Mälardalen University Licentiate Thesis 379

Towards An Improved β-factor Estimation for Safety-Critical Railway Systems

Sirisha Bai Govardhan Rao

Mälardalen University

Mälardalen University Press Licentiate Theses
No. 379

TOWARDS AN IMPROVED β-FACTOR ESTIMATION FOR SAFETY-CRITICAL RAILWAY SYSTEMS

Sirisha Bai Govardhan Rao

2026

Department of Computer Science & Engineering

ISBN 978-91-7485-745-0
ISSN 1651-9256
Printed by E-Print AB, Stockholm, Sweden

“To my dear family”

Abstract

Industries rely on a variety of safety-critical systems, such as signaling systems in railways and fire protection systems in nuclear plants. These systems perform safety functions to protect against undesired and harmful events. Therefore, the failure or malfunction of these systems has serious consequences, including loss of life, environmental damage, and property destruction. Hence, to achieve high reliability of these systems, it is common practice to include redundancy to ensure system functioning despite individual component failure. In particular, Common Cause Failures (CCF) pose a significant threat to these systems as they can cause multiple components to fail simultaneously due to a single underlying root cause. Thus, quantifying CCF is crucial in probabilistic failure analysis, i.e., the evaluation of the likelihood of system failures and their potential consequences in safety-critical industries.

For quantifying CCF, explicit and implicit methods are available. Explicit methods model each failure event in detail, including its possible causes and combinations, to directly represent the dependencies and interactions among the system components. In contrast, implicit methods avoid modeling individual failure events and instead rely on aggregate parameters to account for dependencies among components and their impact on system reliability. These models are advantageous when CCF are not directly observable at the component level, such as those arising from systematic issues related to design, operational practices, or environmental influences, commonly referred to as residual causes. Several implicit models are available, including the α-factor model, which distributes common cause failures among components based on their conditional probabilities, and the Binomial Failure Rate model, which estimates the probability of

multiple component failures using a binomial distribution approach. However, the most widely adopted approach across industries such as nuclear, railway, and process sectors is the β-factor model.

The international functional safety standard, IEC 61508, provides a methodology to estimate the β-factor, applicable in a wide range of safety-critical industries. In this methodology, scores are derived from expert-designed checklist questions, answered based on aspects such as system design, implementation, and operational practices. The scores are aggregated across a relevant, though limited, set of defense measures and mapped to estimate the overall β-factor, representing the fraction of failures caused by common causes. The methodology relies on generic assumptions and is closely tied to the original checklist questions, reflecting the technologies available when the standard was written. Although this enables broad application without requiring detailed CCF data for every system, it often produces conservative estimates, which can lead to unnecessary design features or safety measures that increase system complexity and cost. It also limits practitioners' ability to account for factors from emerging technologies or updated practices that could influence the β-factor accuracy.

This thesis explores how the β-factor estimation methodology outlined in IEC 61508 can be adapted to strengthen its applicability within the railway industry. The work begins by identifying a foundational gap in the literature: the absence of a comprehensive and structured overview of existing β-factor models. A literature review was conducted, identifying 20 distinct models and organizing them to support accurate and efficient application. Building on this foundation, the thesis proposes an extensible β-factor estimation methodology that incorporates a new set of checklist questions and a structured scoring system. This extension improves flexibility, allowing the methodology to better accommodate emerging technologies and evolving safety practices. Furthermore, the applicability of the defense measures of IEC 61508 is critically evaluated using historical safety data from the railway industry. The analysis reveals that operational factors are the primary contributors to CCF, contrasting with the emphasis of the standard on design-focused defenses. These findings underscore the need for industry-specific strategies and support the development of a more context-aware β-factor methodology.

Sammanfattning

Industrier förlitar sig på en mängd olika säkerhetskritiska system, t.ex. signalsystem i järnvägar och brandskyddssystem i kärnkraftverk. Dessa system utför säkerhetsfunktioner för att skydda mot oönskade och skadliga händelser. Därför får fel eller funktionsstörningar i dessa system allvarliga konsekvenser, inklusive förlust av människoliv, miljöskador och förstörelse av egendom. För att uppnå hög tillförlitlighet i dessa system är det därför vanligt att inkludera redundans för att säkerställa att systemet fungerar trots att en enskild komponent går sönder. I synnerhet utgör fel med gemensam orsak (CCF) ett betydande hot mot dessa system eftersom de kan leda till att flera komponenter fallerar samtidigt på grund av en enda underliggande grundorsak. Att kvantifiera CCF är därför avgörande för probabilistisk felanalys, dvs. utvärdering av sannolikheten för systemfel och deras potentiella konsekvenser i säkerhetskritiska industrier.

För att kvantifiera CCF finns explicita och implicita metoder. Explicita metoder modellerar varje felhändelse i detalj, inklusive dess möjliga orsaker och kombinationer, för att direkt representera beroenden och interaktioner mellan systemkomponenterna. Implicita metoder undviker däremot att modellera enskilda felhändelser och förlitar sig istället på aggregerade parametrar för att ta hänsyn till beroenden mellan komponenter och deras inverkan på systemets tillförlitlighet. Dessa modeller är fördelaktiga när CCF inte är direkt observerbara på komponentnivå, t.ex. när de uppstår på grund av systematiska problem relaterade till design, driftspraxis eller miljöpåverkan, vilket ofta kallas kvarstående orsaker. Det finns flera implicita modeller, bland annat -faktormodellen, som fördelar fel med gemensam orsak mellan komponenter baserat på deras villkorliga sannolikheter, och Binomial Failure Rate-modellen,

som uppskattar sannolikheten för fel på flera komponenter med hjälp av en binomialfördelningsmetod. Den mest använda metoden inom branscher som kärnkraft, järnväg och processindustri är dock β-faktormodellen.

Den internationella standarden för funktionell säkerhet, IEC 61508, tillhandahåller en metod för att uppskatta β-faktorn, som är tillämplig inom ett stort antal säkerhetskritiska industrier. I denna metodik härleds poäng från expertutformade checklistefrågor som besvaras utifrån aspekter som systemdesign, implementering och driftspraxis. Poängen aggregeras över en relevant, om än begränsad, uppsättning försvarsåtgärder och kartläggs för att uppskatta den övergripande β-faktorn, som representerar andelen fel som orsakas av gemensamma orsaker. Metoden bygger på generiska antaganden och är nära knuten till de ursprungliga frågorna i checklistan, vilket återspeglar den teknik som fanns tillgänglig när standarden skrevs. Även om detta möjliggör en bred tillämpning utan att kräva detaljerade CCF-data för varje system, ger det ofta konservativa uppskattningar, vilket kan leda till onödiga konstruktionsfunktioner eller säkerhetsåtgärder som ökar systemets komplexitet och kostnad. Det begränsar också utövarnas möjlighet att ta hänsyn till faktorer från nya tekniker eller uppdaterade metoder som kan påverka β-faktorns noggrannhet.

