the second research question RQ2 and its sub-questions (RQ2.1-RQ2.2), answering them will be possible by analyzing the results from the three studies that are presented in chapters 5 (interview study), 6 (survey study) and 7 (documentation analysis).

In the first study, we derive conclusions on functional safety cost and safety-related activities based on the semi-structured interviews performed with Volvo CE industrial experts. Further findings and results on safety-related costs in industry are extracted from the survey study (chapter 6) and the documentation analysis performed at Volvo CE (chapter 7). However, all findings and results on safety-related activities and efforts are summarized in the overall analysis in chapter 8.

1.3 Contribution

The main contribution of this thesis relies on analyzing cost and effort spent exclusively on functional safety in industrial product lines.

In this report, the main contribution areas are included and summarized in the following:

- A literature study conducted on three main paradigms (product lines, functional safety and cost-modeling approaches) which highlights product line effort estimation in existing cost models and expert-based methods.

- Analysis of results on safety-related cost aspects in product lines that are extracted from the three studies (interview study, survey study and documentation analysis). Because of the findings from the literature study that prove to be not sufficient for estimating functional safety effort in industrial product lines, we perform an empirical study on functional safety effort estimation (based on the findings from the three studies). In our analysis, we provide solutions on how to consider functional safety effort in industry as well as guidelines on how to estimate each cost and effort related to functional safety.
At last, directions and guidelines are given for introducing a new cost-modeling approach that takes into consideration functional safety in industrial product lines.

### 1.4 Report Overview

The remaining part of the master thesis is organized as follows.

Section 2 provides general background related to product lines and functional safety. At first, both paradigms are described separately. Afterwards, subsection 2.3 presents a general overview of how functional safety is considered in product lines nowadays.

The research method is explained in section 3. This part consists in explaining how the literature research study was performed and it describes the three studies (interview study, survey study, documentation analysis) conducted in this work.

Section 4 presents the results derived from the literature study. The first subsection summarizes existing product line cost models while the second one is about expert effort estimation methods.

In the next sections, the results from the three studies are presented. Section 5 includes the findings and results from the interview study. Section 6 gives an overview of the results obtained from the survey study. Furthermore, evidence that is found in the documentation analysis (study 3) in order to support the findings in the interview study is presented in section 7.

Section 8 contains the analysis performed based on the results derived from the literature study (section 4) and the three studies (section 5, 6 and 7).

Section 9 presents our proposal for introducing a product line cost model that considers functional safety as well as guidelines and directions on how to extend this model and provide further argumentation to support it.

Summary and conclusions of the work are described in section 10 while section 11 describes the future work we foresee and the potential to further improve and extend our work.
2. Background

2.1 The Product Line Approach

The product line approach is considered as a solution for developing a set of products from a core asset base, in a predefined way [1]. The core asset base is composed of different common artifacts that are intended to be fully or partially reused in order to develop different products and applications that are suitable for different industrial purposes. In other words, the product line approach can be seen as an approach used by industrial domains in order to collect and provide a set of reusable artifacts for a group or family of products. Hence, several products and applications can be extracted and generated from this set of reusable artifacts and they can be tailored according to their purpose of use [2].

There are usually two different industrial ways that an organization use for embracing a product line approach [3]. In the first one, the organization put significant effort on developing the basis i.e., the common artifacts (sometimes completely or almost from scratch) of the new product line. The applications and specific products of the new product line are derived by reusing parts from the basis and integrating new ones. The other way suggests that the organization should not develop common artifacts (i.e., invest in the basis) but instead, develop each new product line member by reusing artifacts from previous product line generation(s) or previous projects.

There is certainly a connection between the product line approach and software engineering areas. Nowadays, it is aimed to investigate software engineering methods for applying them in product lines in order to get a higher abstraction level. These methods comprise a concept that is known as SPLE (Software Product Line Engineering). Pohl et. al provide a definition for SPLE in their book [1]: “SPLE is a paradigm that consists in developing software products and applications by relying on platforms and customization of the mass”. A platform, is a collection of common features such as components and interfaces i.e., a core asset base from which the products are developed and tailored. As for the customization of mass, it refers to the process of developing products from the core asset base according to specific needs and requirements defined by customers and the market.

SPLE consists in two significant phases: Domain Engineering and Application Engineering that are illustrated in figure 1 [1].

The domain engineering phase includes the commonality-variability analysis [1] that is performed in a product line in order to define the common artifacts and functionalities of the products and the specific ones, as well. After performing the commonality-variability analysis, the products and applications are developed in the application engineering phase by reusing the artifacts in the core asset base.

Both domain engineering and application engineering comprise two big development processes that consist in several sub-phases and artifacts.

There are four artifact types that are involved in both development processes [1]:
1. Requirements
2. Architecture parts (Design Artifacts)
3. Components (Implementation Artifacts / Code parts)
4. Tests

The domain engineering phase includes specifically five sub-phases [1]:

1. Product Management
2. Domain Requirements Engineering
3. Domain Design
4. Domain Realization
5. Domain Testing

The product management sub-phase includes the study and a preliminary market analysis in order to investigate and predict the effort that would take developing and managing a certain product line. In addition, product management provides also strategies and techniques on how to develop applications from parts of artifacts in the core asset base.

In the domain requirements engineering sub-phase, the strategies and techniques defined in the product management sub-phase are used in order to derive common requirements that will be used for the entire product line and also a variability model that identifies specific
parts for each product. Hence, only the common requirements are included in the core asset base.

The domain design sub-phase makes use of the common requirements and the variability model derived in the previous phase and produces an architectural view for them. The architecture parts derived from the common requirements are considered as common assets.

Everything is translated into code and implemented components in the domain realization sub-phase and eventually into tests in the successive one i.e., the domain testing sub-phase.

As for the application engineering phase, it comprises four sub-phases [1]:

1. Application Requirements Engineering
2. Application Design
3. Application Realization
4. Application Testing

Each sub-phase in application engineering is matching one sub-phase in domain engineering, with the exclusion of the product management sub-phase. However, the most significant difference between them lies on the artifacts that are being derived in each sub-phase. While common artifacts are being derived in a domain engineering sub-phase in order to be used for the entire product line, the corresponding application engineering sub-phase is responsible for producing specific artifacts for the purpose of being used specifically in only one or some applications of the product line. For example, the application requirements engineering sub-phase is responsible for identifying the specific requirements that are attributed to specific applications that are going to be developed as part of the product line.

### 2.1.1 Benefits of the Product Line Approach in comparison to Single-Product Development

The most notable advantage of software product lines consists on having less effort for development as well enhancement of product quality [4] [5]. The core asset base enables the reuse of development artifacts and it supports their tailoring to several products and applications. Generally, it is considered that developing products as a product line takes less time and effort compared to single development since it is possible to reuse common artifacts in different product line members [4].

Moreover, product quality increases when the product line approach is used for developing products in industry. The fact that the common assets are being reused in different products and applications means that they are also being tested more than once. Therefore, the chances to identify and fix possible errors are higher and the product quality is increased [5].

Investing in developing common assets is expected to pay off when such common assets are utilized and reused in different products of the product line. The fact that development time is significantly decreased compared to the situation when products are developed separately brings to another advantage. A shorter development time means also that the products are ready to reach the market in a smaller amount of time. Hence, time to market is also considered to decrease and that happens because of reusing artifacts in the product line [6].
2.1.2 Drawbacks and Challenges associated to the Product Line Approach

Despite being mostly advantageous compared to conventional single product development approaches, SPLE presents also several challenges.

The system gets more complex while passing from single development to product line development. It is necessary to spend effort on the analysis of identifying all commonalities and variability in order to investigate the common attributes and artifacts in a product line as well as the differences within [1]. Such effort is not necessary when developing single products. Common parts of the product line need to be identified in order to be able to reuse them properly for different product line members. The identification of commonalities takes place in the domain engineering phase while the reuse of such commonalities in different products happens in the application engineering phase. Common parts of the product line can be implemented by using a library with common code which can be tailored later for different applications [7]. The management of variability requires extra effort, as well. The variability in product lines need to be represented for each development phase. If we consider the requirements specification phase, specific requirements need to be defined for the unique parts in different product line members in addition to the common requirements that are already defined for the product line [8].

The organization needs also to invest extra effort at the beginning when developing a product line. In order to assure high quality for the product line, the organization needs to put effort on planning as well as management and operation [2]. In most cases, the organization can be even re-structured in order to adapt to the new product line development approach.

Developing product lines can be specifically challenging compared to single development in cases of distributed development [2]. This case is more obvious in large domains that include several sites distributed in different geographical locations. Developing a product line is more difficult than developing single products in such conditions since there is the risk that different sites propose different solutions for same product line members and hence, there is no much reuse of common artifacts in the product line.

In general, product line development requires at first investing on time, capital and effort. However, this investment is expected to pay off by saving future cost, effort and time. A more detailed overview of this is presented in the successive subsection.

2.1.3 Effort in Product Line Development and Single Development

Despite of the advantages that the product line approach provides in comparison to single development, choosing product line development instead of the single one is not always the best choice. Depending on different industrial cases and situations, it is necessary to analyze first which development method is more beneficial. The chart in figure 2 gives a general overview of the development efforts in both cases depending on the amount of products that are developed [4].
Figure 2: Graphical presentation of product line benefits in the economical perspective [4]

In the case of single development, the effort is proportional to the amount of products that are developed. That means that there is no development effort in the beginning since there are no developed products yet.

The situation with development effort is different in product line development. At the starting point, there is development effort for building the core asset of the product line. This investment is expected to pay off at some point because of reusing from the core asset while developing each product that is part of the product line. This is represented by the payoff point in the chart. At the payoff point, the effort for developing the same amount of products as a product line is equal to the effort for developing each of them separately. For example, if the payoff point is reached for an amount of four products, then it means that the effort for developing those four products separately equals the effort for developing them as product line members. While the amount of products exceeds the amount at the payoff point, the effort for developing products as product line members decrease significantly in comparison to the effort of developing them specifically. Therefore, there are cost savings and economical benefits from the product line investment after the payoff point has been reached. In the example when the payoff point is reached for the fourth developed product, then it is reasonable to conclude that the product line investment will pay off starting with the development of the fifth product and onwards.

2.2 Functional Safety

2.2.1 Basic Concepts

Functional safety is a part of the overall system safety which depends on the correct response of the system when right inputs are entered. Safety is represented by all the regulations, means and mechanisms that focus on protecting system properties, human lives or environments from possible risks and dangers [9]. A system can never be considered to be 100% safe because there are always threats that might present risks and endanger it.
However, it is possible to prevent possible future risks and threats by protecting the system and applying safety mechanisms and concepts on it [9].

At Volvo CE, functional safety is considered for making sure that E/E (Electrical/Electronic) systems and machines are operating correctly in the environment.

The main purpose of functional safety is to mitigate or eliminate any risk that might endanger the system, the environment and most importantly, human lives and health. Such risks are considered unacceptable [9].

In order to achieve functional safety, the first step would be to identify all possible hazards in the system. A hazard is considered to be a potential source of harm for the system or the environment. Hazards can be caused as a consequence of a failure in the system. A failure is represented by the situation when the system or a part of the system becomes unable to perform and function correctly [10].

There is potential that hazards may lead to hazardous events. A hazardous event is an event with potential to lead to accidents and it is caused when hazards and relevant operational situations of the system are combined [10].

An example of a hazard is the situation when there is a malfunction in the brake-by-wire system of a truck. Such hazard can lead to a hazardous event e.g., the braking system may not work properly in case when there is traffic in the highway. As a consequence, the driver would not be able to stop the car and hence, an accident would be caused. The damage would include economical, environmental or in human lives [11].

After the hazards are identified, risk assessment techniques are performed in order to assess possible risks that present threats to the system and provide possibilities for mitigating such risks as much as possible [10].

Every step and lifecycle process undertaken for achieving functional safety needs to be performed according to recognised functional safety standards [9].

2.2.2 Functional Safety Standards

Functional safety standards are used nowadays as regulations by different domains in order to provide a basis for assessing safety lifecycle activities and certifying their products. A wide variety of functional safety standards are used depending on the domain type.

One of the most notable safety standards is ISO 26262 [10]. This standard has been proposed for safety assessment in automotive domains. Nevertheless, it is being investigated in other domains as well. This is also the case for the construction equipment product lines at Volvo CE. Although it is relatively new in industry, ISO 26262 is strongly based on previous functional safety standards.

2.2.2.1 ISO 26262

ISO 26262 is a functional safety standard for automotive E/E systems that has been adapted from the IEC 61508 standard [12]. It is structured in ten parts: (1) vocabulary, (2)
management of functional safety, (3) conceptual phase, (4) product development at the system level, (5) product development at the hardware level, (6) product development at the software level, (7) production and operation, (8) supporting processes, (9) ASIL and safety-oriented analysis, (10) guideline on the standard [10]. ISO 26262 considers the V-model-based development as in figure 3.

![Figure 3: The V-model according to ISO 26262 standard – Part 6 [10]](image)

However, it should be underlined that the V-model presented in figure 3 covers only the software development aspects. This corresponds to part 6 in the ISO 26262 standard [10]. Testing and verification is performed for safety requirements, safety architecture parts (high-level design), detailed design (components) and implemented parts as well.

The risks are evaluated in ISO 26262 by the ASIL value [10], (Automotive Safety Integrity Level). Depending on the situation, ASIL can be one of the following: QM, A, B, C and D. A represents the lowest risk level while D represents the highest. As for the risks defined as QM, they are usually not assessed and no safety requirements are needed to be defined for them. The ASIL is dependent on three variables: severity (S), probability (E) and controllability (C).

The severity level expresses the extent of the damage that is triggered by a situation. There are four levels of severity:

- $S_0$ (there is no damage caused by the hazardous event)
- $S_1$ (there is damage to some extent caused by the hazardous extent)
- $S_2$ (the damage cause is very severe and it can be even life-threatening but survival possibilities are still high)
- $S_3$ (the damage is extremely high and life-threatening and survival is not certain)

The probability level shows what possibilities exist that a failure may bring to a hazardous event. It includes five levels of probability:
• \( E_0 \) (it is very unlikely that such hazardous event can happen)
• \( E_1 \) (the hazardous event may be caused only by very rare operational conditions)
• \( E_2 \) (there is low probability that the failure might lead to hazardous event)
• \( E_3 \) (there is medium probability that the failure might lead to hazardous event)
• \( E_4 \) (there is high probability that the failure might lead to hazardous event which means that most of the operation conditions would favour a hazardous event)

Finally, the controllability level express what chances exist to handle the situation in case of hazardous conditions. Different levels are defined for it:

• \( C_0 \) (the situation is generally controllable)
• \( C_1 \) (the situation is controllable to a high extent)
• \( C_2 \) (the situation is controllable to some extent which means that it is possible to react on time and prevent accidents in most of the cases)
• \( C_3 \) (the situation is either not controllable or very challenging to control)

Table 1 presents the ASIL value depending on \( S, E \) and \( C \) [10].

<table>
<thead>
<tr>
<th></th>
<th>( C_0 )</th>
<th>( C_1 )</th>
<th>( C_2 )</th>
<th>( C_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( E_1 )</td>
<td>QM</td>
<td>QM</td>
<td>QM</td>
<td></td>
</tr>
<tr>
<td>( E_2 )</td>
<td>QM</td>
<td>QM</td>
<td>QM</td>
<td></td>
</tr>
<tr>
<td>( E_3 )</td>
<td>QM</td>
<td>QM</td>
<td>QM</td>
<td>( \uparrow ) A</td>
</tr>
<tr>
<td>( E_4 )</td>
<td>QM</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) B</td>
</tr>
<tr>
<td>( S_2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( E_1 )</td>
<td>QM</td>
<td>QM</td>
<td>QM</td>
<td></td>
</tr>
<tr>
<td>( E_2 )</td>
<td>QM</td>
<td>QM</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
</tr>
<tr>
<td>( E_3 )</td>
<td>QM</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) B</td>
</tr>
<tr>
<td>( E_4 )</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) C</td>
<td>( \uparrow ) C</td>
</tr>
<tr>
<td>( S_3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( E_1 )</td>
<td>QM</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) B</td>
</tr>
<tr>
<td>( E_2 )</td>
<td>QM</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) B</td>
</tr>
<tr>
<td>( E_3 )</td>
<td>( \uparrow ) A</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) C</td>
<td>( \uparrow ) C</td>
</tr>
<tr>
<td>( E_4 )</td>
<td>( \uparrow ) B</td>
<td>( \uparrow ) C</td>
<td>( \uparrow ) D</td>
<td>( \uparrow ) D</td>
</tr>
</tbody>
</table>

The values associated with a red arrow in table 1 represent the cases when there is a considerable risk in the system. In such cases, the ASIL takes one of the four values: A, B, C or D. In other combinations (ASIL=QM), no safety requirements are defined for the risks. It can be noticed that cases when at least one of the three factors takes its minimum value (\( S_0 \), \( E_0 \), or \( C_0 \) are considered safe.
Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study

$C_0$) are not evaluated and presented in table 1. The reason for that is because they are considered as QM level and thus, no considerable risk is assessed for such cases.

The ISO 26262 standard has started to be successfully applied in many industrial domains which are mostly automotive domains. However, there is high focus on investigating and analyzing it in order to propose ways for applying it in other industrial product lines, as well. An example for such effort can be found at Volvo CE in Sweden. Main functional safety standards applied for Volvo CE product lines include ISO 15998 [13] and IEC 61508 [12] which can be considered as the predecessor of ISO 26262 [10]. However, there is high effort on investigating ISO 26262 in the construction equipment context as well.

2.2.3 Risk Assessment Techniques

The system can be safe only by mitigating or if it is possible, by eliminating the hazards that presents threats for it [14]. For this purpose, several types of risk assessment techniques can be performed for avoiding and reducing the chances for hazardous events or accidents. Different risk assessment techniques are summarized in the next subsections.

2.2.3.1 Hazard Analysis

Hazard analysis aims to identify possible hazards in the system, define their significance in terms of endangering the system as well as the environment and finally, provide measurements for eliminating and mitigating the hazards and their effects [14].

Hazard analysis can be present in different software development phases. There are different types of hazard analysis:

1. PHA (Preliminary Hazard Analysis) can be performed right after the Requirements Specification phase and can identify hazards related to the industrial environment.
2. SHA (System Hazard Analysis) identifies hazards in the system level and can be performed after the High-Level Design phase.
3. SSHA (Sub-System Hazard Analysis) identifies hazards in the sub-system level (components) and can be performed after the Low-Level Design phase

PHA focuses on identifying hazards although there is no detailed information on the architecture of the system. For this purpose, it is considered as a preliminary analysis. Based on the limited system architecture information, system safety requirements (SSRs) are derived from the PHA [14]. Table 2 presents the criteria on how hazards are evaluated in the analysis. These criteria are the likelihood that the hazard can lead to hazardous event(s) and the severity of the situation.
SHA is performed after the high-level design constraints have been defined in the PHA. SHA uses the system safety requirements defined for each hazard identified in the PHA. Furthermore, SHA extends the results obtained by the PHA by focusing on the safety functioning of the system as a whole. Hence, interfaces between different components are evaluated and checked for possible hazards.

After the SHA is performed, the SSHA takes place for identifying hazards in the functions belonging to the different subsystems.

### 2.2.3.2 FMEA and FMECA

Other risk assessment techniques used in industry are FMEA (Failure Modes and Effects Analysis) and FMECA (Failure Modes, Effects and Criticality Analysis). They operate in three phases [15]:

1. The identifying phase where the failure modes of the system are evaluated by defining what caused them and what consequences they have.
2. The analysis phase where the risks are prioritized by defining the probability that a situation may bring to failure and hazard.
3. The solution phase where solutions are provided for eliminating the causes of the failures or at least for mitigating their consequences.

FMEA represents an analysis that focus on the functional aspect of the system or system parts. FMECA is an extension of FMEA which adds a criticality analysis. FMECA analyzes the likelihood of a failure mode based on the severity level that the effects of such failure mode might have. An FMECA is documented in the following way [15]:

---

**Table 2: Hazard evaluation in the analysis**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Severity</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Catastrophic</td>
<td>Critical</td>
<td>Marginal</td>
<td>Negligible</td>
</tr>
<tr>
<td>A Frequent</td>
<td></td>
<td>I-A</td>
<td>II-A</td>
<td>III-A</td>
<td>IV-A</td>
</tr>
<tr>
<td>B Moderate</td>
<td></td>
<td>I-B</td>
<td>II-B</td>
<td>III-B</td>
<td>IV-B</td>
</tr>
<tr>
<td>C Occasional</td>
<td></td>
<td>I-C</td>
<td>II-C</td>
<td>III-C</td>
<td>IV-C</td>
</tr>
<tr>
<td>D Remote</td>
<td></td>
<td>I-D</td>
<td>II-D</td>
<td>III-D</td>
<td>IV-D</td>
</tr>
<tr>
<td>E Unlikely</td>
<td></td>
<td>I-E</td>
<td>II-E</td>
<td>III-E</td>
<td>IV-E</td>
</tr>
<tr>
<td>F Impossible</td>
<td></td>
<td>I-F</td>
<td>II-F</td>
<td>III-F</td>
<td>IV-F</td>
</tr>
</tbody>
</table>
Table 3: Template for performing and reporting FMECAs

<table>
<thead>
<tr>
<th>Ref. no</th>
<th>Function</th>
<th>Operational mode</th>
<th>Failure mode</th>
<th>Failure cause or mechanism</th>
<th>Detection of failure</th>
<th>On the subsystem</th>
<th>On the system function</th>
<th>Failure rate</th>
<th>Severity ranking</th>
<th>Risk reducing measures</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the first three columns, a general description for each function of the system is provided in the operational perspective.

In the next three columns of the FMECA table, the possible failure modes for each function are described. Possible failure modes imply the functional requirements that have not been accomplished for a function in the system. Possible causes of the failure as well as possible ways to detect such failures are added respectively in columns 5 and 6. Possible ways to detect failures can be either automated e.g., diagnostic testing or non-automated e.g., through simple perception of failures by practitioners and so on.

The effects of the failures on the subsystem and system level are listed respectively in columns 7 and 8.

The rating for each failure takes place in the ninth column. The frequency of the failure is evaluated depending on the following designations:

1. Very unlikely – The failure might occur once every 1000 years or even less frequent than that.
2. Remote – The failure might occur once every 100 years.
3. Occasional - The failure might occur once every 10 years.
4. Probable - The failure might occur once each year.
5. Frequent - The failure might occur once each month or more frequently.

Column 10 includes the severity level for each failure. The severity level [15] can vary from 0 to 10 (table 4).
Possible solutions for reducing and mitigating the effects of each failure are proposed and listed in column 11.

At last, column 12 is reserved for additional information that could not be listed in the previous columns.

### 2.2.3.3 Fault Tree Analysis

FTA (Fault Tree Analysis) is a top-down technique [16] used to evaluate safety in a system design and check if there is the chance that this design may bring to possible failures in the future. Graphically, it is represented by several nodes that are connected as in a tree design. The hazard is positioned on the top (first level). The causes for this hazard come as nodes in lower levels and they can be connected by logical gates. An example of a FTA is presented in figure 4.

![Figure 4: Example of a FTA where two components fail because of an event](image)

In this case, event "A" is considered as a single point of failure which means that only this event is enough for causing the system to fail. In fact, the system can fail only if both components X and Y fail. The problem is that "A" can cause both components to fail since "A"
is connected to both "B" and "C" via AND gates. Hence, even if "B" and "C" do not cause failures, "A" is sufficient for bringing both X and Y to failure and thus, failing the system itself.

### 2.2.4 Safety Cases

A safety case represents all the documented argumentation that is needed for providing evidence that the safety level of a system is acceptable [10]. This implies that the system would function correctly in the right context without being a risk for the operating environment. In a safety case, there is always a safety goal that should be reached. The safety goal represents a first-priority safety requirement that aims to mitigate or eliminate system hazards. The safety goal can be reached only when enough evidence is provided and argumentation is needed in order to show how the evidence supports and helps on reaching the safety goal [10].

One of the most notable graphical representations proposed for safety cases is GSN (Goal Structure Notation) [17]. The general graphical template for GSN is presented in figure 5.

![Figure 5: General template for GSN argumentation [17]](image)

It should be considered that the template above represents the most simplified version of what GSN would look in a real case. At least one top level goal is defined at the beginning and it is usually related to the scope of achieving a safety level of the system. A strategy needs to be listed in order to mitigate the hazards in the system. Usually, a notation specifying the context for the strategy is added e.g., the context might specify that all hazards are identified in the system level or in another case, in a subsystem level.

A top level goal can be supported by one or several strategies. Each strategy is followed by one or several second level goals. Each of these goals aims to identify a specific hazard. FTAs are used for each hazard identified in the second level goals.
There are also cases when an identified hazard brings to the identification of other hazards as it is the case with the second level goals 1 and 2 in figure 5.

2.3 Considering Functional Safety in Product Lines

Several domains deal nowadays with issues of applying functional safety in their product lines. Functional safety is now part of many domain types including automotive industry, avionics, aerospace, railway, healthcare and so on.

Criticality is evaluated differently in different types of domains. For example, higher effort and cost is spent on avionics and aerospace since failures need to be always avoided. Less effort is put on other domains e.g., the automotive industry regarding the criticality level that needs to be assured.

Criticality can be also evaluated differently for different products that belong to the same domain. Some products may present more serious threats to the environment than other ones.

There is diversity in terms of applying functional safety in the geographical perspective, as well. There are different legislative regulations in different countries which the companies need to fulfil. For these reasons, different functional safety goals and requirements exist for the same product lines that are developed in different countries and planned for different target markets.

The number of domains that is considering functional safety for their software product lines is significantly increasing and there is a demand for evaluating how much effort is put on it and most importantly, if that pays off.
3. Research Method

3.1 Literature Study

The literature study we perform is necessary for getting an overview of existing studies on effort estimation in product lines and functional safety. In addition to this, the findings from the literature study are expected to answer the first research question RQ1 and its sub-questions RQ1.1-RQ1.3 that are presented in subsection 1.2. Regarding the method used for the literature study, we rely on the method proposed by Kitchenham et al. in [18]. However, we do not consider following explicitly every step in detail since the method in [18] is intended more for systematic literature review studies and that is not exactly the case for our literature study.

3.1.1 Literature Search

Specific search terms and keywords were used in order to start searching for literature and possible references. At the beginning, Google Scholar was the main search engine used for this purpose. However, several digital libraries were utilized as well for searching and collecting references. The most preferred ones were:

- IEEE
- ACM
- SpringerLink
- Elsevier

The most common keywords and search expressions used for searching were:

- “Cost Models in Product Lines” and/or “Economic Models in Product Lines”
- “Empirical Study Product Lines” and/or “Empirical Study Effort Software Product Lines”
- “Case Study Software Product Lines”
- “Effort Estimation Product Lines” and/or “Effort Expert Estimation Product Lines”
- “Safety Critical Product Lines” and “Safety Critical Product Line Development”
- “Functional Safety Product Lines” and “Functional Safety Product Families”

3.1.2 Literature Evaluation and Selection

More than 150 published papers, books and articles were found and gathered based also on first appearance from the search process that used the above keywords. At this step, a selection procedure was performed in order to choose the most suitable references. Hence, those publications that seemed to be completely out of the scope or not so helpful in our context were eliminated from the list of papers that were previously collected.

In most cases, abstract and conclusions were read in order to understand the main purpose and contribution of each published paper. Afterwards, the selection procedure was followed in order to choose the most suitable papers and discard the rest of them. The selection criteria
for the chosen papers consist in the fact that they would serve to at least one of the following purposes:

- Criterion 1: The paper describes concepts regarding software product lines.
- Criterion 2: The paper describes concepts regarding functional safety in product lines.
- Criterion 3: The paper describes guidance on conducting empirical studies, literature studies or industrial case studies.
- Criterion 4: The paper is about effort estimation in software product lines.
- Criterion 5: The paper fulfills at least two of the above criteria.

At last, 54 references resulted to satisfy the selection criteria. Table 5 shows their distribution according to the main selection criteria. Five references give an introductory view on product lines while ten more regard functional safety principles, standards and so on. The five studies in [18, 19, 20, 21, 22] are grouped according to criterion 3 because they include respectively guidelines on literature study, case study principles, case study design and research, interview study and finally, empirical studies in Software Engineering. Most of the references are grouped in the fourth column because they are related to effort estimation in product lines. In the final column, literature that includes at least two of the first 4 criteria is included. For example, reference [6] is about an industrial study in product lines. Hence, it satisfies both criteria 1 and 3. The other references in the fifth column are mostly industrial studies that apply product line cost models. Hence, such references satisfy criteria 1, 3 and 4.

<table>
<thead>
<tr>
<th>Criteria belonging to different criteria</th>
<th>Criterion 1</th>
<th>Criterion 2</th>
<th>Criterion 3</th>
<th>Criterion 4</th>
<th>Criterion 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1-3], [7-8]</td>
<td>[9-17], [54]</td>
<td>[18-22]</td>
<td>[23-26], [29-33], [35-36], [38-40], [42,53]</td>
<td>[6], [27-28], [34], [37], [41]</td>
<td></td>
</tr>
<tr>
<td>Total number of references</td>
<td>5</td>
<td>10</td>
<td>5</td>
<td>23</td>
<td>11</td>
</tr>
</tbody>
</table>

### 3.1.3 Literature Search Results

Figure 6 presents the distribution of different digital portals where the references have been extracted from. 16 papers (30%) are publications from IEEE Xplore Digital Library [5-6][8][29][32-33][41][43-44][46][48-53]. There are also six ACM publications [7][22-24][30][36] and eight Springer publications [1][4][9][19][26][31][37][40]. Moreover, there are four papers from Elsevier [18][28][34][47]. The last category includes 20 more references obtained by using the Google Scholar search engine. This category includes three published books [14][20-21], two Master thesis reports [2][45], four references related to safety standards and projects [10][12-13][54], and other research and technical papers that have been published in other digital libraries such as CMU [3][38][42], Citeseer [17][25], International Journal of Applied Software Technology [35], Fraunhofer Institute [39],
Most of sources are conference proceedings and journal papers. Nevertheless, there are a few other types as well that include seven technical reports [11][15][16][19][25][38][39], seven published books [1][3-4][14][20-21][23], two Master thesis reports [2][45] as well as four references related to safety standards and projects [10][12-13][54].

### 3.2 Conducted Studies

We have conducted three studies in order to investigate the effort for developing safety-critical software product lines in real industrial environments. We chose to rely on a multiple-case design (3 studies) for our empirical study in order to capture as many viewpoints as possible related to the subject. Moreover, another goal is also to provide strong evidence for the analysis and the derived results, as it is shown in figure 8.
3.2.1 Interview Study
The first study consists in eight semi-constructed interviews that were held at Volvo CE. Answering the second research question RQ2 which is defined in section 1.2 requires an investigation of effort on functional safety in industrial product lines. Since this is related to industrial effort, we cannot expect to investigate such effort through the literature study. For this purpose, we rely on a study that consists on performing semi-structured interviews with industrial experts at Volvo CE. We started to design the interview study after analyzing existing literature. Ten proposed software product line cost models [21-40] and software effort expert estimation methods [46-54] were reviewed.
We base the questionnaire for the interview study on SIMPLE model which is discussed in subsection 4.1.9, because it provides a detailed structure of the total effort by summing up the effort spent in the following six dimensions:

1. Organizational Effort  
2. Core Asset Base Effort  
3. The Effort for Unique Parts  
4. Reuse Effort  
5. Evolutional Effort  
6. Maintenance Effort

The main scope was to investigate the effort that is spent on each of these six dimensions in industry (i.e., at Volvo CE, in our case) and compare the results with the theoretical statements in existing literature.

Figure 9 gives an overview of the full structure of the interview study. The interview starts with some introductory questions are mostly related to the professional profile and the experience of the interviewee. In the second phase, the questions are about some general scenarios e.g., the changes between two product line generations, possible improvements and so on. Finally, the questions related to each of the above six dimensions are listed.
In the section related to organizational effort, we aim to investigate activities with highest impact on the organization in the safety perspective. In the section related to the core asset base effort, we ask questions to practitioners about the effort on developing common assets for product lines at Volvo CE. In the next sections, we investigate the effort on reusing several artifacts (including safety artifacts) in Volvo CE product lines as well as the effort on developing specific parts or unique products. Furthermore, the focus is put on estimating the effort for evolving Volvo CE product lines in newer generations. At last, we aim also to investigate the effort put on activities for maintaining industrial product lines while still focusing on the functional safety perspective.