Denna avhandling undersöker hur metoden för uppskattning av β-faktorn som beskrivs i IEC 61508 kan anpassas för att stärka dess tillämplighet inom järnvägsindustrin. Arbetet inleds med att identifiera en grundläggande lucka i litteraturen: avsaknaden av en omfattande och strukturerad översikt över befintliga modeller för β-faktorer. En litteraturgenomgång genomfördes, där 20 olika modeller identifierades och organiserades för att stödja en korrekt och effektiv tillämpning. Baserat på denna grund föreslår avhandlingen en utbyggbar metod för uppskattning av β-faktorer som innehåller en ny uppsättning checklistefrågor och ett strukturerat poängsystem. Denna utvidgning förbättrar flexibiliteten, vilket gör att metoden bättre kan anpassas till ny teknik och nya säkerhetsmetoder. Dessutom utvärderas tillämpligheten av försvarsåtgärderna i IEC 61508 kritiskt med hjälp av historiska säkerhetsdata från järnvägsindustrin. Analysen visar att driftfaktorer är de främsta orsakerna till CCF, vilket står i kontrast till standardens betoning på konstruktionsinriktade skyddsåtgärder. Dessa resultat understryker behovet av branschspecifika strategier och stödjer utvecklingen av en mer kontextmedveten β-faktormetodik.

Acknowledgment

This Licentiate journey would not have been possible without the support of the following individuals. My sincere gratitude goes to my main supervisor, *Sasikumar Punnekkat*, whose direction, stability, and expert oversight guided me through every critical phase. I am immensely grateful to my assistant-supervisor, *Julieth Patricia Castellanos Ardila*, who has been an exceptional source of support throughout the process, always patient, responsive, and collaborative, ensuring my success.

A heartfelt thanks to my mentor, *Anna Holmen*, for her kindness, encouragement, and unwavering support throughout this journey. I am also grateful to my manager, *Natalie Asbrink*, and *Ganesh Chandramouli* for their constant support in managing the administrative aspects that formed the core of my research. My sincere thanks to *Lars Tuvesson* and *Goran Larsendahl* for their expert insights. To my dear friend *Sania Partovian*, and to all my colleagues at IndTech, MDU, and Alstom, thank you for always being friendly and supportive.

I am deeply grateful to my family. First, to my husband, *Govardhan Rao*, for being my pillar of confidence and strength. To my daughters, *Nithilla Bai* and *Komal Bai*, for their endless love and patience. I am also grateful to my parents, brother, in-laws, and all my well-wishers for always wishing me the best.

This work has been funded by the Knowledge Foundation within the framework of the INDTECH (20200132) and INDTECH + (20220132) research school project, participating companies and Mälardalen University.

Sirisha Bai Govardhan Rao
Västerås, January, 2026

List of Publications

The papers included in this thesis[1]

Paper 1: A Systematic Review of β-factor Models in the Quantification of Common Cause Failures, Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila and Sasikumar Punnekkat. In Proceedings of the 49th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Durres, Albania, September, 2023.

Paper 2: A Proposal for Enhancing IEC 61508 Methodology for the β-Factor Estimation, Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila and Sasikumar Punnekkat. In Proceedings of the European Conference on Software Process Improvement (EuroSPI), Munich, Germany, September, 2024.

Paper 3: Evaluation of IEC 61508 Defenses for Common Cause Failures in Railway Industry, Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila and Sasikumar Punnekkat. In Proceedings of the European Conference on Software Process Improvement (EuroSPI), Riga, Latvia, September, 2025.

[1]The included papers reformatted to comply with the thesis layout.

Other Publications - not included in thesis

Paper A: Facilitating β-Factor Estimation for Common Cause Failures of Safety-Related System, Sirisha Bai Govardhan Rao. In the 10th Software Engineering Doctoral Symposium, Pisa, Italy, 2024.

Contents

I Thesis **1**

1 Introduction **3**
1.1 Thesis Outline 7

2 Background **11**
2.1 Safety-Critical Systems 11
2.2 System Reliability 12
2.3 Redundancy 14
2.4 Common Cause Failures (CCF) 15
2.5 Root Causes of CCF 16
2.6 Dependency factors 17
2.7 The β-Factor Approach Proposed by Fleming 18
2.8 The β-Factor Approach Proposed by IEC 61508 19
2.8.1 Defense measures 19
2.9 Illustrative Example 22

3 Research Summary **25**
3.1 Research problem 25
3.2 Research questions 26
3.3 Research Process 28

4 Research Contributions **32**
4.1 Approaches to β-Factor Estimation 32
4.2 A Scalable Method for β-Factor Estimation 35

4.3 Evaluating IEC 61508 Defenses in Railways 40

5 Related Work **44**

6 Conclusions and Future work **46**
6.1 Conclusions 46
6.2 Future Work 47

Bibliography **49**

II Included Papers **55**

7 Paper 1:
A Systematic Review of β-factor Models in the Quantification of Common Cause Failures **57**
7.1 Introduction 57
7.2 Background 58
7.2.1 Redundancy 58
7.2.2 Common Cause Failures 58
7.2.3 IEC 61508 Standard based CCF Quantification 59
7.3 Related Work 59
7.4 Research Method 60
7.4.1 Review Protocol 60
7.4.2 Data Collection 61
7.5 Research Results 62
7.5.1 Evolution and classification of β-factor models (RQ1) 62
7.5.2 Analysis of the Models support (RQ2) 68
7.5.3 Identified Industries and Tools (RQ3) 69
7.6 Discussion 70
7.6.1 Implications for the Industry 70
7.6.2 Implications for Research 71
7.7 Threats to Validity 72
7.8 Conclusion and Future Work 73
Bibliography 74

Bibliography 77

8 Paper 2:
A Proposal for Enhancing
IEC 61508 Methodology for the β- Factor Estimation **81**
8.1 Introduction 83
8.2 Background 84
8.2.1 β-factor estimation 84
8.2.2 Defense measures 85
8.2.3 A β-factor methodology focusing industry's safety culture 87
8.3 Proposed methodology 87
8.3.1 Research Problem 88
8.3.2 Research Artifact 88
8.4 Illustrative Example 96
8.4.1 Identify redundancy 96
8.4.2 Study of Safety culture 96
8.4.3 Fill checklist 96
8.4.4 Assigning scores to checklist answers 96
8.4.5 Assign susceptibility scores 97
8.4.6 Estimate β-factor 97
8.5 Discussion 98
8.5.1 Methodology Insights 98
8.5.2 Correspondence to SPI Manifesto 101
8.6 Conclusion & Future work 101
Bibliography 101

9 Paper 3:
Evaluation of IEC 61508 Defenses for Common Cause Failures in
Railway Industry **104**
9.1 Introduction 106
9.2 Background & Related work 107
9.2.1 β-factor model 107
9.2.2 Defense strategy to mitigate Common Cause Failures . 108
9.2.3 IEC 61508 standard 109
9.2.4 Related work 109

9.3 Methodology 110
9.4 Results 113
9.4.1 Selecting the events 113
9.4.2 Categorizing the events 114
9.4.3 Determine the β-factor estimation 114
9.4.4 Analyze the defenses 117
9.5 Discussion 118
9.5.1 Findings 118
9.5.2 Threats to Validity 119
9.5.3 Correspondence to SPI Manifesto 120
9.6 Conclusion & Future work 120
Bibliography 121

I

Thesis

Chapter 1

Introduction

Industries rely on a wide range of safety-critical systems, such as signaling systems in railways and fire protection systems in nuclear plants, which are designed to perform safety functions that protect against specific undesired and potentially harmful events [1]. The failure or malfunction of such systems can lead to severe consequences, including loss of life [2], environmental damage, and property loss [1]. To manage these risks, industries systematically evaluate potential hazards throughout the entire system life cycle, from concept development to decommissioning using structured methodologies such as Probabilistic Risk Assessment (PRA) [3].