Semi-constructed interviews were used instead of well predefined interviews in order to be able to adapt the questions to different contexts. The reason is that the practitioners who participated in the interview study have actually different professional profiles and backgrounds and consequently, different points of view on similar subjects. In total, we interviewed seven practitioners who covered different product line development aspects and phases. Most importantly, all the practitioners had knowledge and industrial experience on functional safety in product lines.

3.2.2 Survey Study
In the second study, a survey has been compiled in order to gather more feedback and investigate functional safety effort in other industrial domains rather than Volvo CE. This study can be utilized also to validate the results obtained from the interview study. In addition, it can also enrich the findings and results derived for safety effort estimation by analyzing more scenarios in different industrial domains.
Figure 10 shows the structure of the survey study. Basically, it consists of the same components that were applied in the interview study. The survey is organized in four pages. The first one is composed of several introductory questions that include also some general information regarding the corporation and its profile. The second page covers the part related to scenarios and the organizational effort while the part about the core asset base, unique parts and reuse effort is situated in the third page. At last, the evolutionary and the maintenance effort are included in the fourth page of the survey.

Before launching the survey online, we tested it with Volvo CE practitioners in order to receive feedback and make sure that the survey questions are understood by experts. During this testing process, the survey was refined many times.

The survey was launched and sent out to a considerable number of industrial experts in product lines as well as functional safety experts who were contacted via LinkedIn. The survey was available for four months after the date when it was launched for the first time.

### 3.2.3 Documentation Analysis

Different types of documentation related to product line development and safety assessment at Volvo CE are analyzed in order to identify and provide more evidence for supporting the results derived from the interview study. Providing more argumentation in this perspective is expected to increase the reliability of the conclusions and the final results of our work.
Different documentation that involves functional safety in Volvo CE product lines is considered for analysis in study 3. Such documentation includes safety plans, project plans, testing documentation, risk assessment documentation, functional safety standards and so on. The main goal is to proceed further with investigating functional safety effort in Volvo CE product lines which is also done in the interview study. At first, we aim to investigate the functional safety effort spent on each document. Such effort is however very hard to evaluate and it is very challenging to split it from the other efforts spent on documentation. For this purpose, the role of the document analysis consists mostly in providing further evidence to support the findings from study 1.

The method that we use for the documentation analysis in order to support interview results is illustrated in figure 11.

In the interview study, we extract and identify several issues and scenarios that have an impact on functional safety effort for Volvo CE product lines. Then, we analyze Volvo CE documentation in order to search for evidence that can support each issue and scenario that is identified from the interview study. The purpose is to provide argumentation for stating that each identified issue and scenario is relevant and this way, to validate the interview results.

In case that evidence is found in documentation for supporting a certain issue or scenario, then we provide more argumentation for the issue or scenario that was identified in the interview study.

In the other case that no evidence can be found, an analysis shall be provided for arguing about the reason why such evidence is missing in the documentation and why the results derived from the interviews can be considered as relevant for drawing relevant conclusions in that context. There might be several causes for not finding evidence in the documentation e.g., the documentation that we accessed was not sufficient for finding that evidence and so on.
4. Related Work

4.1 Software product line cost models

There are several proposed cost models that support effort estimations for product lines. The established cost models mostly consider the effort put on industry for embracing the product line approach i.e., passing from single product development to product line development, which is actually not really very common in current industrial context. In this study, we investigate how well existing cost models support the efforts for achieving functional safety in product lines as well as their general applicability.

Figure 12 provides an overview of the proposed cost models [23-45] and their relations we consider in our study. Each cost model is listed according to its release time (year). There are three models in the figure that are shown in white background: COCOMO [23], ICMSR [24] and COQUALMO [25]. They have not been included in our study since they do not provide any additional useful or substantial information that is not present in their extended versions (respectively COCOMO II [26] [27] [28], SoCoEMo-PLE [29] and qCOPLIMO [30]).

![Figure 12: Overview of proposed cost models in chronological order](image)

Depending on the complexity level and the attributes that it considers, a cost model can have 1, 2 or 3 layers. A 1-layer model relies on cost formula for performing estimating the effort in product lines. In addition to that, a 2-year model adds the evaluation of different industrial scenarios regarding effort estimation. In third layer, it is possible to perform an analysis for determining if an investment is beneficial or not. In order to do that, 3-layer models rely mostly on decision trees.

In order to estimate if and when an investment in product lines will pay off, proposed models rely either on ROI (return on investment) [31] estimation or NPV (net present value) [32] estimation. ROI value defines how efficient an investment is by comparing the benefits with the investment cost. Meanwhile, NPV focus on estimating the cash flow difference between the current situation when the investment is performed and the future situation depending on how the investment will pay off. ROI estimation is more suitable for short-term investments while NPV is used more for long-term ones.
Different cost models might have their primary focus on estimating different efforts. For example, the focus of some models might be mostly on software reuse while others evaluate the effort for developing a product line. There are cost models that consider estimating the effort for product maintenance while others do not.

Each proposed cost model is discussed and summarized in the next subsections.

4.1.1 COCOMO II

This model is an extension to COCOMO (Constructive Cost Model) [23] model and it has been adapted to perform cost estimations for different software development perspectives. The original COCOMO model (also known as COCOMO 81 because of being introduced in 1981) uses the number of source instructions (amount of physical lines of code) as inputs for the software effort estimations. Hence, the lines of code are counted one by one in the source code when estimating the effort for developing it and COCOMO 81 takes into account every single line despite the fact if that line is executable or not (e.g., a comment). Unlike its predecessor, COCOMO II uses the amount of logical lines of code for estimating software effort related to the developed code. A logical line of code is represented by an executable statement (e.g., “if” statements in C programming language). Therefore, non-executable code such as comment lines are excluded from the inputs considered for software effort estimations in COCOMO II. This represents a significant evolutorial change from the previous version of the cost model (COCOMO 81) which helps on increasing the estimation accuracy.

COCOMO II [26] was introduced 14 years after its predecessor in order to adapt to the significant evolutorial changes that affected software development approaches during those years (1981-1995). The most notable ones include the introduction of desktop development (which includes client-server applications, web application development and so on) and the possibility to reuse lines of code from software components. In this section, we do not focus on explaining in detail COCOMO 81 [23] since its most important characteristics are inherited and further improved in COCOMO II.

The original COCOMO 81 model provides cost functions and formulas which are reused and improved further in COCOMO II. The main purpose of introducing COCOMO II was to design a framework for collecting data extensively and to further improve the accuracy and ability to make effort estimations. COCOMO II estimates the cost advantages (or disadvantages) in case when the size of a project is increased [26] by relying on the following general formula:

\[
\text{Effort} = A \times (\text{Size})^B
\]  

(1)

The coefficient A (also known as adjustment parameter) has a defined value depending on the software project type. The formula above is suitable for large projects. Depending on the values that B (that represents the cost advantages/disadvantages) might take, different economical situations may be happening.

As it was already stated, COCOMO II extends the concept of COCOMO by improving the effort estimation. Moreover, COCOMO II estimates the adjusted person-month effort (based on the
nominal person-month effort) taking into consideration - the size of the project and exponent drivers:

\[ PM_{\text{adjusted}} = PM_{\text{nominal}} \times (\Pi_i \text{EM}_i) \]  \hspace{1cm} (2)

In the formula, \( PM_{\text{adjusted}} \) represents the adjusted person-month effort while \( PM_{\text{nominal}} \) represents the nominal person-month effort. \( PM_{\text{nominal}} \) equals the effort described in formula (2) which means that it depends directly on the size of the project. As for the EM (effort multipliers), they represent the exponent drivers which are cost factors that contribute in the overall software effort estimation. The input values for each cost factor are evaluated in a similar way as it was the case for AA and SU. The cost factors considered by COCOMO II for the software effort estimation are grouped in four categories [26]:

1. Product factors that include factors such as database size, product reliability, required reusability, the level to which documentation is suited to the needs of the software different lifecycles and so on.
2. Platform Factors that include parameters from the machine (both software and hardware) perspective such as execution time, storage constraint, processing times and so on.
3. Personnel Factors imply the experience and the capability of the people involved in the process e.g., the programmer’s experience in order to adapt the code for a new purpose.
4. Project Factors include other parameters related to the project such as the effort of adapting to the use of new project tools or to follow the required development schedule and so on.

In our literature study, it was possible to find studies where COCOMO II is applied in practice. One industrial study considers applying COCOMO (and COCOMO II) estimations in the software projects developed by NASA (National Aeronautics and Space Administration) [27]. Formula (2) which is listed above is utilized for estimating the software effort related to the developed lines of code at several NASA projects. Moreover, two extensions of COCOMO model are proposed in the industrial study that aims to increase the estimation accuracy of COCOMO by including more cost factors in the estimations. One important detail regarding this case of applying COCOMO estimations in practice is that the estimations of the software effort in the NASA projects resulted to be of high accuracy. This is confirmed by the evaluation of such estimations in [27].

One more industrial study is presented in [28] with focus on applying COCOMO II for estimating the effort on a software product in a company. Data from the project database are used as inputs for software estimation in this study. Formulas (1) and (2) are utilized for effort estimation. Furthermore, different inputs are given to the cost factors of COCOMO II. Afterwards, it is evaluated that the effort estimations are not very accurate. The reason for that is considered to be the fact that this was the first time that COCOMO II or any other cost-modeling approach in general was applied in the software products of the company.
Overall, the main focus of COCOMO II is on estimating the effort on either developing or reusing and adapting software lines of code. However, this cannot be considered very relevant in our context since estimating the effort on functional safety in product lines is definitely not limited to the effort put on software lines of code. Instead, it involves many artifacts and mechanisms such as safety concepts, architecture, documentation and so on.

4.1.2 COPLIMO

COPLIMO (The Constructive Product Line Investment Model) [33] is a product line cost model that has been designed as an extended version of COCOMO II [26]. This model evaluates the return on investment (ROI) for product lines. ROI [31] shows in percentage value how much an investment has paid off and it is calculated as following:

\[ \text{ROI} = \frac{\text{Economical Benefit}}{\text{IC}} = \frac{(\text{Profit from investment} - \text{IC})}{\text{IC}} \quad (3) \]

IC in formula 4 represents the cost of investing in product lines. Another advantage of COPLIMO towards its predecessor (COCOMO II) is that it investigates only the parts of the product that has been reused in order to make proper economical estimations for reuse. Hence, investigating the whole product is not necessary and the estimation time is reduced.

The COPLIMO model is compound of two important parts:

1. A Product Line Development Cost Model
2. An Annualized Post-Development Life-Cycle Extension

The first part i.e., the product line development cost model is responsible for calculating two cost factors: RCWR (Relative Cost of Writing for Reuse) and RCR (Relative Cost of Reuse). RCWR implies the extra effort put on writing software for product line development when compared to the situation when writing software for single product development. On the other hand, RCR includes the reuse cost for the software while it is being reused in the product line and this is compared to the effort needed if the software would have to be written for each single use.

In order to calculate RCWR, COPLIMO [33] uses the following inputs:

1. RUSE is the cost factor that represents the development for reuse and it can be rated in different levels (e.g., from very low to very high) and then, it can also have a quantified rating value.
2. RELY is the Requires Software Reliability parameter which can also be rated depending on the situation. For example, when the risk is high e.g., human lives can be endangered, RELY takes a very high value.
3. DOCU is a parameter whose value defines the effort put on the documenting the software that is being written for product line development purpose.

In order to calculate RCR, COPLIMO relies on COCOMO II formulas and increase further their estimation accuracy.
As for the second part of COPLIMO i.e., the Annualized Life-Cycle Model [33], it includes also the calculations for the maintenance cost. This is one of the most obvious advantages of COPLIMO since it covers also estimations for the effort put on a product line after it has been developed i.e., maintenance effort.

When reuse is considered in the life-cycle effort, the annualized maintenance size (AMSIZE) is estimated for three different cases and it depends on PSIZE, ACT and UNFM. PSIZE represents the size (lines of code) of the software. ACT and UNFM are two adjustment parameters of COCOMO II. The three different cases are:

1. When there is a specific software part in a product inside the product line, the product specific fraction (PFRAC) value should be included.
   \[
   \text{AMSIZE} = \text{PFRAC} \times \text{PSIZE} \times \text{ACT}(1 + \frac{\text{SU}_{100}}{} \times \text{UNFM})
   \]  

2. When there is a specific software part that needs to be changed and adapted in order to fit the context and work properly inside the product line, the adapted software fraction (AFRAC) value should be included.
   \[
   \text{AMSIZE} = \text{AFRAC} \times \text{PSIZE} \times \text{ACT}(1 + \frac{\text{SU}_{100}}{} \times \text{UNFM}) \times [1 + \text{AAF(N-1)}]
   \]  

3. When there is a specific software part that can be reused in a black-box style i.e., without internal changes inside the product line, the reused software fraction (RFRAC) value should be included.
   \[
   \text{AMSIZE} = \text{RFRAC} \times \text{PSIZE} \times \text{ACT}(1 + \frac{\text{SU}_{100}}{} \times \text{UNFM})
   \]

The introduction of the three parameters (PFRAC, AFRAC and RFRAC) helps on making industrial effort estimations more accurate. Of course, the accuracy strongly depends on the values that will be given to these parameters. The values vary depending on different projects and this can be considered as a drawback for complicating more the estimation.

A study [34] has been performed in order to improve estimations provided by COPLIMO and make it fit more in the product line context. In the original COPLIMO model, there are some assumptions made that facilitate the effort estimations but in the same time, they have a negative impact on the estimation accuracy. For example, it is assumed that there is equality in size between different products. This is expressed by formula (1) which is used by both COPLIMO and COCOMO II. In this formula, the situation of having products of different sizes in a product line is not considered and this represents a big issue in terms of effort estimation in product lines. However, the study in [34] addresses this issue and new formulas as well as algorithms are proposed for making COPLIMO more suitable in terms of estimating the effort in product lines rather than just focusing on the lines of code within single applications.

In our perspective, the same problem as with COCOMO II is identified. Main focus of COPLIMO is still on effort estimation in the software lines of code and that cannot be considered sufficient for investigating functional safety effort in software product lines. Furthermore, more detailed information and guidelines need to be provided regarding how to get the input...
values for cost parameters (e.g., PFRAC, AFRAC and RFRAC) when estimating software effort in industrial projects.

4.1.3 qCOPLIMO

This model [30] is an extended version of two proposed cost-modeling approaches: COPLIMO [33] and COQUALMO [25] which are both extensions of COCOMO II [26]. While the approach for the product line cost modeling part has been mostly based on COPLIMO, the part that handles defects has been extracted from the COQUALMO model. The essence of COQUALMO model is about considering the quality of software i.e., finding and mitigating software errors and defects. For this purpose, COQUALMO [25] is also known as COCOMO II Quality Extended Model. However, we do not focus on explaining COQUALMO as well, since the crucial part of it is incorporated in the qCOPLIMO model. Hence, qCOPLIMO considers software quality, as well.

![Figure 13: General Design of qCOPLIMO model [30]](image)

The general cost estimation formula used by qCOPLIMO [30] is:

$$C_{PL}(N) = C_{RCWR} + (N-1)C_{RCR}$$  \hspace{1cm} (7)

This formula performs the cost estimation for a product line that has N products. It uses the two cost factors: RCWR (Relative Cost of Writing for Reuse) and RCR (Relative Cost of Reuse) just as they are used in other cost models e.g., COPLIMO [33], Poulin's model [35] [36]. These two factors are used also for COCOMO II and COPLIMO. However, they are explained in more detail in the Poulin's model subsection (subsection 4.1.4).

The software quality approach [30] incorporated in qCOPLIMO (and COQUALMO [25] as well) investigates all the cost factors for possible defects. The cost factors are the same as the ones listed in COCOMO II. Some of them are designated by their abbreviations in figure 13 e.g., RUSE (required reusability), RELY (the reliability of the product) and so on. After the cost factors are investigated for possible defects, the found defects are submitted to be mitigated.
or corrected. The approach is usually not 100% successful, which means that some of the defects may remain, not corrected.

The software quality approach operates by using two mechanisms:

1. The Defect Detecting Mechanism, which takes the cost, factors as input and evaluates them for possible defects. This mechanism searches for defects in three perspectives i.e., requirements, architecture and implementation defects. As an output, the mechanism generates some requirements for trying to fix or mitigate these defects. Moreover, the risk associated with each defect is categorized as one of the following: Critical, High or Medium.

2. The Defect Removing Mechanism receives the requirements generated from the first mechanism, in order to start removing or mitigating the defects. At the end, this mechanism lists the defects that could not be removed. In the CQUALMO case (used also in qCOPLIMO), the approach results to be unsuccessful with a rate of 14 defects per 1000 lines of code.

As it was already underlined, one of the strongest points of qCOPLIMO is that it considers software quality as high importance. Moreover, the return on investment (ROI) is much higher in qCOPLIMO rather than in other cost-modeling approaches that do not focus on assuring software quality. A comparison with COPLIMO's ROI is shown in figure 14 where it can be obviously seen that qCOPLIMO is quite superior in this perspective.

![Figure 14: Comparison of ROI in COPLIMO and qCOPLIMO][30]

Having a quite improved ROI towards the one in COPLIMO [33] comes from the fact that qCOPLIMO [30] offers the opportunity to capture possible defects and fix them as well. After these fixes have been made, it is even easier to reuse different parts or components since the defects are no longer present in them. Moreover, higher quality and fewer (not fixed) defects imply lower effort for software maintenance and thus, higher cost savings.

In other words, considering software quality issues clearly pays off and it is quite convenient to include this attribute in a software product line cost model such as qCOPLIMO.

Although qCOPLIMO could have potential for application in industry and be very useful in an industrial context because of considering software quality, there is no study found in our
literature study that refers to a possible case of applying the model (at least the part that addresses software quality issues) in practice.

Since qCOPLIMO is a software quality-oriented cost model, we focused mostly on summarizing the defect detecting mechanism of the model which represents its main contribution. However, it should be considered that cost functions and effort estimations in the model are inherited by COCOMO II and COPLIMO. As we previously explained for the first two cost models, such cost functions and effort estimations have been already utilized by several industrial studies.

4.1.4 Poulin’s Model

This cost model focuses on estimating the cost advantages that are obtained by reusing software in product lines in comparison to single product development.

As it was the case with COPLIMO and qCOPLIMO, Poulin’s model considers calculating the Return on Investment (ROI) factor. According to this model, the ROI value increases each time when a developed common asset or artifact is being reused. Meanwhile, an extra effort put on maintenance because of some errors that could be avoided has a negative impact on ROI. Therefore, ROI is affected positively by a high RCA (Reuse Cost Avoidance) and a low ADC (Additional Development Cost). The appropriate relation between these three concepts is as following [35]:

\[
\text{ROI} = \sum_{i=1}^{n} \text{RCA}_i - \text{ADC}_n
\]  

The number \( n \) in the formula represents the number of times that the common artifacts can be reused after they have been developed in order to be included in the core asset.

In order to perform software effort estimations, Poulin’s model [35] uses RCR and RCWR parameters as in COPLIMO. Apart from their main roles that were explained above, RCR and RCWR are also necessary for calculating two important cost functions [35]:

1. RCA (Reuse Cost Avoidance)
2. ADC (Additional Development Cost)

RCA is a function that is used for evaluating and quantifying the benefits of reuse by comparing them to the situation of developing new content for each application or project. On the other hand, ADC [35] is a function that evaluates the effort that is needed for developing common artifacts i.e., the content that is built with the purpose of being reused later on.

RCA calculation consists in two sub-functions: DCA (Development Cost Avoidance) and SCA (Service Cost Avoidance).

Hence, the following relation is true [35]:

\[
\text{RCA} = \text{DCA} + \text{SCA}
\]  

(9)
DCA (Development Cost Avoidance) estimates the economical benefits that come from reusing software parts by relying on the number of lines of code that are reused and the effort for reusing them.

SCA (Service Cost Avoidance) expresses the benefits in the maintenance perspective by comparing it to the effort needed for maintenance that is now reduced or mitigated thanks to the process of reusing different artifacts. SCA calculation depends also on the error rate i.e., the frequency of errors that are needed to be located and mitigated after the product has reached the market which makes maintenance activities more complex and harder to perform. It also depends on the effort and cost that is needed to locate and mitigate these late errors.

As for the other cost function, ADC (Additional Development Cost), it consists on the effort for developing the core asset with common artifacts compared to the one needed for developing single-purpose ones. Therefore, it relies on the RCWR parameter. ADC is proportional to the (RCWR-1) value since it gives a percentage value. It is also proportional to RSI (reused source instructions) and the effort for writing new lines of code (NewLOC). Hence, ADC is calculated in the following way [36]:

$$ADC = (RCWR - 1) \times RSI \times NewLOC$$  \hspace{1cm} (10)

RCR and RCWR calculations from Poulin’s model are utilized in a study [37] for estimating the effort on software reference architectures when improving architecture-related decisions in different domains. However, this study relies on other existing product line cost models as well (e.g., SIMPLE which is discussed in subsection 4.1.9) in order to get more information regarding what costs and efforts to consider when estimating the overall effort on software architecture in product lines.

An advantage of Poulin’s model compared to the previous three proposed models is the fact that it considers different basic product line scenarios (e.g., estimating the benefits of investing in a product line compared to the effort spent on single development). Moreover, Poulin’s model provides guidelines regarding the input values for cost estimations e.g., the input value for RSI will be the amount of source instructions that are being reused and adapted in a new software code. Nevertheless, this model may present big challenges for estimating functional safety effort since it is proposed mostly for effort estimation of software reuse in the coding perspective.

### 4.1.5 SoCoEMo-PLE

SoCoEMo-PLE [29] is another extended software product line cost model that relies on two established cost models: Poulin’s model [35] and The Integrated Reuse Cost Estimation Model (ICMSR) [24]. ICMSR is a cost model that evaluates the case when a company needs to make a decision for either embracing software reuse or not. This decision making is evaluated in four perspectives (Component, Application, Domain and Corporate level).

Moreover, SoCoEMo-PLE considers the different lifecycle phases of software development (requirements, architecture and implementation) within the product line engineering
paradigm. A big difference between SoCoEMo-PLE and its predecessors (Poulin’s model and ICMSR) is the fact that SoCoEMo-PLE has actually been designed and modelled in UML. This has presented the opportunity to actually simulate this cost model for product lines. Such an option is not possible in most of the previous cost models.

SoCoEMo-PLE evaluates the reuse process in four different dimensions that correspond to the four perspectives considered in ICMSR [29]:

1. Component Engineering
2. Domain Engineering
3. Product Engineering or Application Engineering
4. Corporate Engineering

The evaluation of software effort is done in the above four dimensions in order to handle reuse in the main four perspectives: reuse of several components, reuse of different artifacts that are developed in the domain engineering processes, reuse of different artifacts that are integrated and used in the application and reuse effort seen in the perspective of the corporate. There are four stakeholders that play a crucial role in each perspective [29]:

1. The Component Engineer evaluates the effort for reusing several components. Therefore, he analyzes if it is more beneficial to reuse and integrate them rather than developing them from the beginning.
2. The Domain Engineer evaluates if it is worthy to develop some artifacts that are part of some Domain Engineering processes (such as requirements, architecture parts, code, tests and so on).
3. The Application Engineer makes an analysis of the effort that is needed for applying a product line approach in one application.
4. The Corporate Engineer is the person who analyzes the effort that would be needed for the corporate to adopt a product line approach and evaluates if it is beneficial to adopt it.

The UML modeling of SoCoEMo-PLE cost model [29] represents a big advantage since it helps on considering many situations and points of view in a complex domain. The modeling process starts with gathering requirements and models them as use cases. These use cases are related to the four stakeholders that are listed above. Afterwards, analysis phase takes place where each of the functions that are applied by the stakeholders is explained in details. These functions include:

1. The possibility for the stakeholders (Component, Domain, Application and Corporate Engineers) to make changes in the data e.g., the Component Engineer can make updates to different components.
2. The possibility for the stakeholders to perform effort estimations and calculations e.g., the application engineer can estimate the cost and effort needed for developing and integrating the application.
3. The possibility for the stakeholders to track some archived information that may include estimations for previous components, domains, applications and corporates.
In order to make proper effort calculations and define when the investment for a product line approach really pays off, the following economical parameters are taken into consideration [29]:

1. NPV (Net Present Value)
2. ROI (Return on Investment)
3. PI (The Index of Profitability)
4. ARR (Average Rate of Return)
5. PB (Payback Value)

The values associated to the above economical parameters need to be positive if we want to conclude that a certain investment has resulted to be beneficial and has actually paid off. Regarding the time that is needed to pass until it actually pays off, it is determined by the PB value e.g., PB=1 means that it will pay off one year after the investment will be performed.

Although no evidence was found in our literature study regarding any industrial use of SoCoEMo-PLE, it should be taken into consideration that SoCoEMoPLE inherits the cost functions from Poulin’s model. Since the study described in [37] uses Poulin’s cost functions, it is relevant to conclude that SoCoEMo-PLE cost functions are applied in the same study.

An advantage of SoCoEMo-PLE compared to the previous four cost models is the UML model which considers different viewpoints and situations in product lines. However, the fact that Poulin’s cost estimations are utilized in SoCoEMo-PLE brings to the conclusion that the cost estimations are fitting more for software effort estimation in logical lines of code.

### 4.1.6 Withey’s Model

The model Withey proposes in [38] is an economic model for performing an investment analysis by utilizing decision trees. The main purpose of this cost-modeling approach is to provide a solution for identifying the common software artifacts that are worthy to be developed in several products. Different common software artifacts require different development or integration effort. Withey’s model focuses on performing a detailed investment analysis in order to estimate the cost advantages when developing products as a product line compared to single product development. This way, it can be determined if developing common software artifacts either pays off or not.

Withey’s model provides a cost equation for calculating the economical benefits obtained by relying on a product line approach [38]:

\[ E_M = \sum_i^M \sum_j^V (y_{ij} \cdot w_{current}) - \sum_i^M \sum_j^V (y_{ij} \cdot w_{assets}) \]  

(11)

\( E_M \) represents the economies of scope for \( M \) assets, \( y \) is the effort in quantitative value, \( w \) is the unit used for the effort (e.g., man-hour), \( M \) represents how many software assets are in the portfolio and \( V \) is the amount of products that are planned for the product line.

In order to evaluate options for investment opportunities, the model relies on the Net Present Value (NPV) value that is calculated as following [38]:
Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study

\[ \text{NPV} = \sum_{t=0}^{n} \frac{C_i(t) - C_o(t)}{(1+r)^t} \]  

\( t \) represents the time period of duration for the investment. \( C_i \) represents the cash inflows i.e., the economical benefits of the company because of the investment while \( C_o \) represents the outflows i.e., the economical loss of the company because of the investment. \( n \) is a value that represents how many periods are actually planned and \( r \) is the opportunity cost of the capital.

The main idea is that the company should continue on performing the investment only if NPV has a positive value (NPV > 0). This equation presents some drawbacks, as well. For instance, uncertainty in several situations is not considered. An example would be the case when the interest rate changes and this is not captured in the formula. In this perspective, it can be concluded that the equation is not very dynamic [38]. Nevertheless, estimating the NPV value represents an advantage towards many other models (e.g., COCOMO II, COPLIMO, qCOPLIMO, Poulin’s model and Boeckle’s model).

As we previously stated, Withey’s model applies decision trees for evaluating possibilities of investments and helping on making the right choice. Figure 15 presents a decision tree for evaluating if it is beneficial to invest on building the architecture of a product line and later on, implementing this architecture.

![Figure 15: Decision tree illustration used in Withey’s model [38]](image)

The first node (1) represents the first decision about investing or not on the architecture. In order to make the right decision, the uncertainty should be evaluated as well. In the main case, the first uncertainty is depicted by (A) in figure 15 and it has to do with the fact if the architecture meets the requirements. The probability that it does is (a) while the probability that it does not meet them is (1-a). In case that the requirements are not met, it is better to stop investing in order to avoid further cost disadvantages. In case that the requirements are met, it is time for decision (2) that is about whether investing or not on implementing the architecture that was approved in decision (1). The probability that the market is promising (for the implemented components) is denoted by (b) while the opposite case is denoted by (1-b). A promising market brings to cost advantages while a bad market influences the cost...
negatively. In this case (figure 15), the NPV for estimating the economical benefits obtained by investing on implementation is calculated as follows:

\[
\text{NPV(impl.)} = \frac{-\text{INVimpl} + b \times (\text{Economical Benefits} + \text{IS}) + (1 - b) \times (\text{Economical Benefits} - \text{IS})}{(1 + \text{R2})^{\text{T2}}}
\]  

(13)

Regarding the investment analysis on architecture, the NPV is calculated as follows:

\[
\text{NPV(arch)} = \frac{-\text{INVarch} + a \times \text{NPV (impl.)} + (1 - a) \times 0}{(1 + \text{R1})^{\text{T1}}}
\]  

(14)

R1 represents the opportunity cost of the capital of the industrial domain at the moment when a decision needs to be made on whether investing or not on the architecture. R2 represents the same cost factor at the moment when a decision needs to be made regarding investment on implementation. T1 is the time that has passed (in years) from the architecture investment till the moment when the decision on implementation investment is made (i.e., from point 1 to 2 in figure 15) while T2 represents the time passed from the moment when the investment on implementation was performed (the right part of figure 15 i.e., from point 2 and onwards).

The NPV calculation for the situation is performed from the right side of the decision tree to the left one (i.e., at first for implementation and then, for architecture). If NPV(impl.) results to be very high, then it is better to proceed with the investment on implementation. If the value results to be low and there is high level of uncertainty between industrial experts on rather to proceed, then choosing to wait instead of proceeding right away with the implementation would be the best choice.

In general, decision trees define if the investment is worthy to be undertaken and they rely on probabilistic estimated values as well.

Although no industrial application of Withey’s model could be identified in our literature study, the investment analysis approach introduced in this model represents a big contribution in comparison to other product line cost-modeling proposals. Moreover, this analysis helps on evaluating different product line scenarios and situations which could be very helpful in the functional safety perspective since safety effort estimation would require the evaluation of different safety-related scenarios in an industrial context. The model provides also guide on how to obtain the input values by referring to the decision tree for estimating NPV. The problem with this estimation is that it is limited in industrial scenarios since it captures only short-term changes in industry while it does not take into account the long-term ones such as the change of interest rates and so on.

4.1.7 Schmid’s Model

The structure of this model consists of three layers that are considered for an investment analysis. Each upper layer can be seen also as an improved version of the layer below that.
In the first layer, the model gives us the opportunity to analyze if an investment is beneficial.

In the second layer, additional issues such as monetary and time constraints in terms of software reuse are taken into consideration.

On the third layer, a risk assessment is performed evaluating and defining possible risks for different product line scenarios. Therefore, the 3-layer model provides a comparison of different investment scenarios. Furthermore, it also includes a decision tree analysis, which gives the opportunity to evaluate and compare different options and choose the appropriate one depending on the situation.

Schmid’s model provides its own product line strategy, which is shown in Figure 16.

![Figure 16: Product line strategy performed by Schmid’s model [39]](image)

As we can see from figure 16, the strategy starts with analyzing the market and defining its segments that serve as a better target for the product lines that will be developed. The next step would be to define prices for each product. Afterwards, an overall quantitative analysis should take place in order to predict the associated cost for preparing the product line for the market. At the second level, product evolution is considered and a more specified analysis takes place in order to match each specific product with a market segment. Defining the product evolution implies also to define the variability of a product line and the expected time when each variant is supposed to be ready for the market.

Applying Schmid’s model in practice requires the evaluation of different scenarios. According to the model, a scenario can belong to one of the following scenario categories:

- **Product Line Scenarios**
- **Development Scenarios**

The product line scenario defines the product portfolio itself while the development scenario consists in the activities that altogether comprise the whole process of developing the actual product line. Generally there are two feature reuse scenarios that need to be analyzed for each case:
1. The feature can be developed as a reusable feature to fulfil the needs of more than one product.
2. The feature can be developed for a first product. Later, general parts of it may be used for building a reusable asset to be applied in other products.

Schmid’s model uses the same conventional decision tree design as in Withey’s model [38]. In Schmid’s case, the decision tree is combined with possibilities that characterize different product line scenarios. These possibilities can be of different types:

1. Possibility for expansion i.e., there is space for investments in the future.
2. Possibility for dropping the project that is being invested because of not sufficient economical benefits.
3. Possibility for waiting before investing i.e., postponing the investment in a later phase.
4. Possibility for flexibility i.e., being flexible when developing e.g., some components may be implemented in a different way than the one that was previously defined.