The PRA mainly deals with three objectives, namely: investigating initiators of events, consequences of events, and probabilities of undesirable events. In this context, estimating the likelihood of such events and tracing their root causes is essential. One widely used method for this purpose is Fault Tree Analysis (FTA) [4], a top-down logic diagram that illustrates the relationship between a top-level undesired event and its contributing causes. These causes may be independent failures, arising from unrelated and statistically uncorrelated events, or dependent failures, where the probability of one failure is influenced by another. This thesis focuses on dependent failures, particularly Common Cause Failure (CCF), where multiple components fail simultaneously due to a shared root cause [5]. CCF poses a significant challenge to system reliability, especially in redundant architectures designed to tolerate individual component failures.

To model CCF, two main approaches are used: explicit and implicit [6]. Explicit methods model each CCF as a basic event that can simultaneously impact multiple components. This approach allows for a detailed representation of failure events, their causes, and the dependencies among system elements. In contrast, implicit methods do not model individual failure events directly; instead, they use aggregate parameters, such as joint probabilities or statistical correlations, to account for dependencies and their effects on system reliability [7]. Implicit approaches are particularly valuable when CCF are not directly observable at the component level, often arising from systematic issues in design, operational practices, or environmental factors, collectively referred to as residual causes [8]. Several implicit models exist, including the α-factor model [9], which allocates CCF among components based on conditional probabilities, and the Binomial Failure Rate model [10], which estimates the probability of multiple component failures using a binomial distribution framework. However, the most widely adopted model across industries such as nuclear, railway, and process sectors is the β-factor model.

The β-factor model, introduced in 1974 in the nuclear power industry [11], was developed as a practical approach to modeling CCF in redundant systems of safety-critical industries. The main advantage of the β-factor model is its simplicity [8], which requires only one additional parameter called β. In particular, this model estimates the contribution of CCF by multiplying the total failure rate by a β value. In the absence of empirical data, this β value is typically derived using a checklist-based approach that assesses the effectiveness of implemented defense measures, i.e., control mechanisms that reduce the likelihood of failures. In alignment with this approach, the functional safety standard, IEC 61508 [12], which is applicable to all industries, proposes a qualitative methodology for the estimation of the β-factor. This methodology considers 8 defense measures (i.e., corrective actions taken to prevent the recurrence of similar failures [1]) in the form of 37 checklist questions with pre-defined scores. The responses to the checklist are aggregated into a total score for the calculation of β-factor.

Railway companies, such as Alstom[1], have used the β-factor estimation methodology for years, in accordance with the methodology proposed by IEC 61508. The reason is that railway specific standards, such as EN 50126 [13],

[1]https://www.alstom.com/alstom-sweden

EN 50128 [14], and EN 50129 [15], mandate consideration of CCF but do not prescribe a specific methodology for their quantification. Thus, in this case, the use of β-factor methodology supports in demonstrating compliance with functional safety requirements, especially in systems where CCF can significantly affect reliability. The recognition of IEC 61508 by safety authorities and certification bodies further strengthens its role as a credible and accepted standard to demonstrate safety integrity.

The β-factor estimation methodology proposed by IEC 61508 derives scores from checklist questions designed by experts, which are answered based on the design, implementation, and operational practices of the system. These scores are then aggregated across a defined set of defense measures and mapped to estimate the overall β-factor representing the proportion of failures attributed to common cause. The methodology is based on generic assumptions and is closely tied to the original checklist structure, reflecting the technological context at the time the standard was developed. Although this methodology enables broad applicability without requiring detailed CCF data for each system, it often results in conservative estimates. Such conservatism can lead to additional design features or safety measures, increasing system complexity and cost. Therefore, this thesis aims to adapt the methodology, with the goal of improving its relevance and practical applicability within the context of the railway industry. In this regard, three main limitations have been identified as follows:

1. There is a lack of a structured and comprehensive theoretical foundation for the β-factor model. The current literature is fragmented and unstructured, making it difficult to develop a clear understanding of existing β-factor models and evaluate their applicability. This limitation hinders both practical implementation and methodological innovation.

2. The outdated treatment of technology within the standard limits its applicability to modern systems. Although part 3 of IEC 61508 was updated in 2024 [16], the revision did not extend to the β-factor estimation methodology. Consequently, there is a growing necessity to integrate defense strategies and measures that address emerging technologies such as artificial intelligence (i.e., machine-based intelligence derived from mathematical algorithms and statistical data analysis [17]) and additive

manufacturing (i.e., the process of creating components layer by layer from 3D model data [18]), among others.

3. The generic nature of the defense measures proposed by the IEC 61508 standard, which are designed to be applicable across a wide range of industries, limits their direct applicability to specific domains. In particular, the probability and root causes of CCF can vary significantly between industries due to their distinct operational contexts and safety requirements [1]. As such, industry-specific methodologies are needed that can more accurately address their actual root causes of CCF.

This thesis addresses the identified limitations by proposing practical and methodological solutions.

- First, a literature review was conducted to explore the origin and evolution of the β-factor model. Through this process, 20 β-factor models were identified and subsequently classified based on β-factor estimation methods, applicability in different redundancy configurations, industrial adoption, and available tool support. These insights collectively serve as a valuable resource for deepening understanding of the β-factor model.

- Second, we introduce a generic methodology that is flexible and extensible, allowing practitioners and researchers to incorporate new defense strategies as technologies evolve. The methodology permits to include more questions and calculate additional elements contributing to the CCF that are not currently included in the standard.

- Third, we analyze historical railway safety events to identify the actual root causes of CCF. This analysis finds that most CCF in railways stem from operational issues, whereas IEC 61508 emphasizes design-related causes. This mismatch highlights the need for additional factors to assess CCF more accurately in the railway domain.

Building on these contributions, this thesis achieves its primary objective by providing the foundation for adapting the IEC 61508 β-factor estimation methodology to the specific needs of railway safety-critical systems.

1.1 Thesis Outline

This thesis is organized into two parts. In the first part, we present the following details. In Chapter 2, we present the essential background details. In Chapter 3, we present the summary of overall research. In Chapter 4, we describe the research contributions. In Chapter 5, we present a discussion of related work. In Chapter 6, we discuss the conclusions and future plans. In the second part, we provide an overview of the included publications.