Another characteristic of Schmid’s model is that it considers different viewpoints when evaluating a product line strategy. For example, the following roles exist when an organization is deciding to introduce new parts in a product line:

1. The project manager is concerned about the time that takes to apply these parts in the product line.
2. The testing manager is concerned about the effort put on testing the new parts and the way how they affect the overall system.
3. The organization management board (responsible for the product line) analyzes and checks how often (how many times per year) new parts are introduced in existing product lines in the market.

Guidance on how to apply the model in industry is provided by Schmid in [39] while using an example on how to get the inputs for estimating the benefits of making an investment decision.

The main contribution of introducing this product line cost model includes the evaluation of different development and product line scenarios by using the decision trees as well as considering risk assessment for investment decisions. Nonetheless, going through more specific industrial scenarios and performing an investment analysis for them would fit better the functional safety context in industry which involves many specific industrial scenarios and situations.

4.1.8 Boeckle’s Model (A Cost Model for Software Product Lines)

This model proposed by Boeckle et al. [40] focuses on analyzing several situations when a company embraces the product line approach and when it decides to make changes to existing product lines, as well. Scenarios are considered in Boeckle’s model and different cost calculations are provided for each scenario. The model evaluates if it is beneficial to apply the product line approach in a specific context. Furthermore, the concept proposes methods to
investigate if merging two different product lines can increase the efficiency and if the products should be developed in a specific order to increase cost efficiency as well.

Boeckle’s model is considered as a 1-layer model [40], which implies that it covers quick calculations for different situations. On the other hand, it does not focus on the second layer (as in Schmid’s model) that comprises more planning and a better analysis of the industrial context where the model is going to be performed. The cost estimations are based on three main cost functions:

- The unique cost function \( C_{\text{unique}} \)
- The core asset base cost function \( C_{\text{cab}} \)
- The reuse cost function \( C_{\text{reuse}} \)

The unique cost function \( C_{\text{unique}} \) comprises the effort required for developing both products that are not product line members and unique parts as well that are included in a product line.

The core asset base function \( C_{\text{cab}} \) comprises the effort required for developing the common assets that will be used and adapted for the product line members. The reuse cost function \( C_{\text{reuse}} \) implies the effort put on adapting common assets in order to use them for several products within the product line.

Generally, the total cost for developing a product line is calculated as the sum of the three cost functions above [40]:

\[
C_{\text{PL}} = C_{\text{unique}} + C_{\text{cab}} + C_{\text{reuse}} \quad (15)
\]

Each specific scenario is associated with the respective effort calculation formula (that combines the three cost functions). For instance, the effort for developing a product line from scratch (with \( n \) products), is estimated according to the following formula [40]:

\[
C_{\text{PL}} = C_{\text{cab}} + \sum_{i=1}^{n} (C_{\text{unique}}(P_i) + C_{\text{reuse}}(P_i)) \quad (16)
\]

Other scenarios include: the situation when products that are already developed separately can be tailored within a new product line approach, the situation when two or more product lines might be merged into one in order to decrease the cost, the situation when a new product is about to be developed and an analysis is needed to define if it is more beneficial to include it in a product line or develop it separately, the situation when a new product line is about to be developed while using some parts from existing product lines and the situation when a product that was intended to join a product line is in fact removed from it and its cost or benefits should be estimated.

An extended version of Boeckle’s model is proposed in [41]. This extension addresses the problem of estimating the effort for safety certification in product lines. It is relevant to highlight that this is the only cost model found in our literature study that considers safety certification. Basically, formula (16) has been extended by including two more cost areas: one for the effort put on certifying the products and the other one for the effort put on re-certifying them. The downside is that the model provides safety certification effort estimation
only for the scenario when a software product line is considered to be developed in a domain. Such scenario is happening seldom in industry nowadays since most of domains have already applied and developed product lines and now, they mostly deal with changes and evolution of their existing product lines. Another drawback is that this extended cost model has not been tested yet in an industrial domain that deals with safety certification.

The benefits of introducing the cost model for software product lines by Boeckle et al. include the categorization of product line effort in three areas (core asset base, reuse and unique effort) as well as the possibility to estimate cost in different industrial scenarios. Hence, Boeckle’s model is cost function-based model as well as a scenario-based one. The problem regarding tailoring the model for industrial application is that no detailed instructions are provided for estimating the input values for $C_{cab}$, $C_{reuse}$ and $C_{unique}$ in industrial situations.

**4.1.9 SIMPLE**

SIMPLE (The Structured Intuitive Model for Product Line Economics) [42] is another software product line cost model, which aims to estimate the cost and the benefits of developing product lines in a company. The main purpose is to evaluate if developing product lines is beneficial in a specific context. It evaluates which product line strategy can be applied (e.g., embracing a product line approach or evolving single developed products) and if it is appropriate to build specific core assets with common artifacts.

The SIMPLE cost model includes four basic functions and two additional ones:

1. $C_{org}$ which is the cost related to the organizational effort.
2. $C_{cab}$ which is the cost related to the effort needed for developing the core with common artifacts.
3. $C_{unique}$ which is the unique cost for the unique parts in some specific products or the effort for developing whole specific products.
4. $C_{reuse}$ which is the reuse cost i.e., the effort put on integrating the parts that are being reused in a certain context.
5. $C_{evo}$ which is the evolution cost i.e., the effort needed on adapting the product line while going from a previous generation to a new one.
6. $C_{maintenance}$ which is the maintenance cost i.e., the effort put on each maintenance activity that is performed for maintaining the product line after it has been developed.

In comparison to most of other cost models (excluding Poulin’s model and COPLIMO), Simple takes both maintenance efforts and product line evolution into consideration (the two additional factors). SIMPLE evaluates software product line efforts and benefits in different scenarios, which supports product line decision makers with less experience. Furthermore, it also estimates the ROI (Return on Investment) [43] that is obtained when a company uses a product line approach instead of single product development.

The following product line situations are considered as scenarios for SIMPLE:

1. The situation when a company decides to develop (introduce) a product line.
2. The situation when it is needed to compare the effort for developing a product line with the one for developing products in separate mode.

3. The situation when it is needed to estimate the effort for evolving a specific product that is actually part of a product line.

4. The situation when a company has already some single developed products and should make a decision on whether to evolve them as single products or adapt them into a product line approach (depending on which alternative leads to higher cost savings).

5. The situation when it is necessary to estimate the ROI (Return on Investment) obtained by using a product line approach instead of single product development.

6. The need to calculate the effort for evolving a software product line i.e., passing to a new generation.

7. The need to calculate the effort for reorganizing the products in a different way within existing product lines.

8. The need to calculate the effort for adding a new product to a product line.

9. The need to decide about whether it is more beneficial to build or buy new products that are about to be added to a product line.

SIMPLE provides cost estimations for each scenario:

1. The first scenario has to do with the effort that an organization has to put in order to pass from a single product development to a product line engineering approach. If it is assumed that there are \( n \) products in the product line and \( T \) is the amount of time needed for the process, the effort for adapting the product line approach would be:

\[
C_{\text{PL}}(T) = C_{\text{org}}(T) + C_{\text{cab}}(T) + \sum_{i=1}^{n} (C_{\text{unique}}(P_i, T) + \text{Creuse}(P_i, T))
\]

(17)

2. The second scenario analyzes if the applying the product line approach results to be beneficial by comparing the effort for it with the effort that would be needed for developing the same amount of products (\( n \) products) in a single mode. In case that the effort for the product line approach is lower, then the benefits are calculated as the following:

\[
\text{Benefits} = \sum_{i=1}^{n} C(P_i, T) - [C_{\text{org}}(T) + C_{\text{cab}}(T) + \sum_{i=1}^{n} (C_{\text{unique}}(P_i, T) + \text{Creuse}(P_i, T))]
\]

(18)

In case that the effort for the product line approach exceeds the one for the single product development, then there would be no benefits but losses that are calculated with the following formula:

\[
\text{Loss} = C_{\text{org}}(T) + C_{\text{cab}}(T) + \sum_{i=1}^{n} (C_{\text{unique}}(P_i, T) + \text{Creuse}(P_i, T)) - \sum_{i=1}^{n} C(P_i, T)
\]

(19)

3. The third scenario includes the estimation of the effort needed for updating one product within the product line. Since a new version of it will be produced, the core asset base needs to evolve \( (C_{\text{cabu}}( ) \) since new common artifacts may be developed. Moreover, new specific parts may be developed for this product \( (C_{\text{unique}}( ) \) and other
parts can be reused as well \( (C_{\text{reuse}}( )) \) from the new common artifacts. Therefore, this effort is calculated this way:

\[
C_{\text{update}}( ) = C_{\text{cabu}}( ) + C_{\text{unique}}( ) + C_{\text{reuse}}( ) \quad (20)
\]

4. The fourth scenario evaluates if it is more beneficial to introduce a product line approach or evolve the existing single developed products. In case that there are some economical benefits from the introduction of the product line approach, then they are calculated this way:

\[
\text{Benefits} = \sum_{i=1}^{n} Cevo(P_i) - [C_{\text{org}}( ) + C_{\text{cab}}( ) + \sum_{i=1}^{n} (C_{\text{unique}} (P_i) + C_{\text{reuse}} (P_i))] \quad (21)
\]

5. The fifth scenario estimates the ROI (Return on Investment) that is obtained by introducing the product line approach. ROI is calculated as the division of the benefits that were estimated in scenario 4 with the investment cost that is considered to be the sum of the organizational and the core asset base cost:

\[
\text{ROI} = \frac{\text{Benefits}}{\text{Investments}} = \frac{\text{Benefits}}{C_{\text{org}}( ) + C_{\text{cab}}( )} \quad (22)
\]

6. The sixth scenario analyzes if it is worthy to develop products in a product line fashion over NP number of time periods compared to their development in a single mode for the same amount of time periods. In case that there are benefits, they are calculated by the following equation:

\[
\text{Benefits} = \sum_{T=1}^{NP} \sum_{i=1}^{N} C(P_i, T) - \sum_{T=1}^{NP} (C_{\text{org}}(T) + C_{\text{cab}}(T) + \sum_{i=1}^{n} (C_{\text{unique}} (P_i, T) + C_{\text{reuse}} (P_i, T))) + \sum_{i=1}^{S} C(P_i, T)] \quad (23)
\]

7. The seventh scenario takes into consideration the issue of organizing the products in the product line in a way as optimized as possible so the effort for developing and maintaining them should be minimized. The following equation estimates the effort for \( N \) product lines and \( S \) single developed products. \( NP \) is the number of time periods and \( N_j \) represents the number of products in the \( j \)th product line.

\[
\text{Effort} (N, N_j, S_x) = \sum_{T=1}^{NP} \sum_{i=1}^{N} (C_{\text{org}}(T) + C_{\text{cab}}(T) + \sum_{i=1}^{n} (C_{\text{unique}} (P_i, T) + C_{\text{reuse}} (P_i, T))) + \sum_{i=1}^{S} C(P_i, T)] \quad (24)
\]

8. The eighth scenario estimates the effort for adding some products in a product line that has been already developed and applied in an industrial domain. The following relation calculates the effort for adding a new product in a product line (PL):

\[
C_{\text{add}}(P_x) = C_{\text{org}}(T) + C_{\text{cab}}(T, PL, P_x) + C_{\text{unique}}(T, PL, P_x) + C_{\text{reuse}}(T, PL, P_x) \quad (25)
\]

9. The ninth scenario estimates and compares the effort for developing certain artifacts with the cost of buying them while they are already developed. In this case, the core asset base cost i.e., \( C_{\text{cab}}(T) \) determines everything.
The value for ROI is calculated by dividing the cost savings with the investment cost \([43]\). The cost savings are calculated by comparing the cost needed for developing a product line \(C_{PLdev}\) and the cost needed for evolving all the products in single mode. Hence, the cost savings are estimated by the following formula:

$$C_{SAV} = \sum_{i=1}^{n}[C_{evo}(Pi)] - C_{PL}$$  \hspace{1cm} (26)

When investing for developing a product line, there is significant effort on the organizational side for adapting to the new context as well as on developing common development artifacts:

$$C_{INV} = C_{org}() + C_{cab}()$$  \hspace{1cm} (27)

Finally, ROI is calculated by the following formula:

$$ROI = \frac{C_{SAV}}{C_{INV}} = \left[\sum_{i=1}^{n}[C_{evo}(Pi)] - C_{PL}\right] / \left[C_{org}() + C_{cab}()\right]$$  \hspace{1cm} (28)

Guidelines for applying the scenario-based SIMPLE cost model in practice are provided by Clements et al. in \([42]\). In most cases, holding a workshop with industrial experts is considered to be the best solution for managing to apply SIMPLE in an industrial context. At first, a general discussion with experts should take place in order to investigate product lines that are developed by them and derive industrial scenarios that involve such product lines. The next step would be to provide effort estimations for each identified scenario. This has to be validated and reviewed by the industrial experts in order to check if there has been any misconception regarding the cost areas attributed to each industrial scenario. Next challenge is to provide the input values for each cost area (e.g., the organizational effort when a new generation of a product line is introduced). Such inputs can be derived by discussing with the right practitioners (e.g., they can state the amount of time and people that contributed, the training activities held for the new generation and the effort put on them and so on). After the input values are defined, they are used for performing the cost estimations based on the formulas defined previously for each scenario. The results need to discussed and verified again by the practitioners.

SIMPLE model provides a good structure of the overall product line cost by decomposing the total cost in several cost components and areas. In comparison to most of other models, SIMPLE provides and evaluates more industrial scenarios. A big advantage is that it also explains how to get the input values for product line effort estimations. In this perspective, we can consider this model as more suitable than the previous eight ones for being adapted in a safety-related context. Nevertheless, more scenarios would be necessary for evaluating functional safety effort in different industrial situations. Moreover, one more drawback is that SIMPLE does not consider that some cost areas might affect each other and hence, interdependencies may exist. In addition, SIMPLE model provides no sufficient information for considering the effort in different product line development perspectives (e.g., effort in domain engineering and effort in application engineering).
4.1.10 InCoMe

As it was the case also with Boeckle’s model and SIMPLE, InCoMe (Integrated Cost Model for Product Line Engineering) [44] provides product line effort estimations by decomposing the total effort in several areas and evaluating the effort in different scenarios. Apart from a scenario-based cost modeling approach, InCoMe provides also an investment analysis, which is necessary to determine if an investment is going to pay off. The model is structured in three layers: Cost Factors Layer (bottom layer), Viewpoints Layer (middle layer) and Investment Analysis Layer (top layer). The model structure works in such way that each layer should provide necessary information (estimation, calculations and so on) to the layer above (figure 17).

![Figure 17: Structure of the InCoMe Model](image)

The cost functions in InCoMe are similar with the ones in SIMPLE [42]. The difference is that SIMPLE considers both the effort for the specific parts of some products and the effort for specific single products in the product line to be included inside the unique cost ($C_{unique}$).

The following InCoMe cost functions are used for product line effort estimation in the Cost Factor Layer:

1. **Organizational Cost** includes all the effort put on the organization for introducing the product line.
2. **Core Asset Base Cost** implies the effort of developing common artifacts that will be included in the main core asset with the intention to be reused later.
3. **Unique Cost** is about the effort of developing unique and specific parts of certain products in the product line.
4. **Reuse Cost** includes the effort put on adapting and integrating each reused artifact in a new context in the product line.
5. **Out-of-context Development Cost** implies the cost of developing a single product outside the boundaries of the product line approach.

6. **Product Evolution Cost** is about the effort put on modifying and integrating a single product as it evolves towards a new version.

7. **Asset Evolution Cost** is the effort spent for adapting and integrating the core asset base with the common artifacts while the product line evolves from an old generation to a new one.

The Viewpoint Layer (figure 17) utilizes the estimated cost values in the Cost Factors Layer and evaluates different reuse scenarios (similar to SIMPLE scenarios) by producing cost functions for each scenario and estimating the benefits and drawbacks in each case. However, InCoMe considers fewer scenarios than SIMPLE model does. InCoMe focuses more on reuse-based scenarios e.g., comparing the situation when a company has to develop single products with the one when it develops them as product line members.

Different viewpoints are defined for:

1. **Domain Engineering.** In this scenario, the effort for developing the platform or the core asset of the product line is estimated.

2. **Product Engineering.** In product engineering scenarios, the effort for developing different product line members i.e., different applications from the core asset is compared to the effort for developing them as single products.

3. **Corporate engineering.** In the corporate viewpoint, the effort put from the corporate perspective for developing the product line compared to the effort of developing same products as independent ones is estimated.

At the end, the Investment Analysis Layer takes the output from each viewpoint and calculates the cost for each of them, in order to check if it is worthy to make a certain investment. Three economic functions are involved: NPV (Net Present Value), ROI (Return on Investment) and PB (Payback Value) [44].

In order to test the level of accuracy in practice, InCoMe [45] relies on a parameter called Deviation of Accuracy for defining the accuracy level of the model. The value of this parameter increases when there is more information extracted from accurate sources e.g., history data (P_a) and decreases when there is more information from sources that are not accurate (P_n). If the total amount of parameters (sources of information) is N, the Deviation of Accuracy is calculated in the following way [45]:

$$d(A) = \frac{\sum P_a - \sum P_n}{N}$$

(29)

However, the accuracy level of the inputs (sources of information) depends on the extracted data from the domain. If one of the inputs is estimated with low accuracy, then it will affect the overall accuracy level. For example, if the effort estimation for the core asset base will be not accurate, then the total effort estimation accuracy is going to be affected.
The InCoMe model has been applied in an industrial study [44] where nine products are developed for managing a passport system (a system for handling passport data from a big database). The system is developed as a Java framework and it contains the reusable assets (including common source code and so on) for the nine developed products. The InCoMe has been used for estimating the effort of developing the nine products in two different reuse scenarios: first developed as single products and then, as a product line. In order to make the calculations, historical data from the company is used as inputs. In this case, InCoMe resulted to provide relatively high accurate results since the provided inputs were accurate. The conclusion was that the nine products were more suitable to be developed separately (i.e., not as a product line) in order to obtain higher cost savings.

As it was the case in SIMPLE model, InCoMe gives the possibility to decompose the total product line effort into several cost areas. The fact that the model considers different scenarios and viewpoints makes it suitable for being adapted in an industrial case. However, more guidelines are needed regarding the estimation of cost inputs in real situations e.g., how to estimate the organizational effort when a company evolves their product line(s).

4.1.11 Discussion

After reviewing each of the ten existing cost models, some of their features and attributes that generally characterize a software product line cost model have been summarized in table 6.

Table 6: Evaluation of software product line cost models

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>COCOMO II</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>COPLIMO</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>qCOPLIMO</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Poulin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SoCoEMo-PLE</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Withey</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Schmid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Boeckle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>SIMPLE</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>InCoMe</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Formula-based Cost Models vs. Analytical Cost Models

Most of the cost models use cost functions and formulas for performing calculations of effort in product lines. The only exceptions from the cost models we consider are Withey’s model.
and Schmid's model that rely on investment analysis and decision trees for estimating the benefits and drawbacks of an investment. Except for Withey’s and Schmid’s model, InCoMe is another cost model that includes an approach for investment analysis, as well.

**Scenario-based Cost Models**

Half of the models (Withey's model, Schmid's model, Boeckle's model, SIMPLE and InCoMe) are using different scenarios for evaluating different situations with product lines in industry. The highest diversity of scenarios can be found in SIMPLE model while the other four consider more general scenarios e.g., reuse scenarios or single development vs. product line scenarios.

**Viewpoints**

Different viewpoints are taken into consideration by the two COCOMO II successors (COPLIMO and qCOPLIMO), SoCoEMo-PLE, Schmid's model, SIMPLE and InCoMe. The InCoMe model provides a better structure compared to the other four models for evaluating different viewpoints. This model considers evaluating the effort in domain engineering, product engineering and corporate engineering.

**ROI Estimation vs. NVP Estimation**

COPLIMO, qCOPLIMO and Poulin’s model provide ways for estimating ROI (Return on Investment) while Withey’s and Schmid's models rely on NPV (Net Present Value). Furthermore, SoCoEMo-PLE, SIMPLE and InCoMe use both of them.

**Market Study and Risk Assessment**

Three cost models (Withey’s, Schmid’s and SIMPLE models) include a preliminary market analysis in their approaches. In Withey’s and Schmid’s case, this analysis is covered by the decision trees and the investment analysis, which also can predict if performing an investment may be associated by good market conditions. Good market conditions imply that the there are higher chances that the investment will pay off in a short time. SIMPLE provides a formula for calculating the return on investment when the product line is prepared for a specific market i.e., it estimates the cost advantages obtained from the product line when entering that market.

Risk assessment is considered in three models. qCOPLIMO focuses on software quality by applying a defect-detecting mechanism. In this context, there is risk assessment considered by this cost model since it searches for possible defects that appear as threats for the system. Schmid’s and Withey's models consider performing a risk assessment and a follow-up risk adjustment process in order to evaluate possible risks related to an investment and the possibility to make the most optimal decision to avoid or mitigate these risks. A “risk assessment” in this context means to analyze if a potential risk associated to a future investment is either cost advantageous or disadvantageous. Apart from qCOPLIMO, which is a quality-based extension version of COPLIMO, software quality is also considered by Schmid’s model.
Industrial Applicability and Functional Safety Perspective

There are cost models that have been applied in several industrial studies. However, some of them (e.g., COCOMO II, COPLIMO, Poulin’s model and so on) are more suitable for estimating the effort put on software reuse by taking into account the amount of code that has been changed or adapted. In the functional safety perspective, this does not fit very well since functional safety effort requires the analysis of many more artifacts and mechanisms rather than lines of code.

The cost models that would have higher potential in our context (safety effort estimation in product lines) are: SIMPLE, InCoMe and the models proposed by Withey, Schmid and Boeckle. The investment analysis approaches that are present in Withey’s model, Schmid’s model and InCoMe, represent a great contribution for evaluating different investment decisions for product lines.

Moreover, three models (Boeckle’s model, SIMPLE and InCoMe) provide ways how to decompose the overall product line effort into several effort areas or cost functions. Out of these three models, SIMPLE covers more effort areas by including and estimating the effort for maintaining a product line, as well. Finally, SIMPLE addresses the problem of estimating the input values for the cost functions by providing guidelines on how to estimate them. In this context, relying only on cost functions and parametric models is not considered sufficient. Instead, it is necessary to talk to the right industrial experts for trying to get the value for every input (the input for organizational effort, core asset base effort and so on). This method can be considered more suitable for estimating functional safety effort, as well since it is not possible to investigate safety effort in industrial product lines by relying only on existing cost models.
4.2 Expert Estimation Methods for Product Lines

Several studies have been performed in order to investigate issues regarding software development effort estimation in practice [46-53].

Apart from the formal cost models discussed in subsection 4.1, there are alternative methods for estimating the development effort in product lines. The most notable ones include expert-based estimation methods. In order to provide estimations for the development effort, such methods rely on the industrial expertise of practitioners and empirical studies [46].

Expert-based estimation provides many advantages compared to formal established economic models since it takes into account several problems, characteristics and situations related to the industrial environment that are not considered and included in most of the proposed economic models. Moreover, it is much easier to apply and adapt expert-based methods in an industrial context rather than formal models. The main reason for that is the fact that relying on expert-based methods implies interacting and talking to experts who are directly involved in the industrial development processes [46]. However, the results from expert-based estimation need also to go through a validation process. One weak point of expert-based effort estimation methods is that they also do not produce 100% accurate results. There is always some uncertainty that should be considered and there are always deviations. Of course, there have been attempts to estimate the deviations as well or in other words, to evaluate how accurate is an approach that relies on expert-based software effort estimation.

4.2.1 Methods for Expert-Based Software Effort Estimation

Possible methods for expert-based software effort estimation have been studied and evaluated by Jorgensen et. al [46-54]. Jorgensen performs a review study of research work related to expert-based software development effort estimation in [47]. This review study shows that most of industrial domains prefer to rely on expert-based estimation rather than on other estimation approaches such as formal cost models. As an example, the effort in ten projects is evaluated in one of the studies reviewed in [47] by first relying on the COCOMO model and afterwards, by relying on the estimation provided by five different software experts. The average estimation performed by the industrial experts resulted to be more accurate than the one obtained by using COCOMO. One of the reasons for such result was that COCOMO was not adapted in the context of the domain where the ten industrial projects were developed.

A similar conclusion is derived by Molokken et al. who perform a review study of surveys related to software development effort in [48]. The review of surveys shows that expert-based methods are still the most preferred and used method for estimating the development effort in the investigated industrial projects. Moreover, no evidence could be found from the review study [48] which would bring to the conclusion that expert-based estimations have lower accuracy level than other methods e.g., formal methods. Nevertheless, another crucial results derived by reviewing the surveys is that there are issues with the estimation accuracy in general when applying expert-based methods. One reason for that is when same activities
with the same cost impact on the development effort are reported in different ways and thus, same cost is calculated more than once.

A systematic review on studies on software development estimation effort [49] evaluates that there is significantly more research work performed on investigating and proposing formal methods. After reviewing systematically no less than 304 research papers and articles related to software development effort estimation, Jorgensen et al. observed that there is less focus on investigating expert-based methods in existing literature [49]. Regardless, it was still pointed out that industrial domains prefer expert-based estimation methods over formal methods or alternative solutions. The systematic review did not provide any conclusion related to the estimation accuracy of expert-based methods. The next subsections provide a more detailed overview of the advantages of expert-based methods compared to non expert-based ones as well as their estimation accuracy.

Expert-based estimation methods can be classified into 2 main categories: methods that rely on non-official analogy or those who rely on official analogy. Non-official analogy means that the estimation and evaluation is based on the intuition and the professional experience of industrial experts while official analogy comprises an estimation that uses more formal sources such as written documentation.

After different studies were reviewed in [47], it resulted that there are two different ways of performing an expert-based estimation i.e., the top-down and the bottom-up estimation procedures.

The top-down estimation procedure aims to estimate the effort for developing a project (e.g., a project that includes adapting a product line approach) by viewing the project as a whole one. This method is widely used in cases when there is a previous knowledge on estimating some parts of the project. For example, the project that needs to be estimated is just an extension of a previous project and the effort for the previous project has been already investigated in the past. Hence, the effort for the specific parts that have been added, removed or modified in the new project needs to be calculated and added (or subtracted) to the known effort of the previous project. A typical industrial example where using the top-down estimation is more appropriate would be the case when a unique product (e.g., a special type of car) has been added to the product line (e.g., a car product line).

On the positive side, top-down provides some historical data but in the same time, there is strong dependency from previous projects. In this perspective, the probability to achieve a very accurate estimation is low if there has been no estimation of previous projects that have similar basic features with the project that is being estimated. The bottom-up estimation approach is more appropriate for those cases when estimating a project as a whole is not so easy and hence, it is better to split the project into different parts (i.e., make a decomposition of the project in different layers or components) and estimate the effort separately for each decomposed part (layer or component). This procedure is more appropriate to use in cases when the project is quite new and the level of expert knowledge about it is low. Hence, there is no sufficient historical data related to the development effort.
approach decomposes the project in smaller parts and estimates each part separately. This approach provides a better understanding of the project and how to develop it. However, there is no possibility to evaluate historical data and improve past mistakes or limitations. Regarding the estimation accuracy in bottom-up, it depends on the abilities and experience of engineers and developers that are decomposing the project into smaller units. This represents a big difference with the estimation accuracy in top-down which is mostly affected by historical data.

Based on the investigation [47] performed in several domains that use expert-based effort estimation, it was proposed to use an estimation checklist for tracking estimated data. The use of an estimation checklist can increase the estimation accuracy since the chances to use the same input more than once in the effort estimation are much lower because of tracking data that has been already estimated.

4.2.2 Comparison of Expert-Based Estimation with Formal Methods

The studies performed in [47] [48] [49] concluded that all the organizations that were being investigated are relying mostly on expert-based software effort estimation. In fact, Jorgensen did not manage to find any industrial subject that is highly considering any formal established economic model or choosing it over expert-based estimation [47].

Formal methods are considered to be more complex than expert-based estimation methods when it comes to apply them in industry. Furthermore, they also come with more limitations and as a consequence, they are less flexible than expert-based methods when being adapted in an industrial project or domain. In addition, practitioners do not always have full understanding of formal models and hence, they consider the application of such models in their own industrial context to be more challenging [46].

Another motivation for choosing expert-estimation methods against formal methods regards the uncertainty level and the estimation accuracy. As the studies in [47] [48] [49] suggest, it has not been proven that formal cost models can bring to more accurate estimations compared to expert-based estimating approaches. Even in the hypothetical case when it would be proven that formal cost models bring to more accurate results, practitioners would still hesitate to embrace formal approaches instead of continuing to rely on practical experience and intuition [49]. This would happen because the practitioners would consider that there is high effort into embracing a formal model, making it enough understandable for the staff and adapting it to the main industrial context. Therefore, their hesitation comes because they do not prefer to go through all this new process into adapting a new estimating approach and they are more comfortable and secure with their conventional estimation methods that are based on expert judgement.

4.2.3 Comparison of Expert-Based Estimation with Code-Based Methods

Besides expert-based and formal methods, there are also other alternatives for effort estimation. One alternative is also the development of different tools for performing the measurement of cost and effort in several activities. This method relies on programming. This happens especially when there is interest to measure the effort spent on different software
development projects and activities [50]. In this case, an application has been developed in order to analyze the effort in different projects that have been completed by a team.

However, code-based estimation methods cannot be considered as more suitable than expert-based estimation methods in the product line perspective. Analyzing effort related to developing, evolving and maintaining product lines requires the evaluation of more complex areas e.g., development of product line members, mechanisms, effort by organization on developing the common artifacts of the product line and so on. Therefore, it would be neither relevant nor feasible to incorporate all these areas related to product line effort in the lines of code of a developed application. As a conclusion, expert-based methods remain the most relevant and safest choice when it comes to effort estimation in industrial product lines.

4.2.4 Expert-Based Estimation Accuracy and Deviations

The study review in [48] revealed that estimation accuracy represents probably the biggest concern for the practitioners.

Estimating the effort required for projects related to software product lines is usually not characterized by full precision. Several studies have addressed the problem of how to assess and evaluate the uncertainty when evaluating the effort for software development [51]. In the conventional way of assessing uncertainty, the practitioners are usually asked to estimate both minimal and maximal effort that is required for a certain task. The study shows that defining these two boundaries also presents some difficulties and practitioners cannot answer with precision. The evaluation of the uncertainty is also highly affected by some non-functional properties. The most notable ones:

1. The professional experience and ability of the practitioner who is dealing with the software estimation task.
2. The amount of data related to previous software projects that are related to the one that is going to be estimated.
3. The amount of data related to the project itself.

For this purpose, Jorgensen proposes a non-conventional way of evaluating uncertainty. According to him, asking for minimal and maximal effort is not very productive. On the other hand, it would be easier for practitioners if they are asked for example, to estimate the probability that the effort required for an upcoming project would be two or three times higher than the predicted one.

Furthermore, Jorgensen et al. discuss in [52] possible reasons that trigger errors and deviations in software effort estimation. In their study, they identified some reasons for causing errors in software effort estimation. Some of them are:

1. Unexpected events and overlooked tasks
2. Changing requirements because of new customer requests
3. The requirements have not been well defined in the beginning.
4. The task results to be simpler than predicted and the developer seems to be more capable and faster with his task.
5. There are problems of allocating the resources.
6. Several artifacts are being reused from previous projects and platforms at a higher extent than it was predicted.
7. Not much effort is put on estimating the effort for the project.
8. The whole is put on assuring quality and not on providing an accurate estimation of the effort related to the project.

They consider that these reasons are usually affected by three major factors:

1. The professional profile of the practitioner who is being asked.
2. The approach used for collecting necessary information for the estimation.
3. The method used for analyzing the information related to the project.

The first factor is very important. If a software developer is being asked, then it should be considered that the information that he provides is accurate only for his field of expertise i.e., the effort dedication to implementation activities. On the other hand, a project manager would generally be able to provide a full overview and summary of the activities that would contribute in the total effort.

The phase of collecting the necessary data for estimation is of high importance. In order to extract information, interviews as well as project reports and documentation can be utilized. The study in [52] concluded that it is much easier and productive to identify possible reasons for software estimation errors through conducting interviews with specialists (practitioners) rather than relying on written documentation since the interviewees seemed to provide some additional useful information related to problems faced in the projects while this was missing in the documentation.

It matters also how the reports and documentation are analyzed. The alternatives include qualitative and quantitative analysis of the project reports. A qualitative analysis is focused more on identifying the activities and processes that contribute on the overall cost. Meanwhile, a quantitative analysis implies a statistical analysis and it results that it is more efficient to use this method in order to identify reasons for software estimation errors.

4.2.5 Validation Methods

There is a need to validate formal economic models before they are accepted and adapted in an industrial context. Nguyen-Cong et al. [53] have investigated several cases for validating different formal economic models. They concluded that validation by conducting industrial studies are common. Studies have been mostly conducted in industrial projects, semi-industrial projects and student projects as well.

Other ways for validating formal economic models involve surveys. Several surveys are also reviewed by the authors in [48]. These surveys are performed in order to provide answers for research questions that aim to investigate the most frequent ways of estimating software effort in industry and also the deviation of the actual effort from the predicted one. The second aim is valid for cases when there is a predicted (pre-estimated) effort that a software project may require.
Regarding the validation of results obtained by expert-based methods, the most suitable ways to validate such results would be to hold presentations and workshops with the participation of different industrial experts involved in the projects that are estimated. In addition, peer reviews of the reported results are very beneficial for validation.

4.2.6 General Discussion

In our literature study, we summarized and analyzed existing product line cost models (subsection 4.1) as well as expert-based estimation methods (subsection 4.2). After evaluating the proposed ten product line cost models from the literature study, we foresee big challenges on making such models applicable for safety effort estimation in product lines. The main reason regards the limitations pointed out in the ten proposed cost models. Safety effort estimation requires methods that are more flexible in order to capture all the effort components related to functional safety in product lines.

In addition, we perform an empirical study that is explained in the next sections of this report. As we point out, there are still big challenges on extracting product line safety effort from the expert-based estimations as well. It is not possible to ask the practitioners directly for the effort related to functional because such effort is mixed with other efforts related to product line development and it is very challenging to define it.
5. Conducted Study 1: Interview Study

5.1 Introduction

We investigate how cost and efforts are predicted for the development of safety critical products in the construction equipment industry using the example of Volvo Construction Equipment. Therefore, expert judgment is very important and helpful in our work and we perform an interview study in order to obtain results from an industrial point of view. Furthermore, we relate existing literature on established product line cost models to the study. We conducted semi-structured interviews at Volvo CE to investigate different cost aspects in real industrial cases (Appendix A).

Before performing the interview study, the following problem areas are pointed out based on the literature study and some brainstorming performed before the interviews at Volvo CE.

5.1.1 Problem Area 1: Managing safety in product lines in industry

What are the general challenges and problems that are faced when developing product lines in an industrial domain where safety aspects are considered?

Functional safety represents a whole new concept and approach that is applied in industry (Volvo CE in our case). Different challenges and issues come up and the way how practitioners deal with them have an impact on the overall cost, as well. Interviewing practitioners represent a good method for investigating how industry is dealing with functional safety, what issues and challenges they are facing and what cost impact they have. If we can extract information regarding challenges that industry face when applying functional safety, it is possible to have an overview of possible solutions for overcoming these challenges and an evaluation if these solutions are either cost efficient or not.

5.1.2 Problem Area 2: Efforts related to functional safety in industry

Often the efforts for achieving functional safety are not clearly distinguishable in industrial projects. Project planning and effort prediction is challenging and is often depending on experiences. There is a high risk of inaccurate appraisal, which in turn may lead to project delays and later time to market.

5.1.3 Problem Area 3: Identification of activities and approaches that can affect the cost related specifically to safety aspects

Functional safety standards require that activities are recorded and necessary safety arguments are provided. Developing single products according to specific functional safety standards is straightforward and requirements can directly be applied. For product line engineering, things become more complicated and the requirements stated in the functional safety standard need to be adopted accordingly. The product line engineering approach applied in industry, as far as we could see, is based on an engineer's mind-set. Analyzing the efforts for single activities requires talking to practitioners to capture the activities and according efforts. For this purpose, this approach i.e., interviewing industrial experts is the best option comparing to other alternatives e.g., applying formal cost models (this would be
inefficient and not practical since no existing cost model has been actually designed for functional safety).

### 5.2 Cost Analysis in Product Development

Before performing the interview study, we associate different cost components identified in existing cost models (Boeckle [40], SIMPLE [42] and InCoMe [44]) to each phase in the Software Product Line Engineering diagram [1], which is presented in figure 1 in the first section of this report. Figure 18 shows the association of different cost components to each SPLE phase. Such relation was proposed before the semi-structured interviews were performed at Volvo CE.

However, several preliminary informal interviews with practitioners at Volvo CE took place before proceeding formally with the semi-structured interviews. The purpose of having the informal interviews was to receive expert-based feedback in order to refine further the interview questionnaire. The final version of the questionnaire is presented in appendix A.

![Figure 18: Relation between cost and product development](image)
In the domain phase, the platform of the product line is designed and built. Therefore, the common artifacts (such as requirements, architecture, components, tests) are already designed and developed in this phase. Specific parts are also identified in the domain phase so they can be applied later, in the application phase [1].

A commonality-variability analysis is performed before the artifacts are developed in the domain phase. For each phase, we identify and define different cost parts related to it that can contribute in the overall cost for developing the products within that phase.

We identify the following cost parts in the domain phase:

- The organizational cost ($C_{org}$) – The effort put from the organizational side for preparing the platform (core asset) of the product line e.g., creating expert groups, holding training activities and so on.
- The core asset base cost ($C_{cab}$) – The effort put for developing the common artifacts and performing the commonality-variability analysis.
- The reuse cost ($C_{reuse}$) – The effort put on reusing and integrating artifacts from previous projects or generations in the new core asset of the product line.
- The unique cost ($C_{unique}$) – The effort put on specifying the variable or specific parts (or unique products) in the product line.

In the application phase, products and applications are developed. The following efforts and costs are relevant in the application phase:

- The organizational cost ($C_{org}$) – The effort put from the organization on applying the results from the commonality-variability analysis in the domain phase, in order to develop several products and applications.
- The reuse cost ($C_{reuse}$) – The effort put on reusing and integrating parts from the common artifacts that were developed in the domain phase.
- The unique cost ($C_{unique}$) – The effort put on applying variability i.e., applying specific parts (or unique products) in the product line.

In case when the product line is evolving to a new generation, the following cost is considered for this evolutinal process:

- The evolitional cost ($C_{evo}$) – The effort put on evolving the core with the common artifacts for the new generation and adding new products to the product line.
- The organizational cost ($C_{org}$) – The effort put from the organization in order to adapt to the new generation.
- The reuse cost ($C_{reuse}$) – The effort put on reusing and integrating artifacts from the previous product line generation.
- The unique cost ($C_{unique}$) – The effort put on developing and applying new parts (specific parts) in the new generation.

After it has been developed, maintenance activities are necessary for the product line. During maintenance, the following cost is considered:
The maintenance cost ($C_{\text{maintenance}}$) – The effort put on maintaining the product line in order to make sure that everything is going as planned and developed in the domain and application phases and continuously check the functionality of the products.

The reuse cost ($C_{\text{reuse}}$) – The effort put on reusing several artifacts when maintaining the product line.

The unique cost ($C_{\text{unique}}$) – The effort put on extra maintenance for specific parts and products.

All cost parts we identify and define in each phase are important in a safety context e.g., the reuse cost is dedicated to the effort put on reusing safety artifacts, which the unique cost to the effort on developing specific safety artifacts.

In figure 18, examples of safety artifacts (shown in yellow rectangles) are listed and related to each phase and sub-phase. For instance, the domain phase includes safety requirements, safety architecture, safety components, safety testing and the commonality-variability analysis. For each safety critical product derived from the product line, a specific safety case must be created [10]. All the common artifacts (e.g., common parts of PHAs or other risk assessment techniques) are identified in the analysis that takes place in the domain phase. That is the reason why we associate the core asset base cost ($C_{\text{cab}}$) to this phase. A part of these common artifacts might be newly developed while others might be reused or inherited from previous generations e.g., some safety plans may be provided by previous generations and then, included in the core asset base of the new generations. Hence, we add the reuse cost ($C_{\text{reuse}}$) and the unique cost ($C_{\text{uni}}$) to the development effort in the domain phase. Of course, effort is needed from the organizational side ($C_{\text{org}}$) in order to develop the new core with common artifacts.

On the other hand, there is no need to have an effort dedicated to the core asset base ($C_{\text{cab}}$) in the application phase since developing the core asset takes place only in the domain phase. However, it is reasonable to consider organizational effort ($C_{\text{org}}$) for developing different applications and products. When developing several applications and specific products in the application phase, some parts are reused from the common artifacts developed in the domain phase ($C_{\text{reuse}}$) while others are developed separately ($C_{\text{uni}}$).

It should also be considered that safety artifacts such as safety plans, requirements, architecture, risk assessment techniques or even safety standards should be updated when the product line evolves to a new generation ($C_{\text{evo}}$). During maintenance ($C_{\text{maintenance}}$), practitioners should make sure that safety artifacts are functional e.g., they must assure that safety plans are consistent, run more safety tests to support better safety components or check that safety standards are being followed properly. During both product line evolution and maintenance, it can be necessary to reuse safety artifacts ($C_{\text{reuse}}$) as well as to develop new ones ($C_{\text{uni}}$).

5.3 Interview Study - Results

The following subsections are organized according to the results obtained and extracted by the respective sections of the interview questionnaire (Appendix A). The questionnaire is
structured as we explained in chapter 3. In the first part of the interview, we ask about
general information such as professional profile of the interviewees, the working experience
and working tasks. In the second one, we ask about different scenarios by relying on the
practical experience and context of each interviewee (e.g., we ask about the changes that they
have gone through while passing from an old product line generation to a new one). The rest
of the successive subsections are structured based on the cost parts we identified in the
literature study (organizational, core asset base, unique, reuse, evolitional and maintenance
effort).

5.3.1 General Background
Eight semi-conducted interviews were performed at Volvo CE. The shortest interview lasted
90 minutes while the longest one was conducted for about 150 minutes. The interviewees
have different working backgrounds. However, all of them have some experience on
functional safety and some of them are part of the ISO group. General information (questions
1-4 in appendix A) about the seven interviewees is presented in table 7.

Table 7: General overview of the interviewees

<table>
<thead>
<tr>
<th>Interviewee ID (Nr. of interviews performed)</th>
<th>Years of working in industry (and with Functional Safety)</th>
<th>Role at the company</th>
<th>Main Work Tasks</th>
</tr>
</thead>
</table>
| I1 (1)                                    | 15 (10)                                                  | Senior Safety Engineer | ➢ Project Assessment  
|                                           |                                                          |                      | ➢ Safety Support |
| I2 (2)                                    | 3 (3)                                                    | Functional Safety Manager | ➢ Responsible for Safety Requirements, Safety Architecture and Documentation |
| I3 (1)                                    | 15 (5)                                                   | Technical Project Manager | ➢ Project Manager for the platform project |
| I4 (1)                                    | 29 (3)                                                   | Chief System Architect | ➢ Responsible for system architecture for engines |
| I5 (1)                                    | 16 (6)                                                   | System Architect and Safety Engineer | ➢ Providing technical solutions for safety, product usability and other general issues within the product lifecycle. |
| I6 (1)                                    | 10 (4)                                                   | Project Manager software verification and validation | ➢ Planning and managing testing activities in different projects. |
| I7 (1)                                    | 27 (2)                                                   | Project Manager for research project with functional safety focus | ➢ Deriving safety requirements  
|                                           |                                                          |                      | ➢ Investigating new processes and methods for functional safety work |
Interviewing people of different professional backgrounds covers several areas of expertise. The results and feedback provided by the interviewees involve software development phases such as planning, architecture, testing and so on. Furthermore, the interviewees are often involved in additional functional safety activities beside the ones at Volvo CE. For example, I1 is member of the ISO 26262 group, which consists of international experts that deal with issues of applying this standard [10]. I7 is also involved in the SafeCer project [54], which is a European research project that involves several domains in different countries. The main goal of the project is to establish methods for reusing safety-critical components in industrial domains. It also aims to establish a common platform for safety system certification.

The interviewees are involved in several projects at the company. These projects comprise:

- The platform project, which aims to develop a platform and common architectural structure to be integrated in different Volvo CE machines.
- Machine project 1 includes one specific product line and the goal is to apply functional safety for the product line members while integrating the new generation of the common platform.
- Machine project 2 includes another product line. This project reuses the platform of the previous generation and it utilizes a gateway to support the functionality provided by the new platform.

5.3.2 Key Findings

The interviewees were asked to describe scenarios related to product line development processes where they are involved (questions 5-6 in appendix A). By analyzing the answers provided by practitioners in this perspective, we are able to capture hints to hidden efforts. In the following subsections, we describe the different analyzed situations and provide evidence from the conducted interviews.

5.3.2.1 Area 1: Changes from previous generations

Focusing on typical changes from previous generations is important to understand the character of product lines on the one hand and relate the answers to concrete examples.

Table 8 summarizes the most significant challenges described when a new product line generation or project was introduced.

<table>
<thead>
<tr>
<th>Challenges and scenarios of changes from previous generation(s)</th>
<th>I1</th>
<th>I2</th>
<th>I3</th>
<th>I4</th>
<th>I5</th>
<th>I6</th>
<th>I7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Different strategies for Product Lines</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Identification of commonalities and variability between product lines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>
Integrating the platform in different product lines presents a big challenge because of the differences that exist between Volvo CE product lines. The following scenarios (related to issue 1) present the case of two Volvo CE product lines, which rely on different development strategies and mechanisms. In other ways, they use different approaches for developing safety artifacts and reusing them in their respective applications.

**Scenario 1.1: Different decisions of utilizing the platform in different product lines**

There are different decisions for different product lines and these differences bring to extra functional safety effort for each of them. One product line (machine project 1) utilizes the platform while the other one (machine project 2) is reusing the previous platform and a gateway. Significant effort has been put by the organization side on adapting the platform for the product line in the first project. Safety artifacts (safety requirements, safety plans and so on) are developed for the platform project and then, they are tailored for each product. On the other hand, the machine project 2 relies on the gateway and artifacts are being reused from the previous generation. Hence, there is currently reuse of safety mechanisms and artifacts within each product line but not between them. Each product line applies its own solution, which brings to specific effort on functional safety for both of them.

**Sub-scenario 1.1.1: Focus on preserving Machine 1 functionality while integrating a new platform**

The application functionality should be preserved and the main focus is on integrating the new platform which had an in turn impact on the application. New safety mechanisms are needed to be developed for the platform to support the safety requirements of the applications. The impact of the new platform was that the complete safety case for the machine project needed to be reviewed and improved.

**Sub-scenario 1.1.2: Focus on preserving Machine 2 architecture and functionality to comply with new technical requirements**

In machine project 2, it is a must also to preserve the machine 2 architecture as much as possible. In this case, the challenge is about finding a balance between the need to adapt the machine 2 architecture according to the gateway and the must to preserve the architecture of the product line in machine project 2.

**Scenario 1.2: Safe states in different product lines**

In the machine perspective, I4 states that different hazards are identified for different machines. The identification of different hazards for different machines brings to different safe states for the machine type and it also complicates reuse between product lines. These different hazards and safe states increase the effort needed for functional safety since different mechanisms need to be found.

**Issue 2: Identification of commonalities and variability between product lines**

The differences discussed in issue 1 contribute into making the commonality-variability analysis very challenging.
As we explained in the Cost-Product Development relation in subsection 5.2, the commonality-variability analysis has a very crucial role within the domain engineering phase because of exploiting all the common parts and the specific ones of the product line before the development starts. By performing well the commonality-variability analysis, several costs can be highly reduced. This analysis gives a better overview of the common artifacts (such as safety architecture, safety components, safety plans, risk assessment techniques and so on) and specific parts of the product line and thus, it provides the basis and guidelines for building a good core asset ($C_{cab}$) which brings eventually to the reuse ($C_{reuse}$) and unique cost ($C_{uni}$).

**Scenario 2.1: Identifying commonalities and variability in safety mechanisms and other safety artifacts**

Having different management decisions in each product line represents an obstacle for identifying all commonalities between product lines in general and especially in the safety perspective. The impact is that there are different technical solutions on similar safety-related problems in different product lines. This causes extra effort on functional safety.

A typical example for that is the specific effort put on each product line for different redundancy mechanisms and CAN buses for sending safety-critical messages.

**Scenario 2.2: Identifying commonalities and variability in test specifications**

It is challenging to identify commonalities and variability in test specifications. Right now, there are common tests within one product line (machine project 1) while there are no common tests between the two product lines in the machine projects.

**Impact on Cost**

We present the impact of each scenario on the cost components in table 9. Regarding cost components, we refer to the definitions we provided for them in subsection 5.2. We present our own view on the cost impact of each scenario identified in the interview study.

As we previously stated, there is organizational cost for the domain engineering and organizational cost for the application engineering, as well. Same situation is with reuse cost and unique cost, as well. For this purpose, we include both domain engineering (D) and application engineering cost (A) under $C_{org}$, $C_{reuse}$ and $C_{unique}$, as shown in table 9. While evaluating the cost for each scenario, we use three values: high (H), medium (M) and low (L).
### Table 9: Cost impact of issues and scenarios of changes from previous generations

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios of changes from previous generation(s)</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$C_{org}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>1</td>
<td><strong>Different strategies for product lines</strong></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Different decisions of utilizing the platform in different product lines</td>
<td>High</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Focus on preserving Machine 1 functionality while integrating the platform</td>
<td>High</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Focus on preserving Machine 2 architecture and functionality to comply with new technical requirements</td>
<td>High</td>
</tr>
<tr>
<td>1.2</td>
<td>Safe states in different product lines</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td><strong>Identification of commonalities and variability between product lines</strong></td>
<td>High</td>
</tr>
<tr>
<td>2.1</td>
<td>Identification of commonalities and variability in safety mechanisms and artifacts</td>
<td>High</td>
</tr>
<tr>
<td>2.2</td>
<td>Identification of commonalities and variability in test specifications</td>
<td>High</td>
</tr>
</tbody>
</table>

**Cost Impact in Scenario 1.1**

In scenario 1.1, there are different decisions for different product lines, which means that in domain engineering, the organization spends extra effort for developing and integrating safety mechanisms and artifacts in each product line. Hence, $C_{org}$ for domain engineering is high. As for the application engineering, the organization effort is still considered to be high. If we evaluate the effort put on each project, the effort put on machine project 2 is quite high since that is a very specific solution. The core asset base effort ($C_{cab}$) is not considered high if we consider the perspective of a common core asset between the product lines i.e., platform integration for both of them which is currently not happening. There is no reuse between product lines which means that the reuse cost in domain engineering is low. Nevertheless,
there is effort on reusing artifacts internally in each project. Hence, reuse cost ($C_{\text{reuse}}$) in application engineering is considered as medium. We do not consider it high since it is not the case when high integration efforts are needed for reusing artifacts in machine project 1 or in machine project 2. As for the unique cost ($C_{\text{unique}}$), we already admitted that overall, there is extra specific safety effort because of not reusing more between product lines. This implies that the unique cost in domain engineering is high. Meanwhile, the unique cost in application engineering (effort for specific wheel loaders, articulated haulers and other specific parts in each product line) can be considered medium in comparison with the unique cost in domain engineering which is high. The evolutional cost ($C_{\text{evo}}$) can be also considered high since it requires more effort to evolve two different product lines that do not reuse much from each other. For the same reason, maintenance ($C_{\text{maintenance}}$) requires more effort. However, it should be pointed out that maintenance for the platform project is still initiating.

Cost Impact in Sub-scenarios 1.1.1 and 1.1.2

In sub-scenario 1.1.1, the organization aims to preserve the functionality in machine project 1 while integrating the platform. Meanwhile, focus and effort is put on preserving Machine 2 architecture where gateway is used as well as artifacts from the previous platform generation.

In our view on cost analysis, this causes high effort from the organizational perspective in the domain engineering phase ($C_{\text{org}}$ (D)). Regarding $C_{\text{org}}$ (A), it can be considered medium in sub-scenario 1.1.1 since the platform has facilitated the reuse of artifacts and mechanisms within the machine project. Instead, $C_{\text{org}}$ for application engineering in sub-scenario 1.1.2 is considered high since there are more efforts put on reuse and development because the platform has not been applied on the machine project 2. The core asset base in both scenarios (represented by the effort on integrating the platform and adapting Machine 2 architecture to the gateway) has required high effort. In both projects, there is reuse from the previous generation. Hence, there are also considerable integration efforts at first for adapting artifacts from the previous generation in the new solutions i.e., platform and gateway. For this reason, we consider that $C_{\text{reuse}}$ for domain engineering is high in both scenarios. On the other hand, $C_{\text{reuse}}$ for application engineering is low in the Machine project 1 since the platform has facilitated and decreased reuse efforts in the machine 1. As for reuse within the product line in machine project 2, it cannot be considered high so we evaluate it as medium effort (especially in comparison to sub-scenario 1.1.1 where we evaluated it as low). The unique effort for domain engineering is represented by the effort put on developing new common artifacts. Besides reusing from the previous generation, there is development of completely new solutions in both cases. Hence, $C_{\text{unique}}$ for domain engineering is high in both cases. $C_{\text{unique}}$ for application engineering is represented by the effort put on unique products or specific parts within each product line. Such products and parts are existing in both cases which means that $C_{\text{unique}}$ for application engineering is high in both cases. Applying the platform (sub-scenario 1.1.1) facilitates reuse for future generations, as well while in the machine project 2, this requires more effort. Hence, $C_{\text{evo}}$ can be considered low for the machine project 1 and medium for the machine project 2.
Cost Impact in Scenario 1.2

Scenario 1.2 is about the different safe states between machines. The impact on the cost components is basically very similar to the one in scenario 1.1 since the essential is about the differences between product lines. In our view on cost analysis, we consider that $C_{\text{org}}$ (D) is high since it is hard to perform a commonality-variability analysis because of the different states. $C_{\text{org}}$ (A) is also high since extra effort has been put on developing safety mechanisms and artifacts in the machine project 1 which adapts the platform and other safety mechanisms and artifacts in the machine project 2. $C_{\text{cab}}$ can be considered low because there is no high effort on trying to identify commonalities in the safety perspective between the two different product lines. $C_{\text{reuse}}$ (D) is low since there is no much overall reuse because the platform is not adapted for both product lines. There is however reuse in each product line and integration efforts to some extent. We evaluate such effort as medium since there is more reuse than in domain engineering but it cannot be considered as high either since it has potential to be increased i.e., to reuse more artifacts. Having different hazards in different product lines requires extra effort for each of them i.e., $C_{\text{unique}}$ (D) is high. There is also extra effort (but not as high as in the domain case) for specific product line members with their specific hazards ($C_{\text{unique}}$ (A) is medium). Because of not identifying all common safety artifacts between product lines, reusing them in future generations as well as maintaining them becomes more effort consuming ($C_{\text{evo}}$ and $C_{\text{maintenance}}$ are high).

Cost Impact in Scenarios 2.1 and 2.2

These two scenarios share the issue of not having identified all the commonalities and variability between product lines. This issue was pointed out in scenario 1.2, as well. $C_{\text{org}}$ (D) is high in both cases the organization spends effort on developing safety mechanisms (e.g., CAN buses for sending safety critical messages) that are unique for the machine project 1 and then, it spends extra effort for other mechanisms in the machine project 2. Same goes for testing because common tests for both product lines are not existent. Regarding $C_{\text{org}}$ (A), there is high effort on developing safety mechanisms and making them suitable for the platform as it is the case for the gateway, as well. However, $C_{\text{org}}$ (A) in scenario 2.2 can be considered medium instead of high since there is considerable testing effort only for one of the product lines (machine project 1). $C_{\text{cab}}$ is currently low since no high effort is being put on identifying commonalities between machine projects 1 and 2 (either on safety mechanisms or testing artifacts). $C_{\text{reuse}}$ (D) is not high since not much is being reused from previous generations in both perspectives (safety mechanisms and common tests). Consequently, $C_{\text{unique}}$ (D) is high. As for $C_{\text{reuse}}$ (A), there is some reuse of safety mechanisms and other artifacts (separately) in each product line e.g., there is common safety architecture for different product line members. There is also some reuse of common tests for the product line. Hence, we can conclude that there are integration efforts to some extent i.e., $C_{\text{reuse}}$ (A) is medium. For the same reason, $C_{\text{unique}}$ (A) is medium. Reuse for future generations and maintenance become more complicated and more challenging because of having different safety mechanisms (and lacking common tests) between product lines.
5.3.2.2 Area 2: Organizational Effort

The interviewees were asked about specific changes related to the organization structure that might contribute in the total product line cost (questions 7-11 in appendix A) while focusing on functional safety. In this perspective, the most significant issue attested in the interviews concerns the need to build and spread safety culture as much as possible all over the organization (table 10). During the past years, the organization has begun to embrace functional safety principles and apply them to product lines. Safety standards are being followed, other functional safety artifacts e.g., several safety plans are created and so on. For this reason, safety culture is important and high focus and efforts are put on it.

Table 10: Issues observed on the organizational side

<table>
<thead>
<tr>
<th>Challenges in the Organization</th>
<th>I1</th>
<th>I2</th>
<th>I3</th>
<th>I4</th>
<th>I5</th>
<th>I6</th>
<th>I7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building safety culture takes time and effort</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
</tr>
</tbody>
</table>

Issue 3: Building safety culture takes time and effort

Applying functional safety on Volvo CE product lines is a complex task. In order to achieve that, considerable effort has been put from the organizational side. However, functional safety in industry implies introduction of new concepts and new approaches. Hence, there is always space for improvements and increasing the organizational effort while building safety culture.

Scenario 3.1: Synchronization between distributed company sites

One big issue related to safety assessment in Volvo product lines is the distributed development in different Volvo sites all over the world. Different approaches are used in different product lines and applying the safety work products (PHA, safety goals and most importantly, functional safety concepts) is very challenging. There are cultural differences different solutions existing in each site. This complicates work synchronization.

Impact on Cost

The impact on cost for scenarios of issue 3 is presented in table 11.

Table 11: Cost impact of issues and scenarios related to organizational effort

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to organizational effort</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C\text{org}</td>
</tr>
<tr>
<td>3</td>
<td>Building safety culture takes time and effort</td>
<td>D</td>
</tr>
<tr>
<td>3.1</td>
<td>Synchronization between distributed company sites</td>
<td>H</td>
</tr>
</tbody>
</table>
Cost impact in scenario 3.1

The synchronization issues between Volvo sites bring to a high $C_{org}$ for domain engineering since different solutions are provided for a safety-related problem. On the other hand, the effort on each site for developing its own solution is not as high compared to $C_{org}$ for domain engineering ($C_{org}$ for application engineering is medium). Since there is distribution in the perspective of providing different solutions instead of a common one, we can evaluate $C_{cab}$ as low. For the same reason, $C_{reuse}$ for domain engineering is low while $C_{unique}$ for domain engineering is high. Meanwhile, there is more reuse of safety artifacts and mechanisms within each separate site. Therefore, $C_{reuse}$ for application engineering and $C_{unique}$ for application engineering can be considered medium. The presence of different solutions and the synchronization problems brings to higher effort for evolving the product lines to new generations and higher efforts to maintain them ($C_{evo}$ and $C_{maintenance}$ are high), as well.

### 5.3.2.3 Area 3: Core Asset Base, Reuse and Unique Efforts

The interviewees were asked regarding the common assets of the product lines and the effort for developing them as well as issues related to reuse processes and unique development (questions 12-26 in appendix A). Table 12 summarizes the significant issues that were identified for the core asset, reuse and unique efforts.

<table>
<thead>
<tr>
<th>Issues related to the core asset</th>
<th>I1</th>
<th>I2</th>
<th>I3</th>
<th>I4</th>
<th>I5</th>
<th>I6</th>
<th>I7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not identifying all commonalities in one product line or between different product lines presents obstacle for reuse and increases new development efforts</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>6</td>
</tr>
</tbody>
</table>

### Issue 4: Not identifying all commonalities complicates reuse and increases new development efforts

Issue 2 already pointed out the problem of not having all the commonalities between product lines identified. Besides that, issue 4 includes also the problem when not all commonalities have been identified between the products of the same product line, which has a direct impact on the core asset base and it complicates the reuse of safety artifacts from the core asset, as well. Consequently, reuse is not very high which causes extra effort on developing unique solutions and specific (safety) artifacts.

### Scenario 4.1: Considering functional safety for the common components in the engine is challenging

Three interviewees (I3, I4 and I5) state that there are common components that have been developed for a subsystem. At the beginning, they were not developed according to a specific functional safety standard. There is currently safety focus which is increasing by providing functional safety requirements for this subsystem. The common components are supposed to be utilized by different engine parts. However, this kind of reuse becomes more challenging
when introducing the common components into application since they have not been developed according to any functional safety standard.

**Scenario 4.2: Using different tools makes information tracking harder**
Currently, many different tools are applied. This causes the organization to spend more effort on managing information (e.g., safety requirements) in each tool and does not facilitate the identification of more commonalities between artifacts managed by different tools.

Another consequence of having different tools is that information tracking becomes more challenging. Traceability of data and changes made to different artifacts (e.g., requirements) is possible by tracking and reporting systems that help on tracking changes of information. Problems with traceability bring to loses of information (requirements, tests, documentation) which means that a lot of time is spent to track it again. Because of not tracing back all the information, reusing several safety artifacts becomes more challenging and thus, extra effort is put on developing new components and safety artifacts.

**Scenario 4.3: Extra functional safety effort for unique products in machine project 1**
Three interviewees (I1, I4 and I5) identify two specific products as new unique developed products within a machine product line. Extra effort on functional safety for these two products is represented by the separate safety cases that are developed especially for these products. The reason for this is also the fact that different SIL levels are required for these unique developed products in comparison to the other members of the machine product line.

**Scenario 4.4: Extra functional safety effort for different lines in the Machine project 1**
There is also differentiation between two lines inside the same product line. For example, this is the case for the high speed and low speed lines in the product line included in machine project 1. Different safety concepts, safety architecture, PHAs and other safety artifacts are developed for each line. As in the previous scenario with the two unique products, there is high specific effort on functional safety for each line.

**Scenario 4.5: Extra testing is performed**
There is extra effort in testing, as well. Common tests exists only for machine project 1 but not all commonalities have been identified in the product line that is part of the machine project 1 in order to develop more common tests and hence, avoid performing extra testing. Moreover, not all the functions have been analyzed in order to check if common testing solutions can be provided for them.

**Impact on cost**
The impact on cost for each scenario related to issue 4 is presented in table 13.
Table 13: Cost impact of scenarios from issue 4

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to the core asset base, reuse and unique efforts</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C_{org} C_{cab} C_{reuse} C_{unique} C_{evo} C_{maintenance}</td>
</tr>
<tr>
<td>4</td>
<td>Not identifying all commonalities complicates reuse and increases new development efforts</td>
<td>L H L M H M H H</td>
</tr>
<tr>
<td>4.1</td>
<td>Considering functional safety for common components in the engines is challenging</td>
<td>M H M M M H H H</td>
</tr>
<tr>
<td>4.2</td>
<td>Using different tools makes information tracking harder</td>
<td>M H M M M H H H</td>
</tr>
<tr>
<td>4.3</td>
<td>Extra functional safety effort for unique products in the Machine project 1</td>
<td>M H M M M H H H</td>
</tr>
<tr>
<td>4.4</td>
<td>Extra functional safety effort for different lines in the Machine project 1</td>
<td>M H M M M H H H</td>
</tr>
<tr>
<td>4.5</td>
<td>Extra testing is performed</td>
<td>M H M M M H H H</td>
</tr>
</tbody>
</table>

**Cost impact in scenario 4.1**

According to our view on analyzing the cost impact for scenario 4.2, functional safety has not been properly addressed when the common engine components were developed which means that $C_{org}$ (D) was low. $C_{org}$ (A) is high since it is hard to apply functional safety in different parts of the engines when there were issues with that in the common components. $C_{cab}$ can be also considered low since the core asset base is represented in this case by the common components that have not been developed according to any safety standard which means that safety effort in the core asset is low. There is some reuse from previous generations when developing these new common components. Meanwhile, reusing safety artifacts from the common engine components is hard and requires high integration effort because of not putting high effort at first in the common components. For these reasons, $C_{reuse}$ (D) is medium while $C_{reuse}$ (A) is high. Similarly, it can be concluded that $C_{unique}$ (D) is medium while $C_{unique}$ (A) is high. The problems with functional safety and standard compliance already in the core asset complicate reuse of safety artifacts in future generations and increase maintenance efforts, as well ($C_{evo}$ and $C_{maintenance}$ are high).
Cost impact in scenario 4.2
Problems with tracing information make the organization spend more effort on developing extra artifacts and solutions that were already existent (\(C_{\text{org}}(A)\) is high). \(C_{\text{org}}(D)\) is medium since there is no high focus on trying to put some effort for solving the traceability issues (\(C_{\text{cab}}\) is medium). As a consequence, there is no high reuse of safety artifacts and solutions (\(C_{\text{reuse}}(D)\) and \(C_{\text{reuse}}(A)\) are low). This brings to extra development of same artifacts and solutions. Therefore, \(C_{\text{unique}}(D)\) and \(C_{\text{unique}}(A)\) are high. If not solved, traceability issues affect negatively evolution and also maintenance because there are more artifacts, mechanisms and solutions to be analyzed, modified and maintained (\(C_{\text{evo}}\) and \(C_{\text{maintenance}}\) are high).