Paper 1: *A Systematic Review of β-factor Models in the Quantification of Common Cause Failures*
Authors: Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila and Sasikumar Punnekkat
Abstract: Safety systems, i.e., systems whose malfunction can result in catastrophic consequences, are usually designed with redundancy in mind to reach high levels of reliability. However, Common Cause Failures (CCF), that is, single failure events affecting multiple components or functions in a system, can threaten the desired reliability. To solve this problem, practitioners must use proven methods, such as those recommended by standards, to support quantification of CCF. In particular, the β-factor model has become the de-facto model since the safety standard IEC 61508 considers it. As such, a standard applies to all industries; practitioners must figure out the industry-specific implementation procedures. In this paper, we conducted a systematic review of the literature to understand how the β-factor model has been used in practice. As a result, we found 20 different models, which are industry/project-specific extensions of the first β-factor model proposed for the nuclear sector. We further classified those models by considering how the β-factor is estimated, and the level of redundancy support. The support of the tools for the models and their industrial use is also outlined. Finally, we present a discussion that covers the implications of our findings. Our study aims at practitioners and researchers interested in using the current β-factor models or evolving new ones for specific project needs.
Contribution: I am the primary driver of the paper and was actively involved in conducting the Systematic Literature Review (SLR), as well as writing and

presenting the paper. The second author supported the development of the methodology and contributed to the writing. Additionally, the second author continuously reviewed and improved the quality of the paper, including verifying the collected SLR data to mitigate inconsistencies in data collection. The third author contributed to the writing and thoroughly reviewed the manuscript. In addition, the author provided valuable and constructive feedback throughout the research process, from beginning to end, which significantly contributed to the refinement and overall development of the paper.

Status: Accepted and presented at the 49th Euromicro Conference on Software Engineering and Advanced Applications (SEAA[2]) 2023, which has been published in the IEEE Xplore digital library [19].

Paper 2: *A Proposal for Enhancing IEC 61508 Methodology for the β-Factor Estimation*
Authors: Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila and Sasikumar Punnekkat
Abstract: The standard IEC 61508 provides a methodology to calculate β, a factor used to estimate the probability of common cause failures (CCF), i.e., failures that result from a single cause. This methodology consists of answering 37 checklist questions, each one providing a scored value that is accumulated in the final β-factor. Those questions cover 8 different defense measures, i.e., practices done to mitigate the CCF against system dependencies. Since the inception of the standard in 2010, there has been an evolution in both new technologies with an impact on the system dependency factors and new knowledge on how to address them. Hence, it is important to capture these aspects and update the methodology that can be used to reason about CCF's causes. In this paper, we present an enhanced methodology for estimating the β-factor, which builds upon the core methodology provided by IEC 61508. In particular, we add 33 new questions and provide an estimation method for scoring the β-factor. We also illustrate our methodology by applying it to a realistic system and discuss the findings. Our proposed methodology permits the consideration of aspects not

[2]https://dsd-seaa2023.com/

included in the core methodology, such as the level of defense support and safety culture. It also allows practitioners to consider more dependencies, leading to a reduction in CCF. The rationale is that the more defenses are addressed, the more protection can be achieved against CCF.
Contribution: I am the primary author of the paper and was actively involved in both the writing and the presentation of it. The second author made a significant contribution by helping to define the methodology and supporting the overall writing process. The author also played a key role in continuously reviewing and enhancing the quality of the paper. The third author thoroughly reviewed the manuscript and provided valuable and constructive feedback, which greatly contributed to the refinement and overall development of the paper.

Status: Accepted and presented at the European Conference on Software Process Improvement (EuroSPI 2024[3]), which has been published in the Springer Nature Link digital library [20].

Paper 3: *Evaluation of IEC 61508 Defenses for Common Cause Failures in Railway Industry*
Authors: Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila and Sasikumar Punnekkat
Abstract: The assessment of Common Cause Failures (CCF), i.e., failures of multiple components due to a shared root cause, is essential during probabilistic risk assessment in safety-critical industries. However, not all contributing causes of CCF are directly observable at the component level, as they typically stem from systematic factors, i.e., design, operations, or environmental conditions. Thus, industries need to implement methodologies such as the β-factor model to account for these causes. The β-factor estimation suggested by the functional safety standard IEC 61508 is based on the assessment of a defined set of defense measures. However, the extent to which these defense measures address industry-specific CCF remains unclear due to limited contextual validation. In this paper, we evaluate the defense measures proposed by IEC 61508 with a specific focus on their applicability to the railway industry. To support this evaluation, we define a four-step process inspired by post-mortem analysis, a

[3]https://conference.eurospi.net/index.php/en/

method traditionally used to learn from past projects. This process is applied to a set of historical railway safety events, allowing us to identify significant CCF events and their underlying root causes. We then make a categorization based on the root causes of CCF in relation to the defense measures outlined in IEC 61508 and estimate the corresponding β-factor for each category. Finally, we assess the coverage and adequacy of the standard's defenses in addressing the identified CCF. The insights gained from this study aim to support the development of more robust and context-aware CCF assessment methods for the railway sector.
Contribution: I served as the primary driver of the paper, actively contributing to its writing and presentation. The second author contributed to the draft of various sections and played a key role in developing the methodology. In addition, the second author reviewed the manuscript and helped to improve its overall quality. The third author provided a thorough review and contributed valuable feedback and expertise, supporting the overall development of the paper.

Status: Accepted and presented at the European Conference on Software Process Improvement (EuroSPI 2025[4]), which has been published in the Springer Nature Link digital library [21].

[4]https://conference.eurospi.net/index.php/en/

Chapter 2

Background

In this chapter, we introduce the background information essential for the development of this thesis.

2.1 Safety-Critical Systems

Safety-critical systems [22] are designed to ensure that, even in the presence of faults, the system can reach a predefined safe state. This *safe state* may involve shutting down or switching to a less functional mode to prevent harm. In more complex systems, intermediate safe states are used when full shutdown is impractical. Examples include fallback analog controls in aircraft or blinking red lights in traffic systems. These systems often incorporate backup mechanisms, such as human intervention, to maintain safety under failure conditions. The failure of such safety-critical systems could result in intolerable consequences, such as loss of life, serious injury, environmental damage, or significant property loss [1]. These failures are unacceptable and require systematic risk management. Hence, the safety-critical systems are heavily regulated, and their safe operation is ensured through the principles of functional safety, provided by standars like IEC 61508 [12].

According to IEC 61508 [12], Equipment Under Control (EUC) refers to equipment, machinery, apparatus, or plant used in manufacturing, processing, transportation, medical, or other activities. To safeguard such EUC from haz-

ardous events, a safety-related system is implemented to carry out specific safety functions that ensure the EUC is maintained in or returned to a safe state. A safety-related system may operate independently or in combination with other safety-related systems and risk reduction measures to achieve the required level of safety integrity.

Safety integrity is defined as the probability that the safety-related system will perform its intended safety functions correctly under all specified conditions and within a defined time period. This concept inherently depends on the system's reliability, as a more reliable system is less likely to experience failures that compromise its safety functions. According to the IEC 61508 standard, one of the key threats to achieving safety integrity is the occurrence of Common Cause Failures (CCF) [1]. A CCF arises when one or more events lead to simultaneous failures in two or more independent channels of a multi-channel system, potentially resulting in a complete system failure.