Cost impact in scenarios 4.3 and 4.4
The issues explained in both scenarios are similar and come because of not exploiting all the possible commonalities in the machine product line. In scenario 4.3, not all the commonalities between the unique products and the other product line members are exploited. In scenario 4.4, not all the commonalities between the two lines are identified. Hence, extra functional safety effort is put for the unique products and for each different line, as well. Such extra effort includes specific safety documentation, safety documentation and other artifacts for each line. The first cost impacts are as following: \(C_{\text{org}}(D)\) is medium (there is effort on identifying commonalities but this effort is not very high), \(C_{\text{org}}(A)\) is high (high safety effort on high lifts and each different line in machine project 1). Consequently, \(C_{\text{cab}}\) is medium. \(C_{\text{reuse}}(D)\) and \(C_{\text{reuse}}(A)\) are medium while \(C_{\text{unique}}(D)\) and \(C_{\text{unique}}(A)\) are high. Unique products and specific lines require special attention and extra effort when evolving and during maintenance, as well (\(C_{\text{evo}}\) and \(C_{\text{maintenance}}\) are high).

Cost impact in scenario 4.5
Not identifying all the commonalities and analyzing all functions brings to extra testing (\(C_{\text{org}}(D)\) and \(C_{\text{cab}}\) are medium while \(C_{\text{org}}(A)\) is high). Reuse of tests from previous generations is not very high and same goes for reuse in the current generation (\(C_{\text{reuse}}(D)\) and \(C_{\text{reuse}}(A)\) are medium while \(C_{\text{unique}}(D)\) and \(C_{\text{unique}}(A)\) are high). As a consequence, more specific tests mean higher effort for the next generation and for maintenance, as well (\(C_{\text{evo}}\) and \(C_{\text{maintenance}}\) are high).

5.3.2.4 Area 4: Evolutional Cost
The interviewees were asked regarding the product lines that have been evolving i.e., passing from old to new generations (questions 27-28 in appendix A). Moreover, they were asked about the effort associated with the new generations. Table 14 shows the issues identified regarding evolutional effort and the corresponding interviewees that pointed them out.

<table>
<thead>
<tr>
<th>Issues related to Evolutional Effort</th>
<th>I1</th>
<th>I2</th>
<th>I3</th>
<th>I4</th>
<th>I5</th>
<th>I6</th>
<th>I7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High effort related to safety evolution</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 14: Issues related to evolutional effort
There are challenges on reusing functional safety artifacts while evolving to new safety processes or when new functional safety standards are introduced in the industrial domain. Such evolitional changes complicate the reuse of safety artifacts and thus, extra effort is spent on developing new safety artifacts. Scenario 5.1 provides more details in this direction.

Scenario 5.1: High effort on functional safety while going through evolution processes
Evolution in the functional safety perspective is represented by situations when there are changes of strategies of addressing safety issues, new standards are introduced in the process (as it was the case when ISO 26262 started to be investigated) and so on.

New standards are published over time requiring new effort for functional safety. In this context, there were also some challenges with the development of new safety mechanisms and artifacts including here safety documentation. As an example, challenges are presented for defining all safety requirements. Challenges in defining requirements bring to more challenges in the next safety lifecycle phases.

Scenario 5.2: Integrating new added products in different product lines requires high effort
When passing to new industrial product line generations, new products might be added. An example would be the situation when products with new functionality were added in the machine project 1 (product line) and high integration effort was needed for them. This high integration effort comes from the differences that the new added products (new functionality) and the rest of the product line members. Identifying all commonalities between the new added products and existing members can be very challenging.

Impact on cost

Table 15 presents the cost impact for scenarios 5.1 and 5.2.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to the evolitional effort</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C组织</td>
</tr>
<tr>
<td>5</td>
<td>High effort related to safety evolution</td>
<td>H</td>
</tr>
<tr>
<td>5.1</td>
<td>High effort on functional safety while going through evolution processes</td>
<td>M</td>
</tr>
<tr>
<td>5.2</td>
<td>Integrating new added products in different product lines requires high effort</td>
<td>M</td>
</tr>
</tbody>
</table>

Cost impact in scenario 5.1
Since there were no many safety artifacts from previous generation, evolving to the current one required considerable effort in the safety perspective (C_演化 is high). The organization spent high effort as well on applying safety and making sure that different Volvo CE products...
are in compliance with functional safety standards ($C_{\text{org}}$ (D) and $C_{\text{org}}$ (A) are high). The effort put on the common artifacts (core asset base) is also considerable but we can consider it as medium in our case because of the issues mentioned in scenario 5.1 (e.g., not all the requirements are well defined). As it was already pointed out, reuse of safety artifacts from previous generations is low ($C_{\text{reuse}}$ (D) is low). Consequently, $C_{\text{unique}}$ (D) is high. On the other hand, common safety artifacts (safety documentation, common tests, PHAs and so on) that have been developed have high reuse potential in product lines. Hence, there has been some integration effort on reusing these common artifacts ($C_{\text{reuse}}$ (A) is medium) and some extra effort for applying functional safety on specific parts of the product line e.g., unique products in machine project 1 ($C_{\text{unique}}$ (A) is medium). Regarding maintenance, applying the platform in the new generation is expected to pay off by decreasing effort in maintenance since less specific parts would require maintenance.

**Cost impact in scenario 5.2**

High effort is put for adding new products (with new functionality) in the current product line in machine project 1. For this reason, we can consider a high evolutional effort ($C_{\text{evo}}$ is high). The organization spends significant effort on functional safety for integrating these new products ($C_{\text{org}}$ (A) is high). Analyzing more the commonalities and variability between the added products and the rest of the product line in the safety perspective is challenging ($C_{\text{org}}$ (D) and $C_{\text{cab}}$ are medium). As a consequence, reusing from previous generations becomes harder ($C_{\text{reuse}}$ (D) is low). However, they can reuse now some safety concepts, PHAs and other safety artifacts after they have been developed at first specifically for them ($C_{\text{unique}}$ (A) is medium). Safety maintenance is expected to take place later. Nonetheless, we can identify and predict high (hidden) maintenance efforts for added products because of the extra functional safety effort they require.

### 5.3.2.5 Area 5: Maintenance Effort

The interviewees were asked regarding the activities that are performed for maintaining the product lines and the effort that is being currently dedicated to them (questions 29-30 in appendix A). Only three interviewees could provide some feedback related to maintenance at Volvo CE and they consider that the main focus needs to be on maintenance activities related to functional safety.

#### Table 16: Issues related to maintenance effort

<table>
<thead>
<tr>
<th>Issues related to Maintenance Effort</th>
<th>I1</th>
<th>I2</th>
<th>I3</th>
<th>I4</th>
<th>I5</th>
<th>I6</th>
<th>I7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Considering functional safety during maintenance</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
**Issue 6: Considering functional safety during maintenance**

Results on effort related to maintenance effort in the functional safety perspective are hard to derive from our study since none of the seven interviewees is involved in maintenance activities. Based on this, it is not feasible to draw accurate or very reliable results on safety maintenance effort.

Nevertheless, three interviewees provided indirectly little information regarding maintenance which can be helpful on providing a preliminary view on the maintenance effort but that is not sufficient for drawing general results on the cost impact. However, we observed in general efforts that are necessary for different safety lifecycle phases. Hence, effort is expected in the post-development as well.

### 5.4 Discussion

The biggest challenge is the problem of allocating the appropriate cost to safety critical products. Engineers and other people involved in the industrial environment cannot state explicitly this part of the cost. In the previous subsection, we presented our view regarding the cost impact in different scenarios that were identified in the interviews. Analysis was performed for the following perspectives:

1. Scenarios (Major changes from previous generations)
2. Organizational effort
3. Core Asset Base effort
4. Unique parts effort
5. Reuse effort
6. Evolutional effort
7. Maintenance effort

Basically, the major cost-related issues identified during the interviews are presented in table 17.
### Table 17: Cost-related issues and key findings

<table>
<thead>
<tr>
<th>Issues and Challenges</th>
<th>Key Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Different strategies for product lines</td>
<td>There are differences between product lines in terms of management strategies for applying the platform and addressing functional safety.</td>
</tr>
<tr>
<td>2 Identification of commonalities and variability in product lines</td>
<td>There is currently no high effort on identifying more commonalities between Machine 1 and Machine project 2s that are relying on different solutions</td>
</tr>
<tr>
<td>3 Building safety culture takes time and effort</td>
<td>Safety is relatively new to all of the practitioners and hence, there is high focus on it. There have been safety education activities at Volvo CE but there are still some issues on safety assessment in practice (e.g., the platform case) that need to be overcome.</td>
</tr>
<tr>
<td>4 Not identifying all commonalities complicates reuse and increases new development efforts</td>
<td>All commonalities (between product lines and within the members of each product line as well) are not identified which makes reuse of common artifacts more challenging and encourages more new development i.e., higher extra or unique effort.</td>
</tr>
<tr>
<td>5 High effort related to safety evolution</td>
<td>Going through safety evolution, dealing with the introduction of new standards, new processes and so on, brings to more challenges for reusing several safety artifacts.</td>
</tr>
<tr>
<td>6 Considering functional safety in maintenance</td>
<td>Maintenance effort in the safety perspective is expected since we already identified safety effort in previous development stages. Nonetheless, not having maintenance experts among the interviewees makes it hard to derive accurate results on maintenance effort</td>
</tr>
</tbody>
</table>

While analyzing the cost impact for each of the ten issues presented in the table above, it could be noticed that there are dependencies between these 6 issues. In other words, one issue can be the trigger for other issues presented above. Figure 19 shows the dependencies between the issues presented in section 5.
Figure 19: Interdependencies between issues identified in the interview study

Having different solutions for platform integration in the two machine projects (issue 1) increases the difficulty of identifying commonalities between them (issue 2). The challenges related to identifying commonalities bring to challenges on reusing artifacts and thus, the effort on developing new safety content is increased (issue 4). Extra effort on developing more mechanisms and safety artifacts makes evolution to future product line generations (issue 5) and maintenance (issue 6) more challenging since there is more safety content to consider. Meanwhile, building safety culture requires more time and effort from the organizational side (issue 3). This is related directly to the industrial experience and knowledge of practitioners in the functional safety perspective and it has a cost impact on all the other issues since it regards the way how practitioners deal with functional safety in practice.
6. Conducted Study 2: Survey Study

6.1 Introduction
The survey structure has been adopted from the interview study. Basically, it consists of the same main parts that are presented in the interview questionnaire: general background and introduction, scenarios, organizational effort, core asset base effort, effort for unique parts, reuse effort, evolutional effort and maintenance effort. The survey questions are presented in the Appendix B of this report and we refer to them while discussing the survey results in this section.

The first part of the survey i.e., general background is a bit longer than in the interview. The reason is because the survey was meant for different practitioners from different organizations in different countries while the interview study was exclusively for Volvo CE practitioners and specialists. For example, we ask in the survey about the organization and the country where the respondent come from. Moreover, we ask about the domain of the organization, the experience of the respondent with functional safety, the safety standards or any cost modelling approach they are applying and so on (questions 1-16 in Appendix B).

Unlike the interview questionnaire, the survey contains more multiple-choice and single-choice questions since long text answers are usually not preferable in surveys and the respondents usually have a tendency to avoid such questions as much as possible.

The survey was sent out to different groups of software product line practitioners and industrial specialists that are part of the ISO 26262 group, as well. The survey was open for four months and was sent out several times during this period. Unfortunately, the number of people who responded is quite low. There are only six responses gathered in total. The information given by the six respondents is summarized and analyzed in subsection 6.2. Subsection 6.3 provides a discussion on the survey results and on the reasons why not many practitioners responded.

6.2 Survey Results

6.2.1 General Background
Six practitioners that work in different organizations in Sweden, Germany and USA answered the survey. Table 18 summarizes the answers given by the respondents regarding their general background, which includes the domain category, professional role of the respondent in the company, the amount of years of experience in industrial environments and on functional safety. This part is covered by questions 1-7 in appendix B.

Two companies are of a medium size (100-1000 employees) while one is a small company (<100 employees). The remaining three are all large companies (>1000 employees).

The first four respondents (software architect, safety manager, manager and safety engineer) consider their roles at their respective companies to be related to functional safety while the last two respondents state that there is no such relation. Nevertheless, both R5 and R6 explain
that they have been exposed to functional safety issues respectively to some extent (R5) and to a moderate extent (R6).

Half of the respondents (R2, R4 and R6) have more experience with functional safety (respectively 20, 6 and 10 years) while the others (R1, R3 and R5) have less experience on that (respectively 2, 2 and 1 year). Of course, the experience of each respondent with functional safety affects the answers provided in the survey. Other factors that influence the answers are the domain category as well as the role of the respondent in the domain.

Table 18: General overview of the survey respondents

<table>
<thead>
<tr>
<th>Respondent ID</th>
<th>Domain Category</th>
<th>Role of the respondent at the respective organization</th>
<th>Years of working in industry (and with Functional Safety)</th>
<th>Exposure to Functional Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Railway</td>
<td>Software Architect</td>
<td>21 (2)</td>
<td>Exposed but not sure to what extent</td>
</tr>
<tr>
<td>R2</td>
<td>Construction Equipments</td>
<td>Safety Manager</td>
<td>37 (20)</td>
<td>To a large extent</td>
</tr>
<tr>
<td>R3</td>
<td>Automotive</td>
<td>Manager</td>
<td>12 (2)</td>
<td>To a moderate extent</td>
</tr>
<tr>
<td>R4</td>
<td>Automotive</td>
<td>Safety Engineer</td>
<td>11 (6)</td>
<td>To a large extent</td>
</tr>
<tr>
<td>R5</td>
<td>Automotive</td>
<td>Software Developer</td>
<td>4 (1)</td>
<td>To some extent</td>
</tr>
<tr>
<td>R6</td>
<td>Automotive, Avionics, Aerospace and Healthcare Product Development</td>
<td>Consultant</td>
<td>35 (10)</td>
<td>To a moderate extent</td>
</tr>
</tbody>
</table>

Table 19 summarizes the answers given by practitioners when asked about functional safety standards, lifecycle standards, risk assessment techniques and cost modelling approaches that are being applied in their domains. This part corresponds to questions 8-11 in appendix B.

Among the answers given, ISO 26262 is the most applied functional safety standard. The only domain that is not applying it is the healthcare domain since it relies mostly on safety standards that are applied for medical equipments and devices (ISO 14971: 2009). The most used standards for lifecycle processes are CMMI and Automotive SPICE (ISO/IEC 15504). In fact, four companies out of six have an automotive domain. All six domains are performing either both PHAs and FMEAs or at least one of them with the exception of the third domain for which, R3 explains that no risk assessment is needed for their part of their analysis. The interesting part is the fact that two companies are actually applying established cost models in
their domains. R4 answers that his company is applying COCOMO II while the company where R6 is part of is applying both COCOMO II and its extension, COPLIMO. Unfortunately, there is no further information provided. For instance, it is unknown if they are applying only a part of these cost models or their full approach. Moreover, no information or reference exists regarding how successfully these two models are applied in the two domains.

### Table 19: Survey responses on functional safety and cost modelling

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>ISO 26262</td>
<td>SPICE (ISO/IEC 12207)</td>
<td>PHA</td>
<td>None</td>
</tr>
<tr>
<td>R2</td>
<td>ISO 26262, IEC 61508, ISO 15998, ISO 13849</td>
<td>None</td>
<td>PHA, FMEA</td>
<td>None</td>
</tr>
<tr>
<td>R3</td>
<td>ISO 26262</td>
<td>None</td>
<td>None (not needed for the main part of analysis)</td>
<td>None</td>
</tr>
<tr>
<td>R4</td>
<td>ISO 26262, CMMI, Automotive SPICE (ISO/IEC 15504)</td>
<td>None</td>
<td>PHA, FMEA</td>
<td>COCOMO II</td>
</tr>
<tr>
<td>R5</td>
<td>ISO 26262, Automotive SPICE (ISO/IEC 15504)</td>
<td>None</td>
<td>FMEA</td>
<td>None</td>
</tr>
<tr>
<td>R6</td>
<td>ISO 14971: 2009, CMMI</td>
<td>None</td>
<td>PHA, FMEA</td>
<td>COCOMO II, COPLIMO</td>
</tr>
</tbody>
</table>

Regarding the number of variants for the product line(s) in each domain, only three respondents provided an answer on that. Two of them stated that they are developing just one variant while another respondent stated that about ten variants exist in his domain.

As for the number of product line generations that each respondents has been involved in, only one respondent answered by writing that he has been involved in three different generations. The other respondents did not provide any answer on that and most of them comment that it is difficult for them to provide such answer.

#### 6.2.2 Scenarios and Organizational Effort

In the second page of the survey, the respondents had to define the main changes their domains usually face when passing to a new generation of a product line (question 15 in Appendix B). The number of domains that have gone through each change is presented in figure 20. Even in this case, the answers are influenced by the professional perspective of the respondent. For example, R4 (who is a safety engineer) identifies passing to higher SIL levels as a typical change when adapting a new product line generation. Nevertheless, the most common changes according to all six respondents are: platform change, platform modification...
or improvement, introduction of a new technology, using new tools and implementing in software (passing from software to hardware). As figure 20 shows, each of these changes has been identified by three different respondents.

In question 16, we ask about the effort (activities) that is put on the organization when changing to a new generation or a new project. Most of the respondents answer that training activities are held in this case. Three of them state that training activities are held for small scope while two choose training activities for big scope. In addition, one respondent answers that new expert groups are created while there is even one case where no change in the organization is reported.

![Figure 20: Changes from previous generations](#)
Figure 21: Activities with impact on the organization

Figure 21 presents the choices for each respondent when asked about the activities that have the highest organizational impact (question 17 in appendix B). The most common activities with the highest organizational impact result to be the introduction of new requirements, changing safety architecture parts and using new risk assessment techniques.

After the main activities are chosen, the respondents define also what kind of organizational impact they have in their context i.e., what kind of effort is put in the organizational perspective (question 18 in appendix B). The alternatives for organizational impact are:

A. No change.
B. Training activities are held (small scope).
C. Training activities are held (big scope).
D. New expert groups are created.
E. Changes in several departments.
F. Complete Reorganization (new departments/new management).

The most frequent responses for organizational impact includes: holding training activities (both small and big scope) and creating new expert groups for the new changes that come with the new generation of the product line or with a new project.

6.2.3 Core Asset Base Effort

In order to investigate the effort put on the core asset base, the survey respondents stated what their core assets consist of (by answering question 19 from Appendix B). They had the possibility to choose among the alternatives shown in figure 22 which summarizes and shows how many domains (out of the six that participated in the survey) are including each type of common artifacts in their core asset base.
Moreover, the respondents had to define the lifecycle phases where they put the highest and the lowest effort for developing and integrating new content (respectively question 20 and 21 in appendix B). The most frequent answers in this perspective regard the following common artifacts: communication links and protocols, common architecture framework, common testing framework and tools. Each of these common artifacts is identified as being developed by no less than four domains.

Two respondents stated that they either could not or were not sure about evaluating the respective phases with both highest and low effort. Another respondent sees the highest effort put on software analysis while hardware analysis and qualification take the lowest effort. Meanwhile, there is one case where the respondent cannot provide an answer for the highest effort but points out that the lowest effort is spent on system analysis. The opposite happens with another respondent who chooses both software and hardware analysis for the highest effort while there is no evaluation for the lowest effort. Finally, a safety engineer presents its point of view by attributing the highest effort to lifecycle phases that are mostly related to safety: Safety Concept, Safety Analysis, Software Analysis, System Analysis, Qualification and Safety Argumentation. This answer is influenced by the fact that the respondent is highly exposed to functional safety aspects.

6.2.4 Effort for Unique Parts
When asked about unique parts in their own context (question 22), half of the respondents answered that they either do not know or it is difficult for them to understand and identify these unique parts. For instance, one of them provides a general answer by stating that they...
are applying both software and hardware unique parts and the highest effort (question 23) is put on performing a specific FMEA for these parts. There are two more respondents that confirm the use and development of unique parts in their respective domains. However, they do not really specify what such unique parts consist in. The highest effort consists in performing a specific FMEA and keep specific safety documentation for the unique parts. Furthermore, one of the respondents foresees a trend of reusing such unique parts in the future (question 24).

The fact that four respondents did not identify any unique product or part in their product lines may come because of either not understanding the questions properly or not being directly involved in processes of developing such unique parts and applying functional safety for them.

6.2.5 Reuse Effort

Figure 23 indicates that the most common parts that are being reused (question 25) include safety analysis, software analysis and hardware analysis. Each of these common artifacts is identified by three different industrial experts who answered the survey. The domains that are reusing these parts at a high extent are mostly automotive and construction equipment domains. None of the domains involved in the survey study is reusing maintenance.

Moreover, most of the parts that were the most frequent choice regarding reuse of common development artifacts (software analysis and hardware analysis) seem to require the highest integration effort when reusing from common artifacts (question 26). Figure 24 shows the number of domains that consider such parts to require highest integration effort in their
context. In addition, one more practitioner adds that the highest integration effort in his context is put when reusing supporting documentation.

Figure 24: Highest integration effort when reusing from the common artifacts

The results related to the reuse level of risk assessment techniques documentation are presented in figure 25 (question 27 in appendix B). When the survey was started to be designed, the original question had quantitative values as choices e.g., the reuse level could be evaluated to be one of the following 0%, 20%, 40%, 60%, 80% or 100%. Afterwards, we started to test the survey with practitioners at Volvo CE and all of them stated that it is hard to provide statistical data for evaluating the reuse level of such documentation. This was the case with the reuse level of other safety artifacts, as well. Therefore, the choices were modified to fit instead a qualitative evaluation. This means that the respondent can choose among the following alternatives for evaluating the reuse level: no reuse, low reuse, to a moderate extent, large reuse and full reuse.

Figure 25 shows that not much documentation is being reused. PHA documentation is being reused in two domains: low reuse in a healthcare domain and reuse at a moderate extent in an automotive domain. FMEA documentation is reused at a low extent in two automotive domains. One of these domains is also using FMECA documentation to a low extent.

Figure 25: Number of domains that reuse risk assessment documentation
There are different reasons for having in general low reuse of risk assessment techniques or even no reuse at all in most of domains that participated in the survey. One reason can be that risk assessment documentation has been created recently and thus, it is yet early to start reusing this documentation. In subsection 6.2.2 which summarizes the findings on changes from previous generations and organizational effort, the activities with highest impact on the organization were reviewed. Half of the domains i.e., three of them seem to consider performing new risk assessment techniques as activities with highest organizational impact when working on a new product line generation. In this context, it can mean that high effort is put on creating risk assessment documentation and such effort is expected to pay off by reusing more risk assessment documentation in the future. However, there current reuse level is generally low.

Another reason for receiving answers regarding lack of reuse or low reuse of risk assessment documentation can be the fact that respondents may consider reusing risk assessment techniques as not much necessary for the part of product development they are currently involved in. For example, R3 who is a manager in an automotive domain explains that no risk assessment technique is actually needed for the part of analysis they are performing in their domain.

6.2.6 Evolutional Effort

We aim to investigate the effort spent when the product line evolves to a new generation by asking the respondents if they have added new products in their product line(s). The respondents have also the opportunity to specify what kind of products they have added (question 29) and the extra functional safety effort that is spent for integrating these new products in existing product lines (question 30).

Only two respondents confirmed that there have been cases when they added new products product to their existing product lines. Extra specific safety effort is identified for added products in both cases. For example, specific PHA is performed, specific parts of a standard (ISO 26262) are applied and specific safety documentation is kept.

Since the other four respondents did not provide any answer regarding added products, it was expected not to have extra functional safety effort for such products (answer for question 30 in appendix B) since there are no added products in their case. Two of these four respondents answered that there is no extra functional safety effort which is logical in their case because of not adding products. The problem regards the controversial answers provided by the other two respondents. Despite of stating previously that there are no added products in their case, they still defined extra functional safety effort attributed to product line evolution. The reason for providing such controversial responses can be that they were thinking in a hypothetical way i.e., what would be the extra functional safety effort in case they would add a new product. Another reason can be that they answered based on previous experiences they had with similar situations.

Figure 26 presents the number of domains that identify each case of applying extra functional safety effort when they add new product(s) in their existing product line(s).
The most common functional safety efforts regard specific efforts put on PHAs and FMEAs, specific effort for documentation and also for applying parts of functional safety standards.

### 6.2.7 Maintenance Effort

Finally, we investigate the general effort put on maintenance activities (question 31) as well as the effort put on maintenance in the functional safety perspective (question 32). Figure 27 summarizes the most common maintenance activities performed in the domains that participated in the survey. These activities require the highest overall maintenance effort for their product lines as well as for safety maintenance.

![Figure 27: Number of domains for identified maintenance activities with highest effort on product line maintenance in general and in the functional safety perspective](image-url)
Only three respondents answered the question related to the overall maintenance effort and two of them provided an answer regarding the highest effort on maintenance for functional safety. One reason for having few answers related to maintenance effort is the fact that none of the respondents is involved directly in maintenance activities. Therefore, it is difficult to evaluate maintenance effort by asking practitioners with other industrial backgrounds and profiles such as safety engineer, software architect and so on.

Moreover, maintenance activities that have highest integration effort depend on the domain type as well. For example, the activities with highest effort for maintaining medical devices in a healthcare domain regard mostly testing and replacement of some parts of such devices.

6.3 Discussion

The survey was available for about four months and was sent to a considerable number of practitioners from different domains and countries. They were contacted via email and LinkedIn. Nevertheless, only six of them completed the survey and this can be considered as a very low number compared to the number of practitioners that had the opportunity to access the survey.

One reason why the number of survey responses is very low can be the fact that practitioners might have considered the survey as too complicated for them and their industrial context. Moreover, each domain has its own way of dealing with functional safety. We aimed to adapt the survey questions (appendix B) in a general context as much as possible so it could fit all different types of industrial domains: automotive, avionics, construction equipment and so on. However, some respondents might have found it challenging to answer the questions in their own context.

Based on the fact that only a small number of practitioners answered the survey and based on the responses collected from the survey, it can be concluded that there is still a lot of work to be performed on functional safety in industry. There is still high uncertainty when it comes to discuss functional safety issues. Such uncertainty is observed in many answers provided by the survey respondents as well as by the interviewees in the first study.

Another reason for the low number of survey responses is that practitioners find it still very challenging to deal with functional safety cost estimation in practice. Same issue was identified in the interview study. In fact, we had to refine the semi-structured interviews several times in order to make them more understandable for the interviewees. It was not feasible to ask directly the interviewees for the functional safety effort in their context since it is hard to separate it from other efforts. We had a similar experience with the survey study, as well. The preliminary versions of the survey included questions that were aiming for a qualitative evaluation of functional safety effort. For example, there were questions asking to rate the reuse level of risk assessment techniques by choosing percentage values (e.g., 0% if there is no reuse, 20% of the complete risk assessment documentation, 40% and so on). When such questions were tested with different practitioners, all of them stated that it was not possible to provide such estimations. For this reason, we refined the survey questions so the respondents would have the possibility to evaluate functional safety effort in a more
qualitative way. For example, the respondents have the chance in the final version of the survey to evaluate if the reuse level of risk assessment techniques is low, moderate, high and so on. There is no need for them to make quantitative evaluation such as defining the percentage value for the part that is being reused.

Despite the fact of having only six answers from the survey, there is a considerable diversity regarding the following perspectives that were covered in our survey study:

- Different domains: automotive, railway, construction equipment, healthcare, avionics and aerospace
- Different industrial roles: software architect, safety manager, manager, safety engineer, software developer and consultant
- Different amount of industrial experience among the survey respondents: varying from 4 (1) to 37 (20) years of experience in industry (functional safety).

Having this diversity can be considered as positive in the perspective of extracting answers given by different points of view. However, a consequence is that some answers are influenced by the differences that exist between respondents. For example, a safety manager always sees the highest effort of developing common artifacts in performing safety analysis. This comes because the highest focus of the safety manager is on safety analysis.

Regardless, it is possible to derive some conclusions on functional safety effort estimation based on the six survey responses. As in the interview study, we observe that it is possible and feasible to decompose the overall functional safety effort in industrial product lines in several cost areas: organizational effort, core asset base effort, reuse effort, unique effort, evolutional effort and maintenance effort. However, several cost areas could not be depicted in every response provided for the survey study. This happened because the respondents had difficulties on answering or they simply did not have any information on it. For example, the questions for asking to evaluate the unique effort were answered properly by only two respondents.

We analyze further the results from the survey study in chapter 8 where we compare them with the results from the other two studies, as well.
7. Conducted Study 3: Documentation Analysis

7.1 Introduction

In order to support further the previous two studies (especially the data extracted from the interview study) and provide more evidence for the analysis, we performed an investigation on the following documentation at Volvo CE: safety plans, compliance documents, project plans, risk assessment documentation, guidelines, documentation reviews and testing documentation. The documentation analysis showed that the information and results extracted from the interview study are relevant and there is evidence that supports the key findings and scenarios presented in chapter 5.

7.2 Evidence for issues and scenarios related to changes from previous generations

Table 20 summarizes the list of documentation that provides evidence for supporting issues 1 and 2 that were identified while analyzing the interview results in chapter 5.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related changes from previous generation(s)</th>
<th>Evidence (documentation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Different strategies for product lines</strong></td>
<td>Software Configuration Safety Plan for the Platform, Safety Plan for the Platform and Machine 1 applications, Safety plan for Machine 2</td>
</tr>
<tr>
<td>1.1</td>
<td>Different decisions of utilizing the platform in different product lines</td>
<td>Software Configuration Safety Plan for the Platform, Safety Plan for the Platform and Machine 1 applications, Safety plan for Machine 2</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Focus on preserving Machine 1 functionality while integrating the platform</td>
<td>Safety Plan for the Platform and Machine 1 applications</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Focus on preserving Machine 2 architecture and functionality</td>
<td>Safety plan for Machine 2</td>
</tr>
<tr>
<td>1.2</td>
<td><strong>Identification of commonalities and variability between product lines</strong></td>
<td>Safety Plan for SIL 1 compliance for Machine project 1, Safety plan for Machine 2</td>
</tr>
<tr>
<td>2</td>
<td>Identification of commonalities and variability in safety mechanisms and artifacts</td>
<td>Safety Plan for SIL 1 compliance for Machine project 1, Safety plan for Machine 2, Risk Assessment Documentation</td>
</tr>
<tr>
<td>2.1</td>
<td>Identification of commonalities and variability in test specifications</td>
<td>Verification and Validation Guidelines, Test Design and Architecture for Machine 2</td>
</tr>
</tbody>
</table>
Issue 1 and its scenarios consist in differences between Machine 1 and Machine 2 when it comes to safety solutions. Machine 2 relies on the gateway as it was already explained in chapter 5. Unlike Machine 2, Machine 1 utilizes and reuses safety artifacts from the platform. The evidence found on documents such as the Safety Plan for the Platform and Machine 1 applications support this fact even more. Moreover, the Software Configuration Safety Plan provides more information related to the scope of the platform project in the safety perspective. First of all, reuse of mechanisms and artifacts from the previous generation is attested in the document (as it was already pointed out in the interview study, as well). The idea is that common software components and common functions will be part of the platform. These common artifacts will therefore serve as a framework to utilize or choose from while developing different types of applications. This way, the unique development effort i.e., effort on developing separately each application is significantly reduced. In the document, it is mentioned that the platform is intended for all machines. Nevertheless, it has currently been adapted only for the Machine 1 applications.

Issue 2 is about the challenges on analyzing and identifying commonalities between the two machine projects. In scenario 2.1, challenges regard the commonalities in terms of safety mechanisms and artifacts. Different mechanisms and artifacts (e.g., different safety concepts, different PHAs and so on) are used indeed specifically for each machine project. For this purpose, we compare the safety plans for each machine project (Safety Plan for SIL 1 compliance for machine project 1 and Safety plan for machine 2) and we also checked the PHA and FMEA documentation for the machine applications.

### 7.3 Evidence for issues and scenarios related to the organizational effort

Table 21 summarizes the list of documentation that provides evidence for supporting issue 3 and its main scenarios (related to organizational effort) that were identified while analyzing the interview results in chapter 5.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to the organizational effort</th>
<th>Evidence (documentation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Building safety culture takes time and effort</td>
<td>Production and Operation Safety Plan for the Platform Project, Top Level Safety Plan</td>
</tr>
<tr>
<td>3.1</td>
<td>Synchronization between distributed company sites</td>
<td>Documentation and evidence for only one site (Volvo CE in Eskilstuna, Sweden)</td>
</tr>
</tbody>
</table>

In the general description of the Production and Operation Safety Plan for the Platform Project, the importance of building safety culture is highlighted and its high priority over other tasks (e.g., meeting deadlines) is specified, as well.

Regarding scenario 3.1 i.e., the synchronization issues between different Volvo sites, we would normally need documentation from different Volvo sites distributed all over the world.
In reality, we have analyzed only the documentation related to products developed at one Volvo CE site. Practitioners (e.g., I3 and I4) have industrial experience on product development and safety assessment at Volvo CE and they are also aware of other solutions developed in other Volvo sites.

### 7.4 Evidence and issues related to the core asset base, reuse and unique efforts

Table 22 summarizes the list of documentation that provides evidence for supporting issue 4 and its main scenarios related to core asset base, reuse and unique efforts that were identified while analyzing the interview results in chapter 5.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to the core asset base, unique and reuse efforts</th>
<th>Evidence (documentation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Not identifying all commonalities complicates reuse and increases new development efforts</td>
<td>Safety Plan for SIL 1 compliance for Machine project 1, Safety Plan for Machine 2, Risk Assessment Documentation</td>
</tr>
<tr>
<td>4.1</td>
<td>Considering functional safety for the common components in the engine is challenging</td>
<td>We could not identify any evidence related to scenario 4.1 in our documentation analysis</td>
</tr>
<tr>
<td>4.2</td>
<td>Using different tools makes information tracking harder</td>
<td>Tool Chain Safety Plan for the Platform</td>
</tr>
<tr>
<td>4.3</td>
<td>Extra functional safety effort for unique products in the Machine project 1</td>
<td>Safety Plan for Machine 1, Risk Assessment Documentation</td>
</tr>
<tr>
<td>4.4</td>
<td>Extra functional safety effort for different lines in the Machine project 1</td>
<td>Qualification Document, Safety Plan for Machine 1, Risk Assessment Documentation</td>
</tr>
<tr>
<td>4.5</td>
<td>Extra testing is performed</td>
<td>Tool Chain Safety Plan for the Platform, Verification and Validation Guidelines, Test Design and Architecture for Machine 2</td>
</tr>
</tbody>
</table>

As it was already pointed out in chapter 5, not all commonalities have been exploited between (and within) product lines. This presents an obstacle for achieving higher reuse and therefore, it encourages more unique development i.e., higher extra effort. We identify these issue by comparing different safety plans for each product line. There are big differences on safety assessment, starting from different safety concepts, different safety requirements and so on. Regarding extra unique development, such unique effort is identified by the specific risk assessment techniques that are performed for different Machine 1 applications (PHA and FMEA documentation for Machine 1 applications).

Scenario 4.1 addresses the problem that functional safety has not been addressed in the common engine components when they have been developed. For this scenario, we could not identify any reference to it in the documentation analysis.
In scenario 4.2, different tools are used in Volvo CE for managing information which makes information tracking more complicated and more effort consuming in a cross functional scenario when different product lines should be managed. The Tool Chain safety plan suggests that extra safety effort is put on each tool since the organization should make sure that each tool is fulfilling functional safety requirements as specified in the standard (IEC 61508). It is also aimed that a certain safety level (e.g., ASIL C) should be achieved for each tool.

In scenario 4.3, there is extra effort for unique products within machine project 1. Extra effort for unique machine 1 applications is represented by specific safety concepts, specific safety requirements, separate risk assessment techniques performed for these unique applications. The PHA and FMEA documentation for these applications provides further support for these statements.

As for scenario 4.4, there is extra effort for different lines within the same product line (machine 1). Different lines are suitable for different use conditions e.g., one line is intended for being used on road while the other line is intended for being used off-road. This implies extra specific effort on assessing different safety levels for each line. It also means extra effort on the qualification of hardware components (as it is suggested in the Qualification document). This means that extra effort is put on testing each line in the right environment to make sure that the hardware component or part is exposed to the intended environmental and operational conditions and compliance with its functional requirements is assessed.

Finally, scenario 4.5 consists on the extra testing that is performed for each machine project because of not identifying many commonalities between them. Moreover, we analyzed testing documentation for machine applications and for Requirements Management Tool, as well. The Requirements Management Tool is a tool that is used for modeling requirements, managing development activities and issues as well as development of test specifications i.e. test design, test procedures, test coverage of requirements, test suites and test documentation. Extra testing is being performed for this tool, as well because there is more information to manage in the tool.

7.5 Evidence and issues related to the evolutional effort
Table 23 summarizes the list of documentation that provides evidence for supporting issue 5 and its main scenarios (related to evolutional effort) that were identified in chapter 5.
The effort put on safety assessment for the current generations of different product lines is significant because no much safety heritage was inherited from previous generations. This is proved also in terms of documentation effort. The organization has put significant effort on creating documentation for safety assessment of Volvo CE product lines and applications. Examples for that are safety plans, Compliance documents for making sure that the applications are following the safety requirements as specified in the functional safety standards and so on.

Scenario 5.1 is about safety evolution. A typical example of safety evolution is represented by the situation when new standards are being introduced for the organization. In our documentation analysis, documents as functional safety standards as well as compliance documents were also analyzed. ISO 15998 and IEC 61508 are the standards that are being followed at Volvo CE. In addition to these standards, ISO 26262 is investigated in order to understand the state of the art. In fact, ISO 26262 is a domain specific adaptation of IEC 61508, another standard used and applied at Volvo CE. On the other hand, ISO 15998 principles are followed for control systems of the machines that have electronic components. The normative standard ISO15998 for machine control systems using electronic components is harmonized with the standard EN 474-1 Earth moving machinery, Safety, General requirements which in turn is harmonized with the EU Machinery Directive (Law). Harmonized means that if all normative requirements are fulfilled in a standard, then the legally binding machine directive is automatically fulfilled.

In scenario 5.2, we pointed out the effort put on integrating added products to the product line. In fact, there were different applications or products added to a certain product line. These applications or products usually introduce a new functionality and this causes high integration efforts. In the risk assessment documentation, we identified specific safety effort (separate PHAs and FMEAs) for products and new functionality added to the product line in machine 1.
7.6 Evidence and issues related to the maintenance effort

Table 24 summarizes the list of documentation that provides evidence for supporting issue 6 and its main scenarios (related to maintenance effort) that were identified while analyzing the interview results in chapter 5.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to maintenance effort</th>
<th>Evidence (documentation)</th>
</tr>
</thead>
</table>

As it was stated in chapter 5, none of the seven interviewees is involved directly in maintenance activities. Same thing happens with the documentation analysis since none of the analyzed documents could provide a detailed overview of the maintenance activities.

Nevertheless, it is possible to extract some information indirectly from the documentation we analyzed. In the Production and Operation Safety Plan for the Platform, the importance of making a safety plan for maintenance processes is addressed. This safety plan is supposed to consider the requirements for maintenance and repair of defects and hazards attested in Volvo CE machines and applications. The plan is also supposed to describe the sequence and methods of maintenance activities as well as the necessary tools (e.g., diagnostic tools) for performing them. Of course, maintenance activities are planned for verifying safety-related characteristics of the applications, as well. For example, it should be verified if a certain SIL level is being manifested when using a certain machine application or it should also be verified if a product is working properly and safely in the environment for which it was intended.

Meanwhile, the Software Configuration Safety Plan for the Platform highlights the importance of having common software components in the platform. One of the benefits pointed out in the document would be also the reduction of the cost and time needed for maintaining Volvo CE machines and their applications. Hence, this document provides an evidence for the cost impacts (in this case, the relation between core asset base, reuse and maintenance costs) we identified in chapter 5.

In order to provide better results on cost impact for maintenance, we need more detailed documentation on the actual current status of performed safety activities at Volvo CE (the two documents above regard more planning and predictions). Hence, more sustainable evidence is needed for the future as well as relying on the industrial expertise of practitioners who are involved directly on maintenance activities. These are both considered as potential directions for future work.
7.7 Summary

The purpose of this documentation analysis is to provide more evidence for supporting the results and conclusions on cost impact that are presented in the interview study. After going through each issue and scenario identified in the interview study, it was possible to find evidence in Volvo CE documentation for supporting each of them.

However, there are cases when it was not managed to find directly evidence in the documentation for a certain scenario. This was the case with scenario 3.2 which points out the synchronization problem between different Volvo sites. Since no documentation related to other Volvo sites rather than Volvo CE was analyzed, it is hard to provide directly evidence from documentation for supporting it. However, we rely totally on the industrial expertise of practitioners in this case since they have experience and knowledge on differences and synchronization issues between different sites.

Scenario 4.1 was another scenario for which it was hard to provide directly evidence from the documentation analysis. Common components in the engines are not mentioned or referred in any reviewed safety documentation either which so far, supports the finding from the interview study.

Finally, information for safety maintenance needs to be more detailed and enriched in order to draw better conclusions on the cost impact in this perspective. Moreover, safety maintenance activities have been planned but more time should pass in order to analyze and evaluate how they are being performed and what is their impact. Nevertheless, preliminary conclusions can be drawn and the information gathered from the interviewees and documentation is sufficient for drawing them or analyzing the impact of the hypothetical maintenance situations e.g., when effort put on maintenance is not very high and so on.

In general, it can be added that this documentation analysis serves also for validating the results derived from the interviews.
8. Analysis

In this chapter, we evaluate the results that are derived from the three studies.

We identified six main issues and their respective scenarios in the interview study as well as their impact on functional safety effort. Then, the documentation analysis provided more evidence for the issues and scenarios derived from study 1 since they were also identified in different documents related to Volvo CE product lines and applications.

On the other hand, the survey study provided data from other industrial domains on how they are managing functional safety in product lines and applications in their respective domains.

However, we cannot identify or get directly any effort related to functional safety through analyzing the results from the three studies.

8.1 Conducted Studies 1 and 3

In study 1, we identified six main issues that have a cost impact in the safety perspective. Moreover, we found evidence for each issue in the documentation analysis performed in study 3.

8.1.1 Areas for improvement related to issue 1

In chapter 5, the problem of having different strategies for each machine project was underlined. We evaluated the cost impact of this issue by presenting the way how each cost factor is affected.

Scenario 1.1 is about the different decisions made for different machine projects in terms of utilizing a new platform generation. Machine project 1 reuses safety artifacts from the platform while Machine project 2 relies instead on the gateway which is a specific solution. Relying on different solutions has a high cost impact on the overall system in different perspectives, as it was explained in chapter 5.

One possibility for improvement and reducing this high cost impact would be adapting the platform for both machine projects. This would require at first a significant increase on the effort put on identifying more commonalities between the product lines (product line 1 and product line 2) in order to facilitate platform integration for product line 2, as well. Hence, the core asset base cost will be significantly increased. In that situation, the organization would spend less effort on developing common safety artifacts for the platform (instead of putting specific effort on platform integration for machine 1 applications and specific effort for the gateway in machine 2 ones). Therefore, one consequence would be the significant decrease of the cost for organization in domain engineering. Moreover, the effort on developing common safety artifacts and mechanisms (e.g., CAN buses for sending safety critical messages) for each product line would be still highly reduced since both machines would be sharing artifacts (e.g., using same CAN buses) from the platform projects. This means that $C_{org}$ would be reduced for both domain and application engineering.

Regarding reuse, the increased effort on identifying commonalities would bring to an overall reuse increase (both product lines reusing from the platform) as well as to an increase of
reuse within each product line (more commonalities would be identified between the product lines in the two machines which would mean more internal reuse and less unique development in each of them). This increase of the reuse level is associated with a higher reuse effort (for both domain and application engineering) since more integration efforts would be needed. However, the integration efforts would be not significantly higher (they would rather be slightly higher) since more safety commonalities (safety mechanisms and artifacts) would be identified by reusing the platform).

The reuse increase would also bring to less developed specific applications for the two machines ($C_{\text{unique}}$ for application engineering is significantly decreased). For example, there are specific machine 1 applications that right now require high specific functional safety effort (specific safety concepts, specific safety architecture and documentation). Exploring more common artifacts has potential for reducing the differences between specific machine one products and the rest of the members in the product line. Moreover, the overall unique effort i.e., $C_{\text{unique}}$ for domain engineering (both machines relying on one platform comparing to current situation of relying in different solutions i.e., developing safety artifacts for the platform in Machine 1 and other safety artifacts in Machine 2) would be also significantly reduced.

Another positive impact regards evolutionary and maintenance efforts. Since there would be more common safety mechanisms and safety artifacts (concepts, safety architecture, parts of safety plans and so on) between product lines and consequently, less unique parts, the effort put on evolving them to new generations (assuming the content is not changing significantly in the new generation) as well as the effort needed for maintaining them would be significantly reduced.

Regarding the other scenarios of issue 1, the key for obtaining cost savings relies on identifying more commonalities for each product line. Hence, the logic is the same as in scenario 1.1. More effort is needed for the commonality-variability analysis i.e., for the core asset base. The other cost factors will be affected in the same way as in scenario 1.1.

Table 25: Increase of $C_{\text{cab}}$ in issue 1 and impact on other cost factors

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios of changes from previous generation(s)</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$C_{\text{org}}$</td>
</tr>
<tr>
<td>1</td>
<td>Different strategies for product lines</td>
<td>↓↓</td>
</tr>
</tbody>
</table>

We summarize the dependencies between cost factors in table 25. When a cost factor has been significant increased (e.g., $C_{\text{cab}}$ in scenario 1.1), we note it as “↑↑” in the table. If the increase is not significant, “↑” is used to show the slightly increased cost. Same goes for the cases when the cost is decreased. When the cost factor suffers significant decrease, “↓↓” is used. On the other hand, “↓” implies a slightly decrease of cost. For issue 1, $C_{\text{cab}}$ (highlighted in
the table) represents the cost factor which is changed (increased significantly) and this change affects the rest of the cost factors.

The main idea is that if more focus and effort is put on analyzing all commonalities between the two product lines (i.e., increase $C_{cab}$) in order to make it possible to integrate the platform for both product lines, the other cost parts will be affected as it is shown in table 25.

8.1.2 Areas for improvement related to issue 2

Issue 2 highlights the challenge of identifying commonalities between product lines (commonalities in terms of safety mechanisms in scenario 2.1 and testing commonalities in scenario 2.2). The identification of commonalities is right now challenging because of the different strategies that each product line use (explained in issue 1). An area for improvement in this case would be to analyze more common safety mechanisms as well as other artifacts (tests and so on) in order to make it possible to apply one strategy (i.e., platform integration) in both product lines. This way, extra safety effort would be significantly reduced in both sides since both product lines would be reusing common platform artifacts (e.g., common safety requirements, common safety mechanisms, common safety tests and so on). As in the area for improvement proposed for issue 1, $C_{cab}$ needs to be significantly increased. Consequently, the other cost factors will be affected in the same way as we explained in subsection 8.1.1. Table 26 provides an illustration of cost dependencies in this case.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios of changes from previous generation(s)</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$C_{org}$</td>
</tr>
<tr>
<td>2</td>
<td>Identification of commonalities and variability between product lines</td>
<td>↓↓</td>
</tr>
</tbody>
</table>

8.1.3 Areas for improvement related to issue 3

Issue 3 originates from problems related to the organizational side. Building safety culture should not be seen as a task that can be accomplished successfully in a short time. Effort and time is required for building some industrial expertise on applying properly functional safety in a certain domain. For example, there is high focus on functional safety in general at Volvo CE.

The problem stated in scenario 3.1 in chapter 5 can be solved by increasing the effort on synchronizing work related to safety assessment between different Volvo distributed sites. If this effort ($C_{org}$ (D) and $C_{cab}$) is increased at first, then there will be no need to have so many specific safety solutions for each site. Rather than that, each of them would have the possibility to reuse common safety solutions ($C_{org}$ (A) and the rest can decrease).
Table 27 summarizes the changes of different cost parts depending on the increase of the organizational effort (in order to provide solution for issue 3).

**Table 27: Increase of Corg (D) and Ccab in issue 3 and impact on other costs**

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to organizational effort</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Corg</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>3</td>
<td>Building safety culture takes time and effort</td>
<td>↑↑</td>
</tr>
</tbody>
</table>

8.1.4 Areas for improvement related to issue 4

In issue 4, focus is needed for indentifying more safety commonalities in each product line (or between product lines) in order to increase the reuse of safety artifacts and mechanisms and hence, reduce extra safety effort. There are five scenarios with small differences in cost impact. For this purpose, we evaluate the cost impact separately for each scenario.

The cost impact for each scenario is presented in table 28.

**Table 28: Increase of Corg (D) and Ccab in issue 4 and impact on other cost factors**

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to core asset base, reuse and unique efforts</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Corg</td>
</tr>
<tr>
<td>4</td>
<td>Not identifying all commonalities complicates reuse and increase new development efforts</td>
<td>↑↑</td>
</tr>
<tr>
<td>4.1</td>
<td>Considering functional safety for the common components in the engine is challenging</td>
<td>↓↓</td>
</tr>
<tr>
<td>4.2</td>
<td>Using different tools makes information tracking harder</td>
<td>↑↑</td>
</tr>
<tr>
<td>4.3</td>
<td>Extra functional safety effort for unique products in Machine project 1</td>
<td>↑↑</td>
</tr>
<tr>
<td>4.4</td>
<td>Extra functional safety effort for different lines in Machine project 1</td>
<td>↑↑</td>
</tr>
<tr>
<td>4.5</td>
<td>Extra testing is performed</td>
<td>↑↑</td>
</tr>
</tbody>
</table>
In scenario 4.1, safety has not been considered at all in the common engine components. If high effort will be put right now on applying safety standards (concepts and other safety artifacts) in the common components (i.e., increasing significantly $C_{org}(D)$ and $C_{cab}$), then it would pay off by reusing these safety artifacts in the engine, later. Hence, $C_{org}(A)$, $C_{unique}(A)$, $C_{evo}$ and $C_{maintenance}$ would be significantly decreased. On the other hand, $C_{reuse}(A)$ would suffer a slight decrease since more safety artifacts would be reused. For example, if safety concepts, safety goals and safety requirements will be available for common components in the engine, then these safety artifacts would be reused at a high extent by other engine components, as well. However, considering safety for the common components would mean to start from the beginning because there is no previous safety assessment for these components. Hence, $C_{reuse}(D)$ would be minimal while $C_{unique}(D)$ would be very high.

In scenario 4.2, the existence of different tools for managing data at Volvo CE complicates information tracking. Exploiting more commonalities between different artifacts distributed in different tools can help on reducing the number of unnecessary data and artifacts (e.g., duplicated safety requirements) and hence, reduce the number of tools as well. This requires an increase of $C_{cab}$ but it would contribute in overall cost savings since there would be less tools for managing ($C_{org}(D)$ would be highly decreased). There would be also more reuse between information in different tools ($C_{org}(A)$, $C_{unique}(D$ and A), $C_{evo}$ and $C_{maintenance}$ would be decreased). However, there would be more reuse between tools as well as within each tool. Hence, reuse efforts would increase slightly.

Scenario 4.3 and 4.4 are about the extra effort put on safety for unique products (scenario 4.3) and different lines (scenario 4.4) within product line 1 at Volvo CE. More effort should be put on finding commonalities between different product line 1 members (increase $C_{cab}$ and $C_{org}(D)$) in order to be able to share more common artifacts and hence, decrease the development of specific safety artifacts (reduce $C_{org}(A)$, $C_{unique}(both D and A)$, $C_{evo}$, $C_{maintenance}$). Reuse efforts will thus, be slightly increased.

Same situation and same cost impacts as in scenarios 4.3 and 4.4 are relevant for scenario 4.5, as well. This is because the problem in scenario 4.5 is quite similar. There is high potential to reduce extra testing which is mostly happening for Machine project 1. Performing unnecessary extra machine testing (including here safety tests) can be avoided by putting more focus and effort on identifying more common test specifications and commonalities in test design. Hence, the idea here is also to increase the core asset base effort (increase of $C_{cab}$) and the focus of practitioners involved in testing into identifying at first such commonalities (increase of $C_{org}(D)$). This effort will pay off by causing a significant decrease of most of other costs.

8.1.5 Areas for improvement related to issue 5
In scenario 5.1, the problem of not having much safety legacy from previous product line generations to rely on is pointed out. Therefore, significant effort has been shown from the organizational side in terms of embracing functional safety at Volvo CE for current product line generations. However, an area for improvement (for next generations) would be to have better well-defined requirements in place. This will have a positive impact on cost savings.
regarding development of safety artifacts in later phases i.e., safety architecture, safety components, safety tests and so on. This means to increase $C_{evo}$ as well as $C_{cab}$ and $C_{org}$ (D) for the next generation. Meanwhile, this would facilitate development and reuse of safety artifacts ($C_{unique}$ (A) and $C_{unique}$ (D) will be decreased). $C_{reuse}$ (D) and $C_{reuse}$ (A) will be a bit higher since for the next generation, there are available safety artifacts (requirements, safety mechanisms and so on) for being reused. Maintenance will be facilitated as well. Hence, maintenance effort in safety perspective is also expected to be lower in the next generation.

Table 29: Increase of $C_{evo}$ in issue 5 and impact on other cost factors

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to evolutional effort</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$C_{org}$</td>
</tr>
<tr>
<td>5</td>
<td>High effort related to safety evolution</td>
<td>D</td>
</tr>
<tr>
<td>5.1</td>
<td>High effort on functional safety while going on evolution process</td>
<td>↑↑</td>
</tr>
<tr>
<td>5.2</td>
<td>Integrating new added products in different product lines requires high effort</td>
<td>↑↑</td>
</tr>
</tbody>
</table>

Integrating new added products requires sometimes high safety effort. One reason can be that a higher SIL level is required for the added product comparing to the other existing product line members. One possible solution would be to focus on achieving the maximum of the SIL levels required for different products in the product line. This implies high effort while going through evolution (adding the product in the product line). Hence, there is a significant increase of $C_{cab}$, $C_{evo}$ and $C_{org}$ (D). $C_{unique}$ (D) will be a bit higher in the beginning since the new product is added and extra effort should also be considered for reaching the maximal SIL level. On the other hand, this solution would facilitate reuse between the added product and the rest of the product line. Moreover, there will be also less specific functional safety effort attributed to the added product since it will be sharing more common artifacts with the other product line members.

8.1.6 Areas for improvement related to issue 6

In order to provide a better analysis on the maintenance effort in the functional safety perspective and the impact that it has in other costs, we would need to have answers and feedback from practitioners that are involved directly in maintenance activities. Nevertheless, maintenance effort can be expected to decrease when there are less unique parts to be maintained. According to such view on cost impact, safety maintenance cost can be decreased by putting more effort into developing common safety artifacts and developing less specific ones.
Considering functional safety during the process of maintaining industrial product lines at Volvo CE and generally, in different domains can bring to several benefits and cost savings. Table 30 summarizes the impact of the increasing safety maintenance effort on other cost perspectives.

Table 30: Increase of Cmaintenance in issue 6 and impact on other cost factors

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Issues and scenarios related to maintenance effort</th>
<th>Impact on Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Corg (\uparrow) (\downarrow)</td>
<td>Cab (D) (\uparrow) (\downarrow)</td>
</tr>
<tr>
<td>6</td>
<td>Considering functional safety during maintenance</td>
<td></td>
</tr>
</tbody>
</table>

Considering functional safety during product line maintenance raises the chances for identifying possible defects, hazards or irrelevant states in different machines, product lines, hardware or software functions. By doing so, it is possible to give the organization the opportunity to increase the quality of the product lines. This happens because of the identified hazards and defects during safety maintenance. After that, the organization can take measurements (e.g., perform common FMECAs for the hazards) in order to fix them. Therefore, \(C_{org}\) (D) and \(C_{cab}\) increase while \(C_{org}\) (A) decreases. On the other hand, performing for example common FMECAs or other risk assessment techniques will pay off because they will be reused for different products. This means that both reuse and unique efforts will be low in the application engineering while they will suffer an increase in the domain engineering. The reason for that is because effort is put on the beginning for addressing the hazards found during safety maintenance. After hazards have been addressed, then it is also easier to evolve the product line since the hazards have been already identified and addressed in the current generation.

### 8.2 Conducted Study 2

There is less information and feedback obtained from study 2 compared to the one gathered from studies 1 and 3. Survey answers are provided by only six respondents in total. Moreover, not all the survey questions have been answered by them in the survey. This makes it even more challenging to derive findings and results regarding effort and cost in functional safety.

One of the main reasons for having few answers is related to issue 3 which we discussed in the interview study. Time and effort is needed to build a better safety culture and experience in industry. Functional safety involves complex strategies that should be considered when applying it in industrial product lines. For these purpose, there is still uncertainty when industrial experts are asked to discuss estimation of functional safety effort in the industrial product lines they are developing and maintaining. The reason is that the functional safety effort is usually hidden or hard to extract from the overall effort. For example, it is hard to estimate the effort attributed specifically to safety requirements and separate it from the overall effort spent in general for defining all requirements.
Since there is lack of information related to different effort areas, it is not feasible to derive cost dependencies as in the interview study. However, it is possible to derive findings regarding the cost areas identified in the survey results.

In order to check if the identified cost areas in the survey study correspond to the same context as they were identified in the interview study, we need to evaluate the similarity between the different contexts they are used.

Although, we had only six survey responses to analyze, it was possible to identify the same cost areas as in study 1: organizational effort in domain and application engineering, core asset base effort, reuse effort in domain and application engineering, unique effort in domain and application engineering, evolutional effort and maintenance effort. As in the interview study, we focus here only on the effort related to functional safety.

In table 31, we evaluate and quantify the level of similarity between the context in which the cost areas are identified in the interview study and the context in which they are identified in the survey study. For making this evaluation, we use one the following designations:

- 5 – The contexts match perfectly or they are very similar.
- 4 – The contexts of using the cost area are similar.
- 3 – The contexts of using the cost area are not similar or the similarity is very small.
- 2 – The contexts of using the cost area are different.
- 1 – The contexts of using the cost area are very different or completely different.
- 0 – No finding related to the cost area can be derived from the survey study.

<table>
<thead>
<tr>
<th>Identified Cost Areas in Study 2</th>
<th>Cost Areas</th>
<th>Similarity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Corg Ccab Creuse Cunique C.evo Cmaintenance</td>
<td>5 0 5 5 5 3 4</td>
</tr>
</tbody>
</table>

Regarding the organizational effort in the survey study, the responses consisted of several changes in the industrial domains such as introduction of new safety requirements and their impact on the organization. The organizational impact includes mostly training activities and creation of expert groups. This corresponds to the organizational effort in domain engineering that was identified in the interview study. As for the organizational effort in application engineering, it is hard to depict it based on the survey responses since the practitioners focus mostly on the effort for new common safety artifacts e.g., safety requirements or safety architecture. Hence, we do not have reliable data from the survey for the organizational effort in application engineering.

When investigating the effort on the core asset base in the safety perspective, the survey respondents defined the common safety artifacts that they are developing in their domain.
Moreover, they indicated which common artifacts require the highest effort which means that reusing in domain engineering is very challenging and developing also specific parts for them requires high effort. Moreover, they also evaluated which ones require the lowest effort. Therefore, $C_{\text{cab}}$, $C_{\text{reuse}} (D)$ and $C_{\text{unique}} (D)$ are all used in the same context as in the interview study.

All six industrial experts answered the questions about common artifacts that they are reusing in their product line generations. Safety analysis, hardware analysis and software analysis are among the artifacts that being reused at a high extent while PHAs, FMEAs and FMECAs are barely being reused. Furthermore, only two responses are recorded for unique development. However, the respondents who answered regarding the unique parts they are developing in their domains, added also that they put specific effort on functional safety for such parts. Such effort can be specific documentation and specific FMEAs. Therefore, $C_{\text{reuse}} (A)$ and $C_{\text{unique}} (A)$ have been identified in the survey study in the very same context as in the interviews.

In the part on evolutorial effort, two respondents evaluated the effort in the same context as the interviewees did in study 1. Hence, they identified products they added to their product lines when evolving to new generations as well as the safety effort spent on integrating such new products e.g., the new product may need higher SIL level than the rest of the product line. The problem with the other four respondents is that they do not identify any case in their industrial context when they add new products and still, they write about the extra functional safety effort they put on such new products that seem to be inexistent judging by their answers. Hence, the answers of these four respondents are controversial if we see evolutionary effort in the context that it was used in the interview study. The similarity level for the answers given by these four respondents is definitely 1 (completely different from the evolutorial effort context in study 1). However, the similarity level with the other 2 respondents is 5. Moreover, the four respondents who answered differently may have misunderstood the question. Therefore, we estimate the overall similarity level for the evolutorial effort to be 3.

Finally, the information for maintenance is very vague as it was the case in the interview study. The reason for that is that none of the interviewees or respondents is directly involved in maintenance activities. However, the contexts of use for maintenance effort are similar in both cases although we cannot state they are very similar (level “5”) since we do not have a detailed overview of general and safety maintenance activities in the interview study so we can compare them with the ones that were identified seldom in the survey responses.

The evaluation of similarities between the identified costs related to safety in different studies is important because it shows that same cost areas were identified in the interview study, survey study and documentation analysis. There is very high similarity (level “5”) for most of the cost areas. There are only three cost areas with similarity levels “0”, “3” and “4” and such levels were evaluated mostly because the information extracted from the survey responses is either very vague or is totally missing in these perspectives: organizational effort for application engineering, evolutional effort and maintenance effort.
Discussion

8.3.1 Identifying Functional Safety Effort

In the three studies, we could identify several cost components that contribute significantly in the overall cost attributed to functional safety in industrial product lines. The cost parts related to functional safety effort are defined as follows:

1. $C_{org} (D)$ – The organizational cost for domain engineering. This represents the effort put from the organizational side in order to adapt the core of product line depending on changes that might come e.g., a new standard may be introduced, higher SIL levels may be required and so on. For this purpose, training activities for the big scope of the product line may be held, expert groups may be created and so on.

2. $C_{org} (A)$ – The organizational cost for application engineering. This represents the effort put from the organizational side in order to adapt or develop specific applications within the a product line or project depending on changes that might come e.g., a new standard may be introduced, higher SIL levels may be required and so on. For this purpose, training activities for the safety scope of the specific application(s) may be held, expert groups may be created and so on.

3. $C_{cab}$ – The core asset base cost for domain engineering. This represents the effort put for developing common safety artifacts and applying common safety mechanisms when developing a safety-critical product line or adapting it depending on changes (e.g., common new safety requirements are needed for increasing the safety level).

4. $C_{reuse} (D)$ – The reuse cost for domain engineering. This represents the effort on integrating safety artifacts reused from previous generation(s) and project(s) in the core asset of the new product line generation. For example, most of the common safety tests are available for a certain product line generation because they are reused from the previous generation.

5. $C_{reuse} (A)$ – The reuse cost for application engineering. This represents the effort on integrating safety artifacts reused from the common artifacts of the current generation. For example, there are some commonalities related to safety concepts for the product line generation, in general. However, different product line members reuse separately some of these safety concepts and some additional ones are applied for each member.

6. $C_{unique} (D)$ – The unique cost for domain engineering. This represents the effort on developing new common safety artifacts when changing to a new product line generation or a new project. For example, more common safety components can be added for the new product line architecture in order to increase safety for the new generation.

7. $C_{unique} (A)$ – The unique cost for application engineering. This represents the safety effort on developing specific applications and specific parts of the product line generation i.e., instead of just reusing from safety common artifacts of the product line generation. For example, there might be product line members in the new generation of a product line that require different safety argumentation compared to the one provided for the rest of the generation.
8. $C_{evo}$ – The evolutional cost. This represents in general the effort put on safety when evolving to a new product line generation. When passing to new generations, new products and applications might be added and the specific safety effort put on them is represented by $C_{evo}$.

9. $C_{maintenance}$ – The maintenance cost. This represents the effort put on maintenance activities involving functional safety. For example, repairing as well as monitoring safety functions contributes in the maintenance cost.

Based on what each of the cost factors above represent, it is accurate to present the following relation as relevant:

$$C_{cab} = C_{reuse} (D) + C_{unique} (D)$$  \hspace{1cm} (30)

Indeed, the common safety artifacts in a product line generation are either reused from past experience (past generations or projects) or newly developed.