2.2 System Reliability

Reliability is defined as: *"the probability that a device, machine or system will perform a specified function within prescribed limits, under given environmental conditions, for a specified time"* [23]. In simpler terms, reliability refers to the probability that a system or component will function as intended for a defined period. Since most systems consist of multiple interconnected components or subsystems, evaluating the reliability of the system involves assessing the performance of the entire setup, including all individual parts and their interactions. In general, the components in a system configurations can be connected in **series** or in **parallel** arrangements [24]:

- In a **series configuration**, all components must operate successfully for the system to function. If any single component fails, the entire system fails. For example, in Figure 2.1, the subsystems are shown in a series configuration.
- In a **parallel configuration**, one component serves as a backup for another in case of failure. This setup is typically used when high reliability is required, as it provides redundancy. For example, in Figure 2.2, the

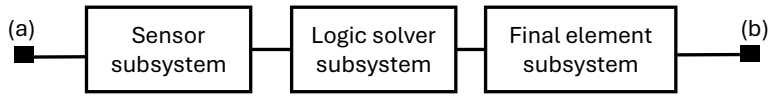

Figure 2.1. Example of series system [1]

subsystems are shown in a parallel configuration, in which the system functions if at least 1 out of n items functions.

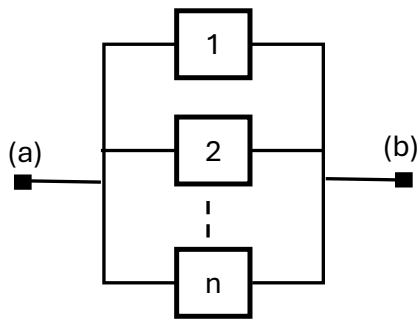

Figure 2.2. Example of parallel system [1]

Hence, redundancy helps to improve the overall reliability of the system by ensuring continued operation even if one component fails.
According to [1], reliability can be achieved through:

- **Design**
  - System architecture, including redundancy.
  - Selection of appropriate components (e.g., transmitter vs. switch).
  - Use of high-quality elements.
  - Built-in self-testing and diagnostics.
- **Installation**
  - Performed according to the manufacturer's guidelines.

- **Testing**
  - Conducted during start-up.
  - Performed at specified intervals or after any modifications.

Industries work to ensure and maintain high reliability by managing each phase of the life cycle of a technical system from the definition of requirements, design, and research, to development, production, installation, operation, and eventual disposal of the product [25]. Industry-related standards such as EN 50126 [13] (a key functional safety standard in the railway industry) define a life cycle framework of the system that includes planning, management, control and monitoring of all aspects of the system which also integrates reliability and safety elements.

2.3 Redundancy

According to IEC 61508 [12], redundancy is defined as "the existence of more than one means of performing a given function". Industrial systems are generally made up of multiple interconnected sub-systems or components, which may be electrical, mechanical, or digital. To improve reliability, safety-critical systems often incorporate redundancy and output voting mechanisms, such as MooN voting [26], where M out of N units must operate correctly to perform a safety function. In this context, N represents the total number of units (e.g., components or channels), and M represents the minimum number required for successful operation, with $M \leq N$. For example, consider a parallel system (recalled in Section 2.2) illustrated in Figure 2.3, configured as 1oo2 (one out of two).

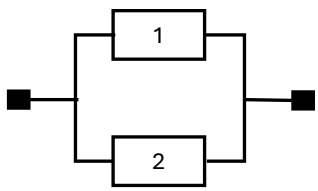

Figure 2.3. System with 1oo2 configuration

In this setup, at least one of the two components must function correctly to achieve the intended safety function.

2.4 Common Cause Failures (CCF)

The IEC 61508 standard [12] defines "Common Cause Failures (CCF) as the result of one or more events causing concurrent failures of two or more separate channels in a multiple-channel system, leading to system failure". The relationship between CCF and individual channel failures is shown in Figure 2.4. A channel refers to an element or group of elements that independently implements a safety function.

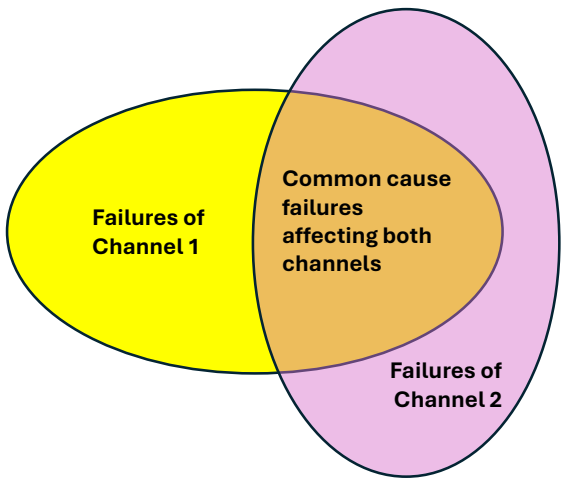

Figure 2.4. CCF impact on two channels [12]

CCF arises from the combination of a *root cause* (the fundamental cause of a failure event) and a *dependency factor*, which is a condition that causes components or systems to rely on one another. This combination increases the interdependence of channels and leads to greater overlap in the types of failure that can simultaneously affect multiple channels, as illustrated in Figure 2.4. Consequently, CCF significantly impacts the reliability of safety-critical systems

by enabling a single shared root cause, amplified by dependencies, to trigger failures across multiple channels. Therefore, identifying both root causes and dependency factors is essential to implementing effective defense mechanisms and minimizing the probability of CCF.

2.5 Root Causes of CCF

The nuclear industry collects and maintains CCF data and identifies the root causes of CCF [27]. A simplified classification of these root causes, based on [27], categorizes them into design, operational, and environmental causes, as described below:

- **Design Causes:** These include engineering-related causes, encompassing both conceptual design errors and realization errors such as construction, installation, and commissioning. The potential CCF effects due to design causes include:
  - *Design deficiencies*, such as logical errors in system logic that lead to simultaneous failure, and poor instrumentation or control logic that fails under specific conditions.
  - *Design realization faults*, including channel dependencies where redundant systems share the same signal path, and the use of identical parts that may fail simultaneously.
  - *Construction-related faults*, such as inadequate quality control during manufacturing, leading to identical defects, and shared vulnerabilities due to insufficient validation during installation or commissioning.
- **Operational causes:** These causes arise from procedural errors during testing, operations, and maintenance phases. They are associated with activities that involve the interface between the system and the personnel. Potential CCF effects due to operational causes include:
  - Repeated errors between systems due to shared procedures, such as imperfect repair, calibration, or testing.

  - Inadequate supervision, which allows systematic mistakes to persist.
  - Operator errors, including repeated errors across systems, poorly written or misunderstood procedures, and communication errors that result in simultaneous incorrect actions.

- **Environmental causes:** These include the extremes of environmental conditions and discrete energetic events occurring within or outside system boundaries. Potential effects of CCF due to environmental causes include:

  - Environmental stressors, such as temperature, humidity, vibration, and corrosion, can degrade multiple components simultaneously.
  - Catastrophic energetic events, including fire, flood, earthquake, and explosion, bypass redundancy and affect all systems at the same location.

2.6 Dependency factors

The dependency factors of CCF refer to the interdependencies between components or sub-systems that lead to multiple failures at the same time or over a period of time due to their shared root cause. Different types of dependency factors [8] exist between components/sub-systems as outlined below:

- Physical: e.g., shared design and shared manufacturer.
- Operational: e.g., same operational procedures and practices.
- Functional: e.g., interrelated functions within an integrated system that rely on each other.
- Human: e.g., mistake in communication, training, and competence.
- Environmental: e.g., extreme environmental conditions that simultaneously affect multiple components.