On the other hand, the functional safety effort on a specific product line member or application can be seen as the sum of the effort put on reusing and integrating from the common safety artifacts and the effort on new safety integration or assessment (e.g., specific safety argumentation) for that member or application.

$$C_{APP} = C_{reuse} (A) + C_{unique} (A)$$  \hspace{1cm} (31)

8.3.2 Challenges for Functional Safety Effort Estimation

Big challenges were presented when investigating functional safety effort in our empirical study. The literature study showed that no existing software product line economic model can be used or adapted for estimating functional safety effort in industrial product lines. For this reason, we performed three studies.

In the first study, none of the seven interviewees could provide accurate information related to the functional safety effort estimation in Volvo CE product lines. The semi-structured interviews and questions that aimed to investigate safety effort were refined many times by talking to practitioners. In the first preliminary versions of the interview questionnaire (appendix A), there were questions asking directly for functional safety effort estimation. For example, there were questions asking the practitioners to estimate the level of reusing safety requirements from 0 to 100%. After testing these questions with different practitioners, all of them stated that it is not possible to give a value for that estimation. Therefore, estimating the functional safety effort based on industrial expert judgment was not possible in the first study performed for Volvo CE product lines.

The biggest problem we have faced after performing the studies and analyzing the results have probably been the fact of not receiving many answers from study 2. As in study 1, we tried to ask the practitioners in the preliminary versions of the survey directly for effort estimation on functional safety. The result was the same. None of the practitioners was able to define the effort which means that the possibility to provide expert-based effort estimations on functional safety can be excluded in this case, as well.
Estimating functional safety effort in product lines is not less challenging in the third study either. Analyzing the effort spent on documentation is very hard to evaluate and thus, extracting functional safety effort is not feasible also here because the effort has not been documented and reported properly.

8.3.3 Possible Solution and Improvements for Functional Safety Effort Estimation in Industry

None of the three studies and neither the literature study can currently give an answer to the issue of providing functional safety effort estimations for industrial product lines.

A common problem for the situations identified in the interview study, survey and documentation analysis is actually the lack of historical data which is crucial for estimating the effort on functional safety. For example, if we take the example of Machine project 1 in the interview study which is utilizing services from the platform project, estimating the functional safety effort for Machine project 1 is challenging because there is no historical data for the functional safety effort put on the platform project. The documentation analysis on the platform project confirms this, too. If the effort put on functional safety for the platform project would be documented properly, then future estimations of such effort would be facilitated significantly. As an example, an interesting effort perspective to be documented would be the effort spent on developing common safety architecture parts. This would require keeping track of time that was spent on the task, number of people who participated, sources that were used and so on. Estimating this effort would derive an input for the overall core asset base effort on the functional safety for the platform.

Besides increasing the effort on providing more accurate historical data for future estimations on safety, a possible solution would also be to introduce an estimation approach which would combine formal cost-modeling techniques and expert-based estimation methods. Cost functions and cost estimations for different scenarios may be derived from existing cost models. However, the inputs for such functions can be estimated based on expert-judgement such as talking to practitioners that deal with industrial product lines or analyzing the right documentation. We illustrate this view in the guidelines we propose in chapter 9 for future estimations of functional safety effort in product lines.

8.4 Validation

An important aspect regarding the results obtained by performing the three studies has to do with their overall quality and the validation of results. We rely on the guidelines provided by Yin in [20] for validating our findings. Validation of results from empirical studies is considered in four different perspectives: construct validity, internal validity, external validity and reliability.

8.4.1 Construct Validity

Construct validity has to do with validation during the phase when data is collected from the studies [20]. Three methods are used for construct validity:

1. Multiple sources are used for collecting information in order to provide more evidence and avoid subjective interpretations of data as much as possible.
2. A chain of evidence is built by different sources of data in order to provide more support for it.
3. The preliminary report which summarizes the findings from the studies is reviewed by people who actually provided the information while performing the studies.

In our context, we relied on such methods because:

1. A multiple-study was performed which included data gathered from the interview study, survey and documentation analysis.
2. A chain of evidence was built by collecting information from the three studies. Moreover, we interviewed practitioners of different profiles and fields of expertise at Volvo CE. Therefore, evidence and common findings were identified in different semi-structured interviews and thus, we aimed to avoid subjective interpretations that might lead to not reliable conclusions and results.
3. The structure of the interview study as well as that of the survey were tested several times with practitioners at Volvo CE in order to make sure that the questions are understandable for practitioners and it is feasible to ask in that direction for effort estimation on functional safety in industrial product lines.

8.4.2 Internal Validity
Internal validity represents the validation process that is needed while analyzing the data collected from the studies [20]. The most used method for the internal validity of study results consists in comparing the patterns based on empirical findings with the one that were predicted from logic models and so on before proceeding with the analysis of the study data.

An example in our own study would be the fact that the interview structure as well as the survey structure were previously highly influenced by the cost areas depicted in existing cost models for product lines, mostly in SIMPLE model. As we investigated such efforts in our empirical study, we can conclude that this pattern of decomposing the total cost for functional safety in the six areas above is resulted to be relevant and thus, it matched the pattern that was predicted from the literature.

Another method for internal validity includes using rival points of view for explaining the same situation or problem.

In our study, such method was also applied since seven practitioners were interviewed and six respondents answered the survey and their points of view on different perspectives were analyzed.

8.4.3 External Validity
External validity consists in performing a multiple study in order to provide more support and stronger evidence for the derived results compared to the situation when a single study is performed and the results are then generalized based on only one source of information [20].

In our context, we conducted three different studies. If we refer to our example regarding the identification of six different cost parts which was mentioned for the internal validity as well,
then we can state that it was possible to identify such parts in all three studies. Therefore, generalizing this finding is supported by our multiple-study design.

8.4.4 Reliability
Reliability consists in redoing the study usually by another researcher and verifying if same results are obtained [20].

Many factors can affect the results obtained from our study. The results depend also on the domains that are involved in the study or the practitioners who answered and so on. An example would regard the investigation done on maintenance effort for functional safety. In our case, no maintenance expert was interviewed. If the study is redone and such expert becomes part of it, then more accurate results can be drawn on safety maintenance effort.

8.4.5 Limitations
Despite having three different studies, there are certain limitations that make validation more challenging in our context. These limitations include the following:

1. Study 1: No more than seven practitioners were interviewed at Volvo CE.
2. Study 2: Only six responses were gathered from the survey study.
3. Study 3: Not all documentation has been analyzed.

All these limitations are related to the quantitative perspective. Having a higher number of different sources for information to analyze in each study would certainly increase the reliability and accuracy of results.

However, we focused on avoiding misinterpretations of gathered data by reviewing it several times and checking with industrial experts and thus, making sure that the derived results are accurate and feasible despite the fact of not having many answers and considerable information from the studies.
9. Proposal for a New Approach

Based on the analysis performed in chapter 8, it is possible to provide some guidelines and directions on how to introduce an estimation approach that considers functional safety effort in industrial product lines. Since neither product line cost models or current expert-based estimation methods can estimate functional safety effort in industry, these guidelines represent an important step in this perspective.

In order to propose a complete estimation approach, sufficient argumentation needs to be added and provided for supporting it further. Regardless, we present some starting points in this perspective and the purpose is to extend the approach in the future by performing a more in-depth analysis to support it.

In the first subsection of this chapter, a preliminary view is presented regarding the combined approach. At first, we start with decomposing the overall safety cost in several areas. Furthermore, different scenarios in industrial product lines are investigated in terms of safety effort estimation. In addition, we provide guidelines on how to estimate the value for each safety cost by documenting properly the effort in different safety-related activities in industry.

As we concluded from our empirical study, the focus on documenting such efforts is currently missing in industry.

We also provide an overview of interdependencies between different safety-related costs which shows the impact that a safety cost increase has on the other safety costs. This analysis is derived from the findings and results on safety costs in studies 1 and 3 that were explained in subsection 8.

Finally, we summarize possible improvements that should be considered to translate our guidelines into an actual approach for estimating functional safety effort industrial product lines.

9.1 Towards a New Combined Estimation Approach

A convenient future estimation approach would be a combination of expert-estimation techniques and formal cost-modeling techniques. The high level design of the proposed combined approach is presented in figure 28.
The structure of the cost-modeling part is inspired by the structure of existing cost models that include investment analysis such as InCoMe, Schmid’s and Withey’s models. This part would deal with formulas for estimating the effort. The lowest layer includes the safety cost areas which are summarized in subsection 9.1.1. In the scenario layer, several formulas that combine different safety cost areas are utilized for effort estimation on different safety-related scenarios in industrial product lines. We provide some example of such scenarios and the respective safety effort estimations for each of them in subsection 9.1.2. Finally, an analysis takes place by evaluating and comparing the safety effort in different industrial situations.

Expert estimations can be performed by using the historical data on documented efforts on functional safety. In subsection 9.1.3, we provide guidelines on how to document the effort on different activities in order to have later some historical data that can be used to estimate the input values for the safety cost areas which are utilized for safety effort estimations in different scenarios.

9.1.1 Safety Cost Areas
Figure 29 gives an overview of each cost component that contributes in the overall safety-related cost (SC\text{tot}).
The safety cost functions that will be used for safety effort estimations in the new approach correspond to the nine safety cost components identified in the analysis in chapter 8:

- $SC_{org}(D)$ – Organizational safety-related effort in domain engineering
- $SC_{org}(A)$ – Organizational safety-related effort in application engineering
- $SC_{cab}(D)$ – Core asset base safety-related effort
- $SC_{reuse}(D)$ – Reuse safety-related effort in domain engineering
- $SC_{reuse}(A)$ – Reuse safety-related effort in application engineering
- $SC_{unique}(D)$ – Unique safety-related effort in domain engineering
- $SC_{unique}(A)$ – Unique safety-related effort in application engineering
- $SC_{evo}$ – Evolutional safety-related effort
- $SC_{maintenance}$ – Maintenance safety-related effort

Since each of the safety cost functions contribute in the overall safety effort estimation, the general formula for safety effort estimation would be the following one:

$$SC_{tot} = SC_{org} + SC_{cab} + \sum_{p=1}^{n} (SC_{reuse}(A)p + SC_{unique}(A)p) + SC_{evo} + SC_{maintenance} \quad (32)$$

Since $SC_{org} = SC_{org}(D) + SC_{org}(A)$ and $SC_{cab} = SC_{reuse}(D) + SC_{unique}(D)$, then the above relation can be reformulated:

$$SC_{tot} = SC_{org}(D) + SC_{org}(A) + SC_{reuse}(D) + SC_{unique}(D) + \sum_{p=1}^{n} (SC_{reuse}(A)p + SC_{unique}(A)p) + SC_{evo} + SC_{maintenance} \quad (33)$$

Depending on how many safety-critical products and applications are included in the product line, the sum of all the efforts put on safety integration when reusing safety artifacts from the core asset ($SC_{reuse}(A)p$) as well as the sum of all efforts on specific safety application for each product ($SC_{unique}(A)p$) are considered to contribute in the total safety-related cost when
applying functional safety in a product line. \( \text{SC}_{\text{reuse}} (A)p \) and \( \text{SC}_{\text{unique}} (A)p \) are designations that represent respectively the safety-related effort of reusing artifacts from the core asset in one product line member and developing specific parts that belong only to that product line member.

However, the above relations may often be not suitable to be applied in several industrial contexts. For this purpose, it is necessary to evaluate different industrial scenarios and provide specific safety effort calculations for each of them. Different scenarios and effort estimations for each of them are presented in section 9.1.2.

9.1.2 Directions for Industrial Safety-Related Scenarios

Depending on the industrial scenario, the overall effort estimation attributed to safety may rely on different cost components. We have identified several safety-related scenarios in our study. Examples of such scenarios are:

1. Addressing functional safety in product lines for the first time
2. Introducing new safety standards during the process
3. Adding maintenance that consider functional safety in product lines
4. Adding new products that require safety assessment
5. Merging different product lines into a single product line

In reality, there are significantly more scenarios that need to be considered when evaluating functional safety in industry.

The next step for the future estimation approach would be to provide effort estimations for each identified scenario. In order to illustrate this, examples of how the effort is estimated for scenarios 1 and 2 are presented in the following paragraphs. Apart from considering more scenarios and providing effort estimations for each of them, the estimation approach would require also to test such estimations in industrial domains that apply functional safety and refine the formulas further. However, we provide some directions here on how to start evaluating different scenarios and their respective efforts on functional safety.

Scenario 1: Functional safety assessment in product lines

The first scenario is about applying functional safety in a product line where there was no previous safety assessment. Hence, the organization has to put significant effort on developing new safety content (applying safety standards, creating safety documentation and so on) in both domain engineering (developing common safety content) and application engineering (tailoring safety artifacts and mechanisms for different products and applications within the product line). For these reasons, the safety effort estimation will be as following:

\[
\text{SC}_{\text{tot}} = \text{SC}_{\text{org}} (D) + \text{SC}_{\text{org}} (A) + \text{SC}_{\text{cab}} + \sum_{p=1}^{N} (\text{SC}_{\text{reuse}} (A)p + \text{SC}_{\text{unique}} (A)p)
\]

Since there has been no application of functional safety in this product line in the past, then it means that \( \text{SC}_{\text{reuse}} (D) = 0 \). Therefore, \( \text{SC}_{\text{cab}} = \text{SC}_{\text{unique}} (D) \) and the safety effort relation above is reformulated:
Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study

\[ SC_{\text{tot}} = SC_{\text{org}}(D) + SC_{\text{org}}(A) + SC_{\text{unique}}(D) + \sum_{p=1}^{n} (SC_{\text{reuse}}(A)p + SC_{\text{unique}}(A)p) \]  

(35)

**Sub-scenario 1.1: Functional safety assessment in common product line artifacts**

There is the case when it is decided to apply functional safety in the common artifacts of an industrial product line. In other words, the organization wants to develop the common artifacts according to functional safety standard(s). It is implied that there was no safety assessment for such artifacts in the past. Therefore, both organizational and core asset base efforts contribute in the overall cost in this scenario.

Such scenario is identified in the first scenario of issue 4 in chapter 5 where no safety assessment has been considered so far for common engine components and the effort put on addressing safety in such components would certainly pay off by reusing later safety artifacts and mechanisms for all the engine parts.

The overall effort for addressing safety in the common artifacts of a product line would be:

\[ SC_{\text{tot}} = SC_{\text{org}}(D) + SC_{\text{cab}} = SC_{\text{org}}(D) + SC_{\text{reuse}}(D) + SC_{\text{unique}}(D) \]  

(36)

In case when there was no safety assessment reused from previous generations or previous projects (and this is the case for scenario 1 since we assumed that there was no safety assessment in the past), then it is feasible to define that \( SC_{\text{reuse}}(D) = 0 \). Therefore, the overall safety cost would be:

\[ SC_{\text{tot}} = SC_{\text{org}}(D) + SC_{\text{cab}} = SC_{\text{org}}(D) + SC_{\text{unique}}(D) \]  

(37)

Therefore, the effort in scenario 1.1 consists on the organizational cost spent for analyzing how to apply functional safety in the common artifacts (training activities or even expert groups can be created for this purpose) and on the safety artifacts and mechanisms developed from scratch (application of safety standard parts for the common artifacts, new safety concepts, safety goals, new safety architecture, new safety documentation and so on).

**Sub-scenario 1.1.1: Benefits of developing common safety artifacts**

If the effort on developing common functional safety artifacts is compared to the effort that would be spent in the situation when functional safety is addressed specifically and separately in each product (i.e., specific solution for each product), then we would obtain the economical benefits (or losses) that are gained by developing common safety artifacts.

\[ SC_{\text{common}} = SC_{\text{org}}(D) + SC_{\text{cab}} = SC_{\text{org}}(D) + SC_{\text{reuse}}(D) + SC_{\text{unique}}(D) \]  

(38)

\[ SC_{\text{separate}} = SC_{\text{org}}(A) + \sum_{p=1}^{n} (SC_{\text{reuse}}(A)p + SC_{\text{unique}}(A)p) \]  

(39)

Economical benefits = \( SC_{\text{separate}} \) when \( SC_{\text{separate}} > SC_{\text{common}} \)  

(40)

Losses = \( SC_{\text{separate}} \) when \( SC_{\text{separate}} < SC_{\text{common}} \)  

(41)
Formula (38) estimates the effort for investing in common functional safety artifacts which requires the organization to adapt and put effort to develop such new artifacts. Since common safety artifacts are developed, then there is also an increase on the core asset base safety effort.

Regarding the effort on addressing functional safety separately in each product instead of building a core asset base for functional safety, it is calculated by the effort that the organization puts on the application level i.e., addressing safety for each product and application. For each product, the effort of developing specific safety artifacts is added as well as the effort on reusing and integrating safety artifacts.

**Sub-scenario 1.2: Functional safety assessment in unique products**

Another special case of scenario 1 is when there are unique products (or specific parts) in a product line that are still lacking functional safety assessment. On the other hand, functional safety has been applied in the developed common artifacts of the product line. In order to apply functional safety in the unique products (parts), the organization has to reuse safety artifacts (e.g., safety concepts, safety plans or parts from risk assessment techniques) from the core asset of the product line and develop new safety artifacts for the unique products (parts) as well. For example, a unique product may require a higher SIL level than the rest of the product line members and hence, it needs more safety argumentation (extra safety effort).

The safety effort estimation for scenario 1.2:

\[
SC_{tot} = SC_{org}(A) + \sum_{p=1}^{n} (SC_{reuse}(A)p + SC_{unique}(A)p)
\]  

(42)

Since functional safety will be applied for specific products, the effort put on each product is different. For this reason, the effort on developing specific safety artifacts as well as reusing common ones is estimated for each of the unique products. In addition, the organization spends effort for each application and this, \(SC_{org}(A)\) is added to formula (42).

**Scenario 2: Introduction of new safety standards**

Situations when industrial experts need to deal with new functional safety standards and start applying them in their product lines are nowadays being quite common in industry. The effort for this scenario is estimated as follows:

\[
SC_{tot} = SC_{org}(D) + SC_{cab} + \sum_{p=1}^{n} (SC_{reuse}(A)p + SC_{unique}(A)p) + SC_{evo}
\]  

(43)

As an example, the introduction of ISO26262 and the effort on investigating this new standard was pointed out in study 1. The introduction of new safety standards represents safety evolution in an industrial domain and the organization must spent effort on training activities and expert groups for investigating and analyzing the new standard(s) in order to check how it can be applied as efficiently as possible in their industrial context.
9.1.3 Guidelines on estimating input values for safety cost areas

The next step is to provide guidelines on how practitioners and industrial experts need to document each safety-related effort in product lines in order to provide historical data for future estimations of functional safety effort in industry.

I - Guidelines on how to estimate $SC_{org}(D)$:

1. Document the effort put on each training activity that is related to functional safety application in the domain engineering phase. Every parameter such as number of people, time spent and other resources used for such activities must be documented.
2. Document the effort put on creating group experts when there is a change or situation that regards the safety critical aspects in industrial product lines.
3. Document the effort put on changing the structure of the organization, rearrangement or existing department, creation of new departments and so on. Such changes are supposed to be done in order to adapt the organization to a new product line situation e.g., applying functional safety in a product line for the first time or increasing the SIL levels for some product lines.

II - Guidelines on how to estimate $SC_{org}(A)$:

1. Document the effort put on each training activity that is related with addressing functional safety in specific applications or product line members. Every parameter such as number of people, time spent and other resources used for such activities must be documented.
2. Document the effort put on creating group experts when there is a change or situation that regards functional safety in specific applications or product line members.
3. Document the effort put on changing the structure of the organization, rearrangement or existing department, creation of new departments and so on. Such changes are supposed to be done in order to adapt the organization to a new safety-related situation e.g., applying functional safety in a specific product or increasing the SIL levels for specific parts of the product line.

III - Guidelines on how to estimate $SC_{cab}$:

1. Document the effort on analyzing functional safety commonalities and variability in a product line e.g., common safety concepts, common safety requirements.
2. Document the effort put on defining and developing common safety artifacts: common safety concepts, common safety requirements, common safety architecture, common safety components, common safety mechanisms, common safety tests, common PHAs, FMEAs and so on.
3. When creating or refining common safety documentation that is intended for all product line members (common safety plans, risk assessment documentation and so on), carefully document the effort put on it.

4. *An alternative way to estimate $SC_{cab}$ is to first estimate $SC_{reuse}(D)$ and $SC_{unique}(D)$ separately and then, calculating $SC_{cab}$ as the sum of these two safety-related cost functions.
Guidelines on how to estimate $SC_{\text{reuse}}$ (D) and $SC_{\text{unique}}$ (D) separately are provided in the successive paragraphs.

**IV - Guidelines on how to estimate $SC_{\text{reuse}}$ (D):**

1. Document the effort on analyzing functional safety commonalities and variability in a product line e.g., common safety concepts, common safety requirements.
   1.1. Define if there are parts of the commonality-variability analysis which are reused from the analysis performed in past projects or previous product line generations.
   1.2. In case that there are such parts, define and document the effort on adapting such parts of the analysis in the new context (time, people and sources spent for making the changes in the analysis).
2. Document the effort put on defining and developing common safety artifacts: common safety concepts, common safety requirements, common safety architecture, common safety components, common safety mechanisms, common safety tests, common PHAs, FMEAs and so on.
   2.1. Define if there are parts in each of these common artifacts that are being reused from previous generations or past projects.
   2.2. In case that there are such parts, define and document the effort on adapting and integrating reused parts of the common safety artifacts and mechanisms in the new product line generation.
3. When creating or refining common safety documentation that is intended for all product line members (common safety plans, risk assessment documentation and so on), carefully document the effort put on it.
   3.1. Define if there are parts of safety documentation that are being reused from past projects or product line generations.
   3.2. In case that there are such parts, define and document the effort put on changing and refining the reused parts of safety documentation.

**V - Guidelines on how to estimate $SC_{\text{unique}}$ (D):**

1. Document the effort on analyzing functional safety commonalities and variability in a product line e.g., common safety concepts, common safety requirements.
   1.1. Define if there are parts of the commonality-variability analysis that are new parts in the performed analysis which are not reused from past analysis in previous generations.
   1.2. In case that there are such parts, define and document the effort on the new analysis parts (time, people and sources spent for performing the new analysis).
2. Document the effort put on defining and developing common safety artifacts: common safety concepts, common safety requirements, common safety architecture, common safety components, common safety mechanisms, common safety tests, common PHAs, FMEAs and so on.
   2.1. Define if there are parts in each of these common artifacts that are being developed as new content instead of being reused from previous generations or projects.
2.2. In case that there are such parts, define and document the effort on developing and integrating new content.

3. When creating or refining common safety documentation that is intended for all product line members (common safety plans, risk assessment documentation and so on), carefully document the effort put on it.

3.1. Define if there are parts of safety documentation that are being developed as new content for the current generation instead of being reused from past projects or product line generations.

3.2. In case that there are such parts, define and document the effort put on developing and creating new safety documentation parts.

**VI - Guidelines on how to estimate SC\text{reuse} (A):**

1. Identify all the safety artifacts that are being reused for different product line members from the common safety artifacts of the product line e.g., common safety concepts, common safety architecture, common safety mechanisms, common safety tests and so on.

   1.1. Define and document the integration efforts on reusing and tailoring each of the common safety artifacts in different product line members.

2. Identify all safety documentation that is being reused from the common safety documentation of the product line and tailored for different application of the product line. Such safety documentation includes safety plans, safety standards, PHAs, FMEAs and so on).

   2.1. Define and document the effort on changing and tailoring common safety documentation in the context of different product line applications.

**VII - Guidelines on how to estimate SC\text{unique} (A):**

1. Identify all the safety artifacts that are developed specifically for unique parts or applications within the product line instead of being reused from the common safety artifacts of the product line. Specific safety artifacts developed for unique parts or applications can be new safety concepts, new safety architecture parts, specific safety mechanisms, specific safety tests and so on.

   1.1. Define and document the effort on developing each specific safety artifact.

2. Identify all the specific safety documentation that is created as new documentation for specific parts or applications within the product line instead of reusing from the common safety documentation in the core asset of the product line. Specific safety documentation includes specific parts of safety plans, applying specific parts from safety standards, specific PHA parts, FMEA parts and so on).

   2.1. Define and document the effort on creating specific safety documentation for unique parts or applications in the product line.

**VIII - Guidelines on how to estimate SC\text{evo}:**

1. Identify all the products or applications that have been added when evolving to a new product line generation.
1. Define and document the extra functional safety effort put on the added new products or applications. Such effort can be for example performing extra PHAs or FMEAs, applying new parts of a standard, achieving higher SIL levels and so on.

2. Identify cases when new safety requirements are added for specific product line members or for the whole product line in general.
   2.1. Define and document the effort spent (people, time, resources) in order to adapt to new changes and fulfil the new safety requirements.

3. Identify cases when new safety standards are introduced.
   3.1. Define and document the effort spent (people, time, resources) in order to adapt to new changes and comply with the new safety standards.

IX - Guidelines on how to estimate $S_{\text{maintenance}}$

1. Identify all maintenance activities that are affecting functional safety. For example, safety maintenance activities can include: the work performed on making sure that it is being complied with functional safety standards, keeping standards and safety functions up to date, safety testing, checking for hazards that have not been captured during the PHA and so on.
   1.1. Define and document the effort on each maintenance activity that affects functional safety in product lines.

9.2 Safety Cost Interdependencies

We generalize here findings on the interdependencies between different safety cost areas based on the analysis performed on such dependencies in the context of the issues and proposed improvements in subsection 8.1. The most common situation identified from the analysis in subsections 5.3 and 8.1 regards the case when higher effort is put on the organizational side and in general, on developing and improving the common safety artifacts ($S_{\text{org}}(D)$ and $S_{\text{cab}}$ increase) and this extra effort is expected to be followed by the decrease of most of the left safety cost components. This would actually mean that investing and increasing the effort on $S_{\text{org}}(D)$ and $S_{\text{cab}}$ would finally pay off.

In table 32, we summarize all the dependencies by considering every case when each of the safety cost components increases (each component listed in the first column of the table) and checking the impact that this cost increase has on the other safety cost components (listed on the first row of the table).
Table 32: Identified cost dependencies based on the analysis of findings from studies 1 and 3

<table>
<thead>
<tr>
<th>Safety Cost Dependencies</th>
<th>SC&lt;sub&gt;org&lt;/sub&gt; (D)</th>
<th>SC&lt;sub&gt;org&lt;/sub&gt; (A)</th>
<th>SC&lt;sub&gt;cab&lt;/sub&gt;</th>
<th>SC&lt;sub&gt;reuse&lt;/sub&gt; (D)</th>
<th>SC&lt;sub&gt;reuse&lt;/sub&gt; (A)</th>
<th>SC&lt;sub&gt;unique&lt;/sub&gt; (D)</th>
<th>SC&lt;sub&gt;unique&lt;/sub&gt; (A)</th>
<th>SC&lt;sub&gt;evo&lt;/sub&gt;</th>
<th>SC&lt;sub&gt;maintenance&lt;/sub&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC&lt;sub&gt;org&lt;/sub&gt; (D)</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;org&lt;/sub&gt; (A)</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑</td>
<td>↓</td>
<td>↑↑</td>
<td>↑↑</td>
<td>↑↑</td>
<td>↑↑</td>
</tr>
<tr>
<td>SC&lt;sub&gt;cab&lt;/sub&gt;</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↑</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;reuse&lt;/sub&gt; (D)</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↑↑</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;reuse&lt;/sub&gt; (A)</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;unique&lt;/sub&gt; (D)</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↓</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;unique&lt;/sub&gt; (A)</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↓↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;evo&lt;/sub&gt;</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↑</td>
<td>↓</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↓</td>
</tr>
<tr>
<td>SC&lt;sub&gt;maintenance&lt;/sub&gt;</td>
<td>↑↑</td>
<td>↓↓</td>
<td>↑↑</td>
<td>↑</td>
<td>↓</td>
<td>↑↓</td>
<td>↓↓</td>
<td>↓↓</td>
<td>↑</td>
</tr>
</tbody>
</table>

A typical case when SC<sub>org</sub> (D) is increased and the other safety costs are affected is shown in the areas for improvement for issue 3 in the interview study. Indeed, if the organization increases the safety effort in domain engineering, there would be less effort on safety assessment for each product or each application (SC<sub>org</sub> (A) decreases). An example of increasing SC<sub>org</sub> (D) would be to apply safety standards when developing common components or apply functional safety concepts or risk assessment techniques in a common platform or common framework that incorporates different products and product lines. In the same time, this means that SC<sub>cab</sub> increases as well since higher effort is put on developing the common safety artifacts. The main purpose on doing that is to decrease as much as possible the efforts on specific safety assessment in different products or parts of the product line as well as to decrease safety integration efforts when reusing from common safety artifacts (e.g., facilitate PHA reuse in different product line members) or when adding new products that need safety assessment (e.g., a new product is added and some of the safety requirements are different from those available for the rest of the product line). Increasing the effort on common safety artifacts and mitigating extra safety effort on specific applications is expected to facilitate safety maintenance. Since SC<sub>cab</sub> = SC<sub>reuse</sub> (D) + SC<sub>reuse</sub> (A) and since SC<sub>cab</sub> increases significantly in this case, it is hard to define if SC<sub>reuse</sub> (D) or SC<sub>reuse</sub> (A) will either increase or decrease. That depends on the fact if high efforts will be put mostly on integrating (reusing) common safety artifacts from previous generations or developing new common artifacts in the current generation. What we can state is that when SC<sub>cab</sub> increases, either both SC<sub>reuse</sub> (D)
and $SC_{\text{reuse}}(A)$ or at least one of them will be increased. Since it is not always certain if each of them will increase, we use the designation “↑↓” for them in table 32.

In the second case, we have the situation when $SC_{\text{org}}(A)$ is increased. We cannot find any such situation in the cases we evaluated in our studies. However, having a high organizational effort in application engineering implies that the organizational structures are spending specific effort for addressing safety problems in each of their applications and different product line members. Hence, there is no high effort on trying to define all the commonalities between different applications and hence, save some safety effort by developing less specific safety artifacts ($SC_{\text{org}}(D)$ and $SC_{\text{cab}}$ are not high). $SC_{\text{reuse}}(D)$ and $SC_{\text{unique}}(D)$ are also decreased since no effort is spent on increasing $SC_{\text{cab}}$, i.e., reusing more common safety artifacts or developing new safety content and integrate it in the common artifacts. Specific safety effort on each application is translated in higher unique effort and less reuse of safety artifacts (e.g., specific safety documentation effort for each application or product). However, integration efforts are higher when reusing safety artifacts between applications. Finally, evolutional and maintenance efforts are significantly higher since different safety artifacts (e.g., different safety concepts) need to be considered in both of them.

In the third case, $SC_{\text{cab}}$ is increased. This represents probably the most common situation out of the ones we identified in our studies. Examples we can refer to include the areas for improvements for issues 1 and 2 in study 1. An increase in $SC_{\text{cab}}$ means also that the organization should increase the effort on developing and integrating new safety content. Hence, $SC_{\text{org}}(D)$, $SC_{\text{reuse}}(D)$ and $SC_{\text{unique}}(D)$ are increased. The purpose of doing so is to decrease the effort put on addressing safety problems specifically for each product line member. Therefore, $SC_{\text{org}}(A)$, $SC_{\text{unique}}(A)$, $SC_{\text{evo}}$ and $SC_{\text{maintenance}}$ are expected to decrease. However, there are few differences and inconsistencies between these general conclusions on cost dependences and the situations explained in the studies.

Regarding safety reuse and unique efforts, they are directly related to $SC_{\text{cab}}$. In domain engineering, $SC_{\text{cab}} = SC_{\text{reuse}}(D) + SC_{\text{unique}}(D)$. As for application engineering, when $SC_{\text{cab}}$ is increased, it is expected to pay off by increasing reuse from common safety artifacts (integration effort in $SC_{\text{reuse}}(A)$ slightly increases) and hence, reduce unique or specific safety effort ($SC_{\text{unique}}(A)$ decreases significantly). That is why most of the other safety cost impacts are similar as in the case when $SC_{\text{cab}}$ is increased. In cases when $SC_{\text{cab}}$ goes through a decrease (e.g., when $SC_{\text{unique}}(A)$ increases), then the safety cost impacts should reverse e.g., $SC_{\text{evo}}$ will increase (instead of decreasing when the organization puts higher effort on the common safety artifacts).