2.7 The β-Factor Approach Proposed by Fleming

This research focuses on the β-factor model proposed by Fleming [11], as it is one of the prominent and well-established models. In this β-factor model, the CCF quantification is performed using an equation (see equation (2.3)), in which different parameters are used. Here, the β-factor is referred to as the fraction of unit failures that are common mode. The other parameter used in the methodology is referred to as 'λ' (see equation (2.1)), which is the probability of system failure rate given by the number of failures over a period of time. In this methodology, two distinct forms of 'λ' are discussed. They are 'λ_1' (see equation (2.2)), which is referred to as independent failure, i.e., failure of a component that does not impact other components in the system and 'λ_2', which is referred to as the parameter for the CCF rate (see equation (2.3))

$$\lambda = \frac{\text{number of failures}}{\text{part-hours of operation}} \tag{2.1}$$

$$\lambda_1 = (1 - \beta)\lambda \tag{2.2}$$

$$\lambda_2 = \beta\lambda \tag{2.3}$$

In [11], the reliability of a redundant system is analyzed and demonstrated through an example involving a one-out-of-two diesel-generator configuration. The analysis incorporates U.S. nuclear power plant operating experience data, with a mission time of 100 hours. The value of β is derived from diesel-generator failure data [28]. Using these data, the failure rates for independent and common mode failures, 'λ_1'and 'λ_2' are derived as follows:

- Total failure rate: $\lambda = 1 \times 10^{-3}$ failures/hour
- Fraction of failures that are common mode: $\beta = 0.133$

Then:

$$\lambda_1 = (1 - \beta)\lambda = (1 - 0.133)(1 \times 10^{-3}) = 0.000867 \text{ failures/hour}$$

$$\lambda_2 = \beta\lambda = 0.133 \times 10^{-3} = 0.000133 \text{ failures/hour}$$

2.8 The β-Factor Approach Proposed by IEC 61508

The β-factor model proposed by Fleming (recalled in Section 2.7), utilizes operational experience data to estimate the β value. However, such data are not always available making it difficult to apply the model universally. In response, the IEC 61508 standard [12] proposes a methodology that, instead of relying on operational data, uses an alternative approach to assess and manage CCF.

In particular, this methodology estimates the β-factor by evaluating 37 checklist questions grouped under 8 defense measures, each considered as sub-factor. The checklist questions are assigned values based on engineering judgment. Additionally, the methodology considers the impact of diagnostic tests to account for the diagnostic capabilities of modern Programmable Electronic (PE) systems.

As these systems can detect a non-simultaneous CCF before it fully manifests. Thus, the methodology considers dangerous detected failures (DD) with diagnostic tests, since a large fraction of CCF can be detected by repeating the frequency of diagnostic tests before the CCF affects all available channels. This methodology also considers dangerous undetected failures (DU) that lie outside the diagnostic coverage. This means that, two different β-factor parameters are considered accordingly, i.e., β and β_D. In particular, β is the CCF factor for undetectable dangerous failure, and β_D is the CCF factor for detectable dangerous failure. The CCF rate i.e., λ_{CC} is calculated according to the equation (2.4) in the standard.

$$\lambda_{CC} = \lambda_{DU}\beta + \lambda_{DD}\beta_D \tag{2.4}$$

This thesis focuses exclusively on the β-factor (i.e., β for undetectable dangerous failures), and β_D is not considered in the scope of this work. To support the estimation of the β-factor, IEC 61508 introduces a set of defense measures aimed at mitigating the likelihood of CCF.

2.8.1 Defense measures

The IEC 61508 standard in its β-factor estimation methodology [12], established certain defense measures against the dependency factors (recalled in Section 2.6)

to minimize the probability of occurrence of CCF. In this regard, the implementation of these measures in the system leads to a reduction in the β (recalled in Section 2.7) used to estimate the probability of CCF failure.
The defense measures considered in the IEC 61508 β-factor estimation methodology are grouped under dependency factors (recalled in Section 2.6), and are explained in detail as follows [1]:

1. **Physical**

    1.1. **Separation/segregation:** This refers to the physical or electrical isolation between channels or components in a safety-related system. By enhancing the independence of each channel, separation significantly reduces the susceptibility to CCF. A practical example includes physically separating redundant units, such as placing two cameras that monitor the same event in distinct enclosures, ensuring that a single fault does not compromise both units.

    1.2. **Diversity/redundancy:** This refers to the use of different approaches, components, and technologies in the design and implementation of redundant systems to reduce the likelihood of CCF. For example, managing redundant units through separate design teams or using varied technologies helps avoid shared vulnerabilities and coupling factors. Diversity enhances system resilience by ensuring that a single fault is less likely to affect multiple components simultaneously.

    1.3. **Complexity/design/application/maturity/experience:** Redundant systems that utilize well-established designs and techniques proven effective over time are generally less prone to CCF, due to their *maturity.* Systems with lower *complexity*, characterized by fewer inputs and outputs, tend to have a reduced likelihood of CCF. Additionally, protecting these interfaces from potential over-voltage and over-current conditions (*application robustness*) further decreases susceptibility. Prior *experience* with the same hardware in similar operational environments also contributes to lowering the probability of CCF.

2. **Functional**

2.1. **Assessment/analysis and feedback of data:** It involves studying historical failure data and conducting design reviews to identify and mitigate CCF. It includes engaging with designers to implement design changes that eliminate potential CCF and analyzing field failures from previous projects. Techniques such as Failure Modes, Effects, and Criticality Analysis (FMECA) and other reliability assessments are used to uncover root causes and recommend measures to reduce the likelihood of CCF.

3. **Operational & Human**

3.1. **Procedures/human interface:** This refers to clear documented procedures, such as detailed installation and maintenance instructions are essential for minimizing human error. An intuitive and adequately designed human-machine interface further reduces the likelihood of mistakes. Additionally, minimizing human interaction with the system, or ensuring it is performed with care and precision, contributes to lowering the risk of errors and enhancing overall system reliability.

3.2. **Competence/training/safety culture:** This refers to the active involvement of designers, operators, and maintainers who understand the root causes and coupling factors. Proper training in emergency operations, system-specific procedures, and preventive measures is essential. Competence refers to the stakeholders' familiarity with the system, including their ability to identify risks and implement effective solutions. Regular reviews, discussions, and experience-based learning contribute to building a knowledgeable and capable workforce that can effectively mitigate CCF.

4. **Environmental**

4.1. **Environmental control:** For this, systems must be tested under expected environmental conditions such as temperature extremes, corrosion, dust, and vibration during development. These tests ensure that the system operates within its specified environmental

limits. Additionally, implementing protective measures like weatherproofing enhances the system's ability to withstand environmental stressors.

4.2. **Environmental testing:** Environmental testing is an engineering activity performed during system development to verify that components and systems can withstand expected environmental conditions such as temperature extremes, humidity, corrosion, dust and vibration. Type tests are one example, involving the qualification of a component based on testing one or more similar types.

For each defense measure, the methodology includes a set of checklist questions, each assigned a value based on engineering judgment. These values are organized in tabular format, with separate columns distinguishing between the logic subsystem (LS) and the sensors/final elements (SF). The methodology accounts for diagnostic tests, as recalled in Section 2.8, and splits the values assigned to each measure into X and Y. In this context, the values for the questions related to the logic subsystem (LS) are referred to as X_{LS} and Y_{LS}, and the corresponding values for the sensors or final elements (SF) are referred to as X_{SF} and Y_{SF}.
For example, the first defense measure, that is, the separation/segregation, has five questions. Among these, two pertain to the logic subsystems, two are related to sensors/final elements, and one question is related to both. The questions and associated values are shown in Table 2.1.

In this way, the standard [12] defines distinct sets of questions and associated values for each defense measure to support the estimation of the β-factor.

2.9 Illustrative Example

A safety-related system with two redundant diesel generators (1oo2 configuration) has the following failure data:

- Total dangerous failure rate: $\lambda = 1 \times 10^{-3}$ failures/hour
- The value obtained from the checklist scoring (see, for example, the checklist questions on separation and their associated values in Table 2.1)

Separation/segregation				
Checklist questions	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Are the logic subsystem channels on separate printed-circuit boards?	3,0	1,0		
Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.	2,5	0,5		
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?			2,5	1,5
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?			2,5	0,5
Are all signal cables for the channels routed separately at all positions?	1,5	1,5	1,0	2,0

Table 2.1. Checklist questionnaire and the associated values

is used to determine the β-factor. The β-factor is derived from the scoring of all checklist questions grouped under defense measures (see Section 2.8.1), resulting in a β-factor value of 0.133.

- Diagnostic coverage: 66% (i.e., 66% of failures are dangerous detected (DD), while 34% are dangerous undetected (DU))

Step 1: Dangerous detected and undetected failure Rate

$$\lambda_{DD} = 0.66 \cdot \lambda = 0.66 \cdot 10^{-3} = 0.00066 \text{ failures/hour}$$

$$\lambda_{DU} = 0.34 \cdot \lambda = 0.34 \cdot 10^{-3} = 0.00034 \text{ failures/hour}$$

Step 2: Assign β and β_D

$$\beta = 0.133 \quad \text{(for DU)}, \quad \beta_D = 0.05 \quad \text{(for DD)}$$

Step 3: The overall failure rate due to CCF

$$\lambda_{CC} = \lambda_{DU} \cdot \beta + \lambda_{DD} \cdot \beta_D$$

$$\begin{aligned}
\lambda_{CC} &= \lambda_{DU} \cdot \beta + \lambda_{DD} \cdot \beta_D \\
&= (0.00034 \cdot 0.133) + (0.00066 \cdot 0.05) \\
&= 0.00004522 + 0.000033 = 0.00007822 \text{ failures/hour}
\end{aligned}$$

Chapter 3

Research Summary

In this section, we discuss the research problem, the research questions, and the overall research process of this thesis.

3.1 Research problem

This thesis was initiated in response to a practical need identified by Alstom[1], a railway company that applies the IEC 61508 β-factor estimation methodology for the CCF analysis of redundant systems. In practice, Alstom observed that the β-factor values derived from the standard were overly conservative, leading to inflated failure rates. These inflated rates can prevent systems from achieving the required Safety Integrity Levels (SIL), forcing the implementation of additional safety measures, such as stricter design constraints or enhanced diagnostics that may not be justified by actual risk. This results in increased complexity, cost, and certification challenges.

A contributing factor to this issue is the definition of the dependency factors and defense measures embedded in the β-factor estimation methodology of IEC 61508 standard, which have remained largely unchanged for over a decade. The methodology relies on a fixed set of checklist questions and defense measures that are generic and design-focused, with limited flexibility to account for

[1] https://www.alstom.com/alstom-sweden

industry-specific operational realities or emerging technologies.

In parallel, the railway sector faces increasing pressure to deliver safety solutions that are not only reliable and certifiable but also cost-effective. As system complexity increases and access to operational data improves, the limitations of traditional approaches become more apparent. The industries such as nuclear has the capability to estimate the β-factor [11] using their historical CCF databases, such as those mentioned in [29] and [30]. However, railway companies such as Alstom rely on the IEC 61508 β-factor estimation methodology due to the absence of such data. This reliance reinforces conservative assumptions that may no longer reflect current operational realities.

This research supports the advancement of more accurate, less conservative, and context-sensitive safety assessments. As standards and practices evolve, there is a clear demand for methodologies that better reflect real-world operational conditions. The findings of this research suggest that the development of an industry-specific β-factor estimation methodology could help reduce conservatism and reveal the limitations of relying solely on standardized assumptions.

Overall research goal: *To propose improvements to IEC 61508 β-factor estimation methodology for addressing the specific needs of railway safety-critical systems.*

3.2 Research questions

In this section, the list of research questions that this thesis aims to answer is presented and explained in detail.

- RQ1. What β-factor estimation methodologies exist and how do they differ in approach, assumptions, and applicability across industries?

  The β-factor model is commonly used to assess CCF in safety-related systems, yet its theoretical foundation remains fragmented and inconsistent. This lack of structure makes it difficult to understand, apply, and evolve the methodology effectively. In domains such as the railway industry, where precision in safety assessment is crucial, this gap limits

both practical implementation and methodological advancement. This research addresses the need for a comprehensive and structured overview of existing β-factor models to support accurate application and enable further development of context-aware safety assessment approaches.

- RQ2.How can the β-factor estimation methodology in IEC 61508 be enhanced to better accommodate emerging technologies and future uncertainties?

  The β-factor estimation methodology proposed in IEC 61508 is widely applied in industries such as railways to quantify the probability of CCF in redundant systems. However, its current form does not fully reflect the complexity and evolving failure dynamics introduced by emerging technologies, which present novel CCF risks that are not captured by traditional β-factor assumptions. Enhancing the methodology by making it more flexible to accommodate new defense measures could significantly improve risk modeling accuracy and support the development of more robust and adaptive safety strategies, ensuring the continued relevance of IEC 61508.

- RQ3. To what extent do the defense measures proposed in IEC 61508 align with the CCF risks observed in the railway industry?

  IEC 61508 outlines generic defense measures intended to mitigate CCF in various industries using E/E/PE safety-related systems. However, these measures may not fully capture the unique characteristics and operational realities of the railway sector, where CCF may arise from different factors. This research question aims to critically assess the alignment between the generic provisions of the standard and the actual CCF risks encountered in railway applications. By identifying mismatches and gaps, the study contributes to a deeper understanding of the limitation of current approaches in the railway sector.

3.3 Research Process

This thesis adopts a research approach known as Mixed Methods Research (MMR) to address the limitations outlined in Chapter 1. MMR is defined as an approach that employs multiple procedures to investigate a research problem by collecting, analyzing, and integrating both qualitative and quantitative data, thereby generating novel insights [31].

MMR typically encompasses four primary research designs: exploratory sequential, explanatory sequential, convergent parallel, and embedded. In this thesis, we adopt the exploratory sequential design, in which the qualitative method is prioritized and serves as the foundation for a subsequent quantitative phase. The insights derived from the qualitative analysis inform and guide the development of the quantitative procedure.