Finally, the safety cost impacts when $SC_{\text{evo}}$ and $SC_{\text{maintenance}}$ are increased are illustrated in the areas for improvement for issues 5 and 6 in the interview study. We generalize these impacts in the last two rows of table 32. Increasing the effort on safety evolution (e.g., when applying new standards or when integration new products with higher SIL levels in the product line) and safety maintenance (e.g., for capturing possible defects and hazards in product line applications) facilitates the effort on applying safety in each application and reduces integration efforts. This decreases the following safety costs: $SC_{\text{org}}(A)$, $SC_{\text{unique}}(A)$ and $SC_{\text{reuse}}$
(A). As a consequence, this also requires an increase (a slight increase in some cases) in the overall effort for developing common artifacts (in domain engineering).

9.3 Areas for improvement and future consideration

The scenarios and safety cost calculations presented above are thought to serve as useful guidelines on how to propose a functional safety-related cost model for industrial product lines. Typical safety-related scenarios were evaluated based in our study but more scenarios can be added for providing further argumentation. In addition to that, an investment analysis approach as the one in InCoMe or in the cost models proposed by Withey and Schmid can enrich the new approach.

It should be also taken into consideration that only short-term changes (e.g., the scenarios listed above or the ones identified in the studies) are taken into account when evaluating product line safety effort. Meanwhile, the safety effort is also affected to a high extent by long-term changes such as non-economical decisions on keeping different solutions for the same problem and so on. Long-term changes were observed occasionally while performing study 1. However, the impact of such changes is very complex to consider and include in a cost-modeling approach.
10. Summary and Conclusions

In this chapter, we summarize the essentials of our work as well as present the main conclusions. In subsection 10.1, a summary of what has been presented in this thesis report is provided. Conclusions derived from evidence and findings that are analyzed in our study, are presented in subsection 10.2.

10.1 Summary

In this master thesis work, we performed an empirical study in order to investigate cost and efforts in industrial product lines when developing safety critical products. For this purpose and in order to provide enough argumentation for the evidence and derived results, we relied on a triple study (interview study, survey study and documentation analysis).

In study 1, we performed semi-structured interviews with industrial experts. The interview structure was organized by findings and preliminary conclusions that were previously extracted from the literature study. Ten established product line cost models were selected from related work and previous publications as models with higher potential for fitting our context: effort estimation in industrial product lines with focus on functional safety. However, no proposed cost model in the literature did consider functional safety. This was the main motivation for interviewing industrial experts since the functional safety effort could not be investigated through methods proposed in literature. Different cost areas were identified in the interview study as potential effort factors that contribute directly in the overall industrial effort attributed to applying functional safety in Volvo CE product lines. Challenges were faced while using the interview study information for producing safety-related results in the cost perspective. For example, there was no considerable information related to safety maintenance mostly because of the fact that none of the seven interviewees was involved directly in industrial product line maintenance at Volvo CE. However, it was possible to produce some general effort-related results indirectly from the available feedback received in this perspective.

Studies 2 (survey study) and 3 (documentation analysis) were performed to provide more data as evidence and also argumentation for our analysis and results. Only six respondents could provide information related to situations how they are applying and dealing with functional safety in their domains and working environments. Such few number of respondents can be explained by the fact that knowledge and industrial expertise on functional safety needs probably more time to build and experts and practitioners still feel that there are much uncertainty when functional safety aspects and their application in specific domains is discussed.

Nevertheless, a high level of similarity was observed between the results regarding safety cost areas from studies 1, 2 and 3. We analyzed and identified nine different cost components that contribute in the overall safety effort in industrial product lines. In addition, guidelines were provided for documenting the right efforts in order to have some basis for future safety effort estimations and provide input values for the identified safety cost components.
According to the work we performed, neither the literature study nor the empirical study resulted to be sufficient for providing effort estimations on functional safety in industry. Hence, we foresee a combination of both methods to be the best choice to address this problem in the future.

10.2 Conclusions

Regarding the research questions we formulated in chapter 1, it can be stated that we have answered them while performing, analyzing and evaluating our empirical study.

In RQ1, we formulate the problem of identifying existing literature study and related work that considers cost-modeling approaches for industrial product lines. The answer for RQ1 and its sub-questions rely on our own literature study we performed and presented in chapter 4 of this thesis report. We summarize ten product line cost models based on the literature study (RQ1.1). Each cost model has advantages and disadvantages for making effort estimations in a product line. These advantages and disadvantages are summarized in the last section of subchapter 4.1. In this section, we also identify seven proposed cost models that have been applied in industry (RQ1.2). Two of these cost models are the ones proposed by Schmid and Withey. Their strongest point regards the investment analysis approach which is very detailed and takes into account several industrial risks and situations.

Poulin's model is also applied in practice. However, this model is used more for software estimation in the code perspective. Analyzing the effort in product lines involves more complex estimations.

Other cost models that have been applied in practice are SIMPLE and InCoMe. In fact, their structure and the costs and effort identified in these two cost models were used as guidance and inspiration for proceeding with our three studies (interview, survey and documentation). After evaluating the safety-related effort and costs in industrial product lines in our three studies, we can state that the cost components identified in SIMPLE and InCoMe were proved in general to be relevant even for estimating safety-related effort in industrial product lines. However, we extended the cost calculations proposed in SIMPLE and InCoMe in order to fit better to the safety industrial-scenarios we identified and evaluated in our study.

The results from study 2 revealed that two domains are applying COCOMO II and COPLIMO. However, no information is provided on how they are dealing with the application of these cost models or what parts of the cost models they are actually applying.

Finally, we can answer RQ1.3 by concluding that we could not find any product line cost model in the literature study that considers functional safety.

As for the RQ2 and its sub-questions, we answer them through our analysis of the findings and results derived from the interview study, survey study and documentation analysis.

RQ2.1 is about investigating possible cost factors that contribute in the overall functional safety effort in product lines. In our analysis, we identified the following nine cost components that affect the overall effort attributed to safety aspects and activities in industrial product
lines: organizational safety-related cost in domain engineering, organizational safety-related cost in application engineering, core asset base safety-related cost, reuse safety-related cost in domain engineering, reuse safety-related cost in application engineering, unique safety-related cost in domain engineering, unique safety-related cost in application engineering, evolutional safety-related cost and maintenance safety-related cost. There are interdependencies between the nine safety-related cost areas. Changing one of them can affect most of the other safety-related costs. This needs to be considered in different industrial safety-related scenarios. Moreover, guidelines on how to estimate these cost factors are provided in subsection 9.1.3.

However, there are challenges for answering RQ2 and RQ2.2. RQ2 aims to investigate efforts related to functional safety in product lines while RQ2.2 aims to investigate efforts related to safety-related activities. These two research questions cannot be answered by the results of the literature study since none of the proposed models considers functional safety. In addition, we cannot provide an accurate answer for the two questions by relying on the empirical study either. The reason for that is that practitioners and industrial experts cannot provide estimations on functional safety effort. This conclusion was derived by analyzing both the interview and survey results. Moreover, evaluating the effort spent on documentation is also very challenging because the effort for functional safety is not well documented.

Because of such consistent challenges faced while investigating functional safety effort in product lines, we propose that the best way to overcome them is to start documenting the effort properly and thus, provide some basis for future effort estimations. Improving the work on documenting functional safety efforts in several industrial activities will increase the amount of historical data which is currently missing. The existence of more historical data in the future will facilitate the task of deriving the effort attributed to functional safety aspects.
11. Future Work

After analyzing the results from our study, we presented directions for introducing a new combined estimation approach that considers functional safety in industrial product lines. The approach relies on expert-based methods which provide estimations for the input values for the safety cost areas that are used by the cost-modeling technique to perform effort estimations. We evaluated different scenarios identified in industrial domains that apply functional safety in their products. An interesting orientation for future work would be to provide enough argumentation and a more detailed analysis that would be sufficient for extending the directions we propose into a proper approach for estimating functional safety effort.

In addition, more safety-related industrial scenarios can be added to the ones we listed and evaluated in the cost perspective in chapter 9.

This study has also high potential to be improved in the future by enriching it with more data and industrial findings from different types of domains. For example, gathering more responses from the survey study would definitely contribute on making the results of our analysis more accurate and suitable for a wide range of domains. Probably, more safety cost areas can be identified as well.

Furthermore, a safety-related cost area that needs further investigation in the future is the safety maintenance effort. We were able to generalize some findings and results on some limited information about maintenance effort that was collected from three of the semi-structured interviews. However, more accurate results related to safety maintenance effort can be derived by talking to experts involved directly in safety maintenance activities.
References


Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study


Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study


Appendix A: Interview Questionnaire

The following abbreviations are used in the questionnaire:

- Qx (e.g., Q1, Q2 and so on) = Question x
- SQx.y (e.g., SQ1.1, SQ1.2 and so on) = Subquestion x.y which is a subquestion of Qx.

A.1 General Questions

A.1.1 Q1: What is your current position in the company?
Rationale: With this question, some information about the current role of the interviewee in the company shall be collected. This question helps to put answers in the right context.

A.1.1.1 SQ1.1: What does that role involve?
Rationale: Companies might define the responsibilities of a role differently. More detailed information what the interviewed person is working with is helpful to get a common view.

A.1.2 Q2: Which of your work tasks are related to functional safety? Please describe them.
Rationale: In case that the interviewee has experiences with functional safety, the single tasks should be listed and described shortly.

A.1.3 Q3: Which of your work tasks are related to product line development? Please describe them.
Rationale: Similar to question Q2, this question is aiming for evaluating the interviewee's experience about product line development.

A.1.4 Q4: What is your company's domain?
Rationale: Depending on the company's domain, different development processes are common and different functional safety standards are relevant. Most likely this will lead to a different implementation of the product line concept and accordingly different challenges and best practices are identifiable.

A.2 Scenarios

A.2.1 Q5: What has changed since the last generation of the product line?
Rationale: This question aims to compare the current product line generation with the previous one. The changes that the generation has gone through might be of technical background, process-related, safety-related and so on.
A.2.2  Q6: What has been done to adapt to the new generation?
  
  **Rationale:** This question aims to investigate the effort that has been put into the process of adapting to the new generation.

A.2.2.1  **SQ6.1 What were the main challenges for it?**
  
  **Rationale:** It is intended to get an overview of the main issues that the process of going from one generation to another one has faced.

A.2.2.2  **SQ6.2 What has been done to overcome the challenges?**
  
  **Rationale:** This question aims to investigate the effort for solving the issues that are discussed in the previous question.

A.2.2.3  **SQ6.3 How well did it work it out?**
  
  **Rationale:** This question aims to investigate the level of success that characterizes the solutions given to the main issues and challenges discussed in the previous questions.

A.3  Cost of Organization

A.3.1  Cost of Organization (in the industrial context)

It implies the cost needed for an organization to adapt the product line approach for its products. This cost may include:

- Reorganization
- Process improvement
- Training
- Other necessary organizational remedies

Cost for organization (Ideas):

- Reorganizing because of new product line
- Training of employees
  - Process
  - Tools
  - Methods
  - Standards
- Domain Engineering
  - Number of Developers needed for developing core assets
  - Number of testers
  - New tool introduced-extra effort is put on adapting the organization

A.3.1.1  **PRACTICAL ISSUES**

Practically, everything is adapted to the product line approach at Volvo.

A.3.2  Q7: How did the change from one project to another one affect the organization?
  
  **Rationale:** This question aims to investigate the effort that has been put into the process of adapting to the new project e.g., the wheel loader application project.
Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study

**Expected Answer:** More people involved, time spent, training employees, new technology, new tools etc.

A.3.3 Q8: Which training activities have been considered so far in the company? What is needed to be done more in this area? Please, provide examples.

**Rationale:** This question aims to investigate the training activities that have taken place in order to educate several employees on the new context e.g., training for FMEAs.

**Expected Answer:** Training activities for new technologies, tools and techniques.

A.3.3.1 SQ8.1 Can you estimate the organizational effort for these activities?

**Rationale:** This questions aims to investigate the effort put on training activities e.g., education for FMEAs.

**Expected Answer:** People involved, time spent.

A.3.4 Q9: Has there been cases when the scope of a product line has been changed? Please provide examples.

**Rationale:** This question aims to investigate cases when the scope of the product line changes. For example, the company may decide to pass from a product family of cars to one with a higher level of safety.

**Expected Answer:**
- Yes/No
- Given examples regarding scope change of product line.

A.3.4.1 SQ9.1: If yes, which impact did this change have on the organization?

**Rationale:** This is related to question 13. It aims to investigate the effects of the product line scope change on the organization.

**Expected Answer:** Impacts on the organization e.g., the need to have more people involved in the process, internal reorganization issues and so on.

A.3.5 Q10: If new technologies are introduced, which impact does this have on the organizational efforts?

**Rationale:** This question aims to investigate organizational efforts in case when there are changes such as new technologies being introduced.

**Expected Answer:** Examples of what should change in the organizational aspect when new technologies are introduced. For example, more people should be involved in the process or a certain number of employees need to be trained for the new technology.

A.3.6 Q11: Have new functional safety standards been introduced? If yes, which organizational efforts did this implicate? Please provide examples.

**Rationale:** This question aims to investigate the way how introducing functional safety standards during the process can affect the organizational cost.

**Expected Answer:**
• Yes/No
• Effect of introducing the new functional safety standards on the organization
• Examples e.g., department rearrangement, role redistribution.

A.4 Cost of Core Asset Base

A.4.1 Cost of Core Asset Base (in the industrial context)
It implies the cost needed for developing a core asset base for a suitable scope. It can include
the cost of performing a commonality/variability analysis; defining the product line scope;
designing and evaluating a generic software architecture; developing the software so
designed; building production plan; establishing development environment; producing a
testing architecture; producing other artifacts that are reusable across the family. It can also
include plans, budgets, schedules, scope definition and other documentation. It can also
include the artifacts that tell you how to produce products from core assets e.g., production
plan.

A.4.1.1 PRACTICAL ISSUES
Practitioners may not be familiar with the term “core asset base”!

A.4.2 Q12: How did changing from one project to another affect the core with the common artifacts?
Rationale: This question aims to get an understanding of the reuse level.

Expected Answer: Artifacts that have been reused from previous projects and artifacts
developed from scratch specifically for the project (wheel loader application project).

A.4.2.1 SQ12.1: What has been reused in the safety aspect?
Rationale: This is related to question 12. It aims to get an understanding of the
safety reuse.

Expected Answer: Safety artifacts reused from previous generations.

A.4.2.2 SQ12.2: What was the effort put on adapting the reused safety artifacts in the new project?
Rationale: This is related to question 12. It aims to investigate the effort spent
on using and adapting some of the existing artifacts in the new environment.

Expected Answer: People involved, time, resources and so on.

A.4.2.3 SQ12.3: Did you succeed with the effort that you put there?
Rationale: This is related to question 12. It aims to investigate if reusing certain
parts did actually pay off.

Expected Answer: Analysis of the effort put on reuse and results of the work.

A.4.3 Q13: What is generally the effort spent on the guidelines that serve for indicating how to use
common core assets in order to develop the products?
Rationale: This question aims to investigate the effort related to guiding the
application projects in using the core assets.

Expected Answer:
Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study

- What guidelines are created and for which parts?
- How well did it work out? Was the description in the guidelines sufficient?
- How should it be applied to achieve functional safety?

A.4.4 Q14: Can you think of other documentation that is needed before releasing the products? Can you give an estimation of the effort (cost) that is needed for it (them)?

Rationale: This question aims to investigate the cost related to other documents that should be included in the core asset base.

Expected Answer:

- Yes/No
- Other documentation that is not mentioned in the previous questions.
- Example: Safety documentation, Documentation Reviews and so on.
- Effort (number of people and working hours) spent on this documentation.

A.5 Cost of Unique Parts

A.5.1 Cost of Unique Parts (in the industrial context)

It implies the cost needed for developing unique parts that are not included in the core asset base. The result can either be a complete unique product that is not part of a product line or a unique part of a product that has its other parts built in the core asset base of a product line.

A.5.1.1 PRACTICAL ISSUES

We should not expect to deal with single unique products at Volvo! Everything is expected to be based in product lines! What about unique parts of a product? (This can be related to some commonality/variability analysis since it also tries to investigate which are the unique (variable) parts of each single product.

A.5.2 Q15: Are you applying parts that are unique for a specific product in the product line? If yes, could you name some?

Rationale: This question aims to identify the specific parts for certain products that belong to the same product line.

Expected Answer:

- Yes/No
- Defining some unique parts
- Examples given (maybe with some details) regarding these unique parts.

A.5.3 Q16: Has there been such unique parts in the past?

Rationale: This question aims to investigate if these specific parts were already existent.

Expected Answer:
- Yes/No

**A.5.3.1 SQ16.1: What was specific about them and what was needed to be done?**  
**Rationale:** This is related to question 16. It aims to investigate some details regarding the unique parts in the past and the process of changing them to their current state.

**Expected Answer:**
- Details regarding specific parts and their role
- The effort needed to be done for them
- What has been done in the functional safety aspect?

**A.5.4 Q17:** Can you give an estimation of the cost needed for developing the unique parts mentioned in the previous question?  
**Rationale:** This question aims to investigate the cost of unique parts that are present in products which belong to the same product line.

**Expected Answer:**
- Number of people and working hours (days) needed for developing this specific parts (e.g., specific safety components, specific tests and so on.

**A.5.5 Q18:** What is happening to those unique parts in the next generation of the product line? Do you see a trend that they become part of the core assets and have reuse potential?  
**Rationale:** This question aims to investigate if the unique parts will be include in the core asset for the next generation and thus be reused later.

**Expected Answer:**
- Explaining the trend of using the unique parts in the next generation

**A.6 Cost of Reuse**

**A.6.1 Cost of Reuse (in the industrial context)**  
It implies the cost needed to build a product by reusing core assets from a core asset base.

**A.6.1.1 PRACTICAL ISSUES**  
What artifacts can be reused in the industrial context?

**A.6.2 Q19:** How did changing from one generation to another affect reuse? What has been reused from the previous generation?  
**Rationale:** This question aims to get an understanding of the reuse level.

**Expected Answer:**
- Artifacts that has been reused from previous generation.

**A.6.2.1 SQ19.1: What the effort for adapting the reused artifacts to the new generation?**  
**Rationale:** This question aims to get an understanding of the effort spent on reusing existing artifacts.
Expected Answer:

- Effort spent on adapting reused artifacts

**SQ19.2: What has been reused in the safety aspect?**

**Rationale:** This question aims to get an understanding of the safety reuse.

**Expected Answer:**

- Safety artifacts that have been reused from previous generations e.g., Hazard analysis, safety requirements, FMEAs and so on.

**SQ19.3: What was the effort put on adapting the reused safety artifacts in the new generation?**

**Rationale:** This is related to the previous question. It aims to investigate the effort spent on using and adapting some of the existing artifacts in the new environment.

**Expected Answer:** People involved, time, resources and so on.

**Q20:** Please, rate to which extent you are reusing each of the following artifacts.

**Rationale:** This question aims to get an understanding of the reuse level (a quantifiable value) of different kinds of artifacts.

**Expected Answer:**

- Reuse level (in percentage value where 0% means no reuse while 100% means full reuse) of each artifact.
A.6.4  Q21: Please, rate to which extent you are reusing each of the following safety artifacts.

**Rationale:** This question aims to get an understanding of the reuse level (a quantifiable value) of different kinds of safety artifacts.

**Expected Answer:**

- Reuse level (in percentage value where 0% means no reuse while 100% means full reuse) of each safety artifact.
**Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study**

A.6.5 **Q22**: In case when you are having requirement changes, how does this influence safety aspects?

**Rationale**: This question aims to get an understanding of the impact that requirements changes might have on several functional safety aspects. For example, some architecture parts that have been already implemented, might need to be changed.

**Expected Answer**: Cases when functional safety aspects are affected when requirements change.

A.6.5.1 **SQ22.1**: Can you estimate the extra effort put on functional safety aspects in case when you face situations when requirements change?

**Rationale**: This is related to the previous question. It aims to investigate the effort spent on functional safety when requirements change.

**Expected Answer**: Extra effort put on functional safety (more people involved, more resources spent etc.).
A.6.6  Q23: Judging by your experience, what are the general challenges for reusing each of the artifacts mentioned in the previous questions?

**Rationale:** Reusing artifacts often facilitates things in industry. However, it is not easy sometimes because reusing some artifacts implies also to adapt these artifacts in a new environment and this may require some professional experience.

**Expected Answer:**

- Identifying issues that usually rise when trying to reuse the artifacts listed in the previous questions.

A.6.6.1  SQ23.1: What was been done to overcome these challenges?

**Rationale:** This is related to the previous question. It aims to investigate the effort spent on solving the issues and challenges that appear when trying to adapt the reused artifacts in a new environment.

**Expected Answer:** Evaluate the effort (involved people, time spent, internal changes) required for making these artifacts suitable for a new purpose i.e., for reusing them.

A.6.7  Cost of Reuse in the Functional Safety context

A.6.7.1  Q24: Do you use any risk assessment technique when you develop a product? Can you please provide some details regarding the risk assessment technique(s) that you use?

**Rationale:** This questions aims to investigate the type of risk assessment techniques that are used in the industrial environment.

**Expected Answer:**

- Yes/No
- Identifying which risk assessment techniques (e.g., Hazard Analysis, FMEAs etc.) are used when developing product lines at Volvo.

A.6.7.2  Q25: Please, rate to which extent are you reusing each of the risk assessment techniques shown below.

**Rationale:** Reusing risk assessment artifacts (which are safety artifacts) is common in industry. However, it is worthy to know to which extent is each technique being reused.

**Expected Answer:** Reuse level (percentage value 0-100%) of each risk assessment technique.
A.6.7.2.1 SQ25.1: Can you estimate the effort put on adapting the reused risk assessment technique parts in a new project or environment?

**Rationale:** This is related to the previous question. It aims to investigate the effort spent on adapting the reused risk assessment techniques for a new project, new product line or a new generation. This can include integration effort on safety argumentation and so on.

**Expected Answer:** Effort expressed in man-hours, resources, time spent on research and so on.

A.6.7.3 Q26: Do you reuse some concepts or documentation related to safety standards? Can you provide some illustration?

**Rationale:** Some concepts and safety documentation can be reused in order to prove that a system part is safe.

**Expected Answer:**
- Yes/No
- Details provided for the safety documentation that is being reused.
- Example: Some parts of the ISO 26262 may be reused for each product line.

A.7 Evolution Cost

A.7.1 Evolution Cost (in the industrial context)
It implies the cost of producing a new version of the product. The asset base needs also to be updated in order to adapt to the new version.
A.7.1.1 **PRACTICAL ISSUES**

What does evolution mean in the practical sense? Can it be considered as maintenance activity?

**A.7.2** Q27: How do functional safety issues change while going to a new generation? What is the effort needed for adapting new changes related to functional safety? Please provide some details.

**Rationale:** This question aims to investigate how functional safety is affected by evolution and what is the cost associated only to the safety part while evolving from one generation to another.

**Expected Answer:**
- Examples on how functional safety aspects change through evolution e.g., new functional requirements are added.
- The effort for adapting these functional safety changes.

**A.7.3** Q28: What is the cost needed for adding products to the product line?

**Rationale:** This question is aiming for a practical estimation related to the situations when there are product changes in the product line.

**Expected Answer:**
- Identifying cases or scenarios when new products are added.
- Evaluating if this change require more effort i.e., more people involved in the process or more time and also if it causes some internal changes in the organization.

**A.8 Maintenance Cost**

**A.8.1** Maintenance Cost (in the industrial context)

It implies the cost related to all maintenance activities that are needed for maintaining the PL.

**A.8.2** Q29: What is done during maintenance from your perspective?

**Rationale:** This question is aiming to receive a specific answer depending on the professional profile of the interviewee and his/her role in maintenance.

**Expected Answer:**
- Naming maintenance activities and processes where the interviewee is involved.

**A.8.3** Q30: Which maintenance activities are related to functional safety? What is the effort required for such activities?

**Rationale:** This question is aiming to filter the maintenance activities that regard functional safety aspects and tries to get an overview of the effort spent on them

**Expected Answer:**
- Naming maintenance activities related to functional safety
- Explaining the effort for such activities
Hello! This survey aims to investigate the cost and effort needed for developing safety-critical products in product lines. Answering the survey takes about 15-20 minutes depending on how much feedback you want to give. Thanks a lot in advance for your support! Please, feel free to contact us: stephan.baumgart@mdh.se dpa12001@student.mdh.se Best regards, Stephan Baumgart and Ditmar Parmeza.

1. Please, define the country and the organization where you are currently working.

   *(a) Country: ____________________________ ____________________________

   *(b) Organization: ____________________________ ____________________________

2. What is the domain of your company?

   [ ] Automotive  [ ] Avionics  [ ] Healthcare

   [ ] Railway  [ ] Aerospace

   [ ] Other (please specify) ____________________________

3. What is the size of your company? (Select one option)

   [ ] Small ( < 100 employees)  [ ] Medium (100-1000 employees)  [ ] Big (>1000 employees)
4. What is your current position in the company? (Select one option)

- Manager
- Software Architect
- Software Developer
- Hardware Developer
- Safety Engineer
- Safety Manager
- Test Developer
- Maintenance
- Other (please specify) __________

5. Is your role in the company related to functional safety? If yes, please explain it briefly.

- Yes
- No

If yes, please specify. ______________

6. How would you rate your exposure to functional safety aspects? (Select one option)

- Not at all
- To little extent
- To some extent
- To a moderate extent
- To a large extent
7. How many years of experience do you have on working in industry and working with functional safety issues?

* (a) Industry:

________________________________________________________________________________

* (b) Functional Safety:

________________________________________________________________________________

8. What functional safety standards are you using in your company?

☐ ISO26262  ☐ IEC61508  ☐ ISO15998

☐ ISO25119  ☐ IEC62061  ☐ ISO13849

☐ Other (please specify) ____________

9. Which risk assessment techniques are you currently using?

☐ PHA  ☐ FMEA  ☐ FMECA

☐ Other (please specify) ____________

10. What standard for lifecycle processes are you using?

☐ CMMI  ☐ Automotive SPICE (ISO/IEC 15504)

☐ SPICE (ISO/IEC 12207)  ☐ None

☐ Other (please specify) ____________
11. Are you applying any cost model in your industrial domain?

- COCOMO II
- InCoMe
- None
- SIMPLE
- Coplimo
- Other (please specify) ____________

12. How many product variants are you currently managing?

* (a) Number of Variants:
____________________________________________________________________
____________________________________________________________________

13. How often are you having releases of new generations (e.g., once a year, twice a month etc.)?

____________________________________________________________________
____________________________________________________________________

14. How many generations have you been involved in?

____________________________________________________________________
____________________________________________________________________
15. What has typically changed from one generation to another one, in your case? Please, choose one or some of the alternatives below or define another one.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed Platform</td>
<td>Merging different product lines into one</td>
<td>Passing from unique parts in a previous generation to common artifacts in a new one</td>
</tr>
<tr>
<td>Modified/Improved Platform</td>
<td>Adding new products to the product line</td>
<td>Implementing in Software (Passing from Hardware to Software)</td>
</tr>
<tr>
<td>Introduction of a new technology</td>
<td>New tools are used</td>
<td>Higher SIL-levels</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16. How is the organization affected in your case when changing to a new project or a new generation of the product line?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No change</td>
<td>Training activities are held (big scope)</td>
<td>Changes in several departments</td>
</tr>
<tr>
<td>Training activities are held (small scope)</td>
<td>New expert groups are created</td>
<td>Complete reorganization (new departments/new management)</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17. When creating a new product generation in your case, which of the following changes related to functional safety have the highest impact on the organization?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>New safety requirements are introduced.</td>
<td>Safety tests need to be partially or completely changed.</td>
<td>New safety standards are used for the new project.</td>
</tr>
<tr>
<td>Safety architecture parts need to be changed.</td>
<td>New risk assessment techniques such as hazard analysis, FMEAs etc. have to be used for the new project.</td>
<td>Safety documentation should be extended.</td>
</tr>
<tr>
<td>Safety components need to be partially or completely changed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
18. For the change(s) you chose from the previous question, which of the following organizational impact did it (they) have?

- No change
- Training activities are held (big scope).
- New expert groups are created.
- Changes in several departments
- Complete reorganization (new departments/new management)
- Other (please specify) ______________

19. What kind of common artifacts do you use for your product lines?

- Hardware Components
- Software Components
- Communication Links and Protocols
- Common Architecture
- Common Tests/Generic Testing Framework
- Tools
- Interfaces for Common Components
- A common set of functions
- Other (please specify) ______________
20. Common Development Artifacts: Which of the following lifecycle phases require the highest effort for developing and integrating new content, in your case?

☐ Safety Concept  ☐ Software Analysis  ☐ Safety Argumentation

☐ Safety Analysis  ☐ System Analysis  ☐ Maintenance

☐ Hardware Analysis  ☐ Qualification

☐ Other (please specify) __________

21. Common Development Artifacts: Which of the following lifecycle phases require the lowest effort for developing and integrating new content, in your case?

☐ Safety Concept  ☐ Software Analysis  ☐ Safety Argumentation

☐ Safety Analysis  ☐ System Analysis  ☐ Maintenance

☐ Hardware Analysis  ☐ Qualification

☐ Other (please specify) __________

* 22. Are you applying any unique parts in some products in your product line? If yes, please specify which parts.

☐ Yes  ☐ No  ☐ I don’t know

☐ If yes, please specify which parts. __________
### 23. Which of the following requires the highest effort for the unique part(s) that you are applying?.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A specific PHA is performed</td>
<td>Specific parts of a safety standard are applied</td>
</tr>
<tr>
<td>A specific FMEA is performed</td>
<td>A new safety standard is applied</td>
</tr>
<tr>
<td>A specific FMECA is performed</td>
<td>Specific safety documentation is kept for the specific parts</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>________________</td>
</tr>
</tbody>
</table>

### 24. Do you foresee a trend for reusing these unique parts in the future? If yes, could you briefly explain why it is so beneficial to reuse them in the future?

<table>
<thead>
<tr>
<th>Option</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Please, explain the benefits in terms of future reuse. ________________</td>
<td></td>
</tr>
</tbody>
</table>

### 25. What parts are you reusing at a larger extent from the common development artifacts?

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Concept</td>
<td>Software Analysis</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>System Analysis</td>
</tr>
<tr>
<td>Hardware Analysis</td>
<td>Qualification</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>________________</td>
</tr>
</tbody>
</table>

---

Cost and Efforts in Product Lines for Developing Safety Critical Products – An Empirical Study
26. Where is the highest integration effort when reusing from the common development artifacts?

- [ ] Safety Concept
- [ ] Software Analysis
- [ ] Safety Argumentation
- [ ] Safety Analysis
- [ ] System Analysis
- [ ] Maintenance
- [ ] Hardware Analysis
- [ ] Qualification
- [ ] Other (please specify) ______________

27. Are you reusing any documentation related to a specific risk assessment technique? If yes, please rate the extent to which you are reusing them.

(a) PHA documentation (Select one option)

- [ ] Not at all
- [ ] To a low extent
- [ ] To a moderate extent
- [ ] To a large extent
- [ ] Full reuse

(b) FMEA documentation (Select one option)

- [ ] Not at all
- [ ] To a low extent
- [ ] To a moderate extent
- [ ] To a large extent
- [ ] Full reuse

(c) FMECA documentation (Select one option)

- [ ] Not at all
- [ ] To a low extent
28. Please, feel free to add any comment related to the previous three questions.

____________________________________________________________________

____________________________________________________________________

29. Has there been a case where a new product was added to an existing product line? Please, describe it shortly.

____________________________________________________________________

____________________________________________________________________

30. Which of the following requires the highest effort for a product that is added to an existing product line?

- [ ] A specific PHA is performed
- [ ] A specific FMEA is performed
- [ ] A specific FMECA is performed
- [ ] Specific parts of a safety standard are applied
- [ ] Specific safety documentation is kept for the specific parts
- [ ] A new safety standard is applied
- [ ] There is no extra effort related to functional safety
- [ ] Other (please specify) ________

31. Which of the following activities requires in general the highest effort when you maintain your product lines?

- [ ] Software Maintenance
- [ ] Inspection
- [ ] Repair of some parts of the products
32. Which of the following activities requires the highest effort for functional safety when you maintain your product lines?

- [ ] Software Maintenance
- [ ] Hardware Maintenance
- [ ] Safety Maintenance
- [ ] Inspection
- [ ] Repair of some parts of the products
- [ ] Testing
- [ ] Replacement of some parts of the products
- [ ] Other (please specify) ______________

33. Please, feel free to add any comment related to the survey:

____________________________________________________________________
____________________________________________________________________

THANK YOU! You have successfully completed this survey! Thank you for helping us by providing your feedback and useful information! Stephan Baumgart and Ditmar Parmeza. stephan.baumgart@mdh.se dpa12001@student.mdh.se