In this MMR, we consider three different methodologies as presented in Figure 3.1. First, we adopt a Systematic Literature Review (SLR) procedure, which is "a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest" [32], to explore and structure the theoretical foundation. Next, we adopt the Design Science Methodology (DSM), which is "a structured approach to solve practical problems through the design and investigation of artifacts and generates scientific knowledge about the effectiveness and applicability of the artifacts in conditions of practice" [33]. Finally, we develop and implement a methodological process inspired by Post-Mortem Analysis (PMA), which is "a series of steps aimed at examining the lessons to be learned from completed projects to improve future practices" [34], to solve practical challenges using that foundation.

Following the principles of MMR, we explain the methodological rationale behind the set of methods adopted in this MMR and the procedural rigour with which the study is conducted.

1. **Systematic Literature Review (SLR)**: The SLR method was adopted following the guidelines of Kitchenham and Charters [32] to investigate the evolution and application of β-factor models. This review aims to address three main research questions. In this section, we refer to research questions using the notation **Pi-RQj**, where **i** denotes the paper number

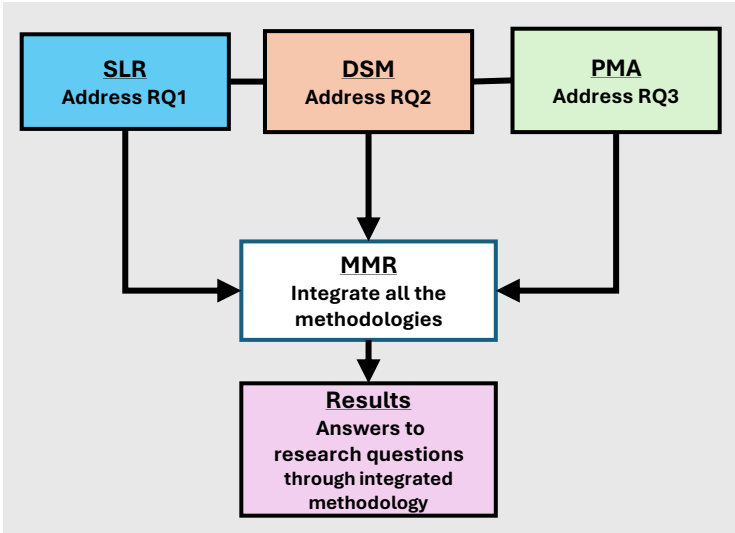

Figure 3.1. Mixed Method Research process

and **j** denotes the research question number as described in that paper:

P1-RQ1. *How did the β-factor models evolve over time, and how could we classify them?*
P1-RQ2. *How do the identified models provide support in the quantification of CCF with respect to redundancy and expert judgment?*
P1-RQ3. *What are the identified tools to model the β-factor models and the list of industries that are using different β-factor models?*

To identify relevant primary studies, a search was conducted across five digital libraries: 1) Google Scholar, 2) ScienceDirect, 3) Springer Link, 4) Web of Science, and 5) IEEE Explore using the search strings:

(*"Beta factor model" OR "β-factor model" OR "common cause failure model" OR "CCF model"*)

The search was conducted between December 2022 and January 2023, without any restrictions on the year of publication. The selection process involved multiple filtering stages, including title screening, duplicate removal, abstract screening, full-text review, and backward and forward snowballing, resulting in 51 primary studies. The inclusion criteria focused on peer-reviewed articles and technical reports written in English that discussed β-factor models, while studies that were not peer-reviewed or lacked relevance were excluded. Data extraction was performed using structured Excel sheets to capture metadata and model characteristics.
In conducting this SLR, we addressed ethical considerations by proactively mitigating potential threats such as publication bias, missing primary studies, and data collection inconsistencies. This was achieved through transparent documentation of the review protocol and the application of rigorous validation procedures. All sources were properly cited, and the limitations of the review process were acknowledged.

2. **Design Science Methodology**: The Design Science Methodology (DSM) for Information Systems and Software Engineering, as proposed by Wieringa [33], was adopted to enhance the β-factor estimation process outlined in the IEC 61508 standard. This methodology primarily involves the design and evaluation of an artifact to solve a practical problem.
In this research, the limitations of the β-factor methodology in the IEC 61508 standard are considered to be the core problem. To address this, a research artifact was developed, comprising two parts: *creation of an extended checklist* and *the proposal of an applicable estimation method for the β-factor.*

   This structured approach ensures that the artifact is designed in alignment with DSM principles, emphasizing relevance, rigour, and applicability in addressing the practical problem targeted in this research.

3. **Post-Mortem Analysis (PMA)**: In this research, a methodological process was developed, inspired by PMA, a method used to collect and study historical data from completed projects [34]. This adapted PMA-based approach was employed to address the following two research questions. In this section, we refer to research questions using the notation **Pi-RQj**,

where **i** denotes the paper number and **j** denotes the research question number as described in that paper:

P3-RQ1. *How can CCF be identified from historical events recorded in the railway domain?*
P3-RQ2. *To what extent are the defense measures proposed in IEC 61508 applicable to the railway domain?*

The key elements of our approach include data collection from historical records spanning five years, from 2020 to 2024, using a defined selection criterion and a systematic, objective filtering process. The collected data were organized into Excel sheets to enable structured and traceable analysis. Expert reviews were conducted to validate the findings. Our adopted process in this research is comprises of four main steps: *Select Events, Categorize Events, Determine β-factor, and Analyze Defense Support*.
In this research, mitigation strategies were effectively applied to address threats to construct validity, internal validity, and external validity threats, thereby strengthening the validity of the research results.

The integration of SLR, DSM, and PMA ensures a comprehensive exploration of both theoretical foundations and practical applications. The SLR establishes a robust knowledge base on β-factor models, DSM facilitates the development and evaluation of a novel artifact to enhance β-factor estimation, and PMA provides empirical insights from historical data in the railway domain. The subsequent chapters provide a detailed discussion of the findings and implications derived from each methodology.

Chapter 4

Research Contributions

This chapter present the details of the technical contributions of this thesis.

4.1 Approaches to β-Factor Estimation

Common Cause Failures (recalled in Section 2.4) can cause multiple component failures due to a single shared root cause. These failures pose a significant threat to the reliable functioning of safety-related systems in various industries. To address this, practitioners often adopt proven quantification methods recommended by safety standards. Among these, the β-factor estimation methodology suggested by the IEC 61508 safety standard (recalled in Section 2.8) is one of the most widely used approaches.

However, limited research has systematically analyzed β-factor models to provide a solid theoretical foundation for their development and application. To address this, we conducted a systematic literature review and identified 20 distinct β-factor models. These were categorized based on their estimation approach. Their key features and relationships are illustrated in Figure 4.1. We also analyzed the practical application of β-factor models identified through the literature review. The level of redundancy support (recalled in Section 2.3) provided by different models to achieve more accurate results was also examined and presented. In addition, we identified the available tool support for these models, including *SAPHIRE*, *CAFTA*, *Risk Spectrum*, and *Isograph*.

As shown in Figure 4.1, we classified the β-factor models into three categories based on their estimation approaches: quantitative, qualitative, and hybrid.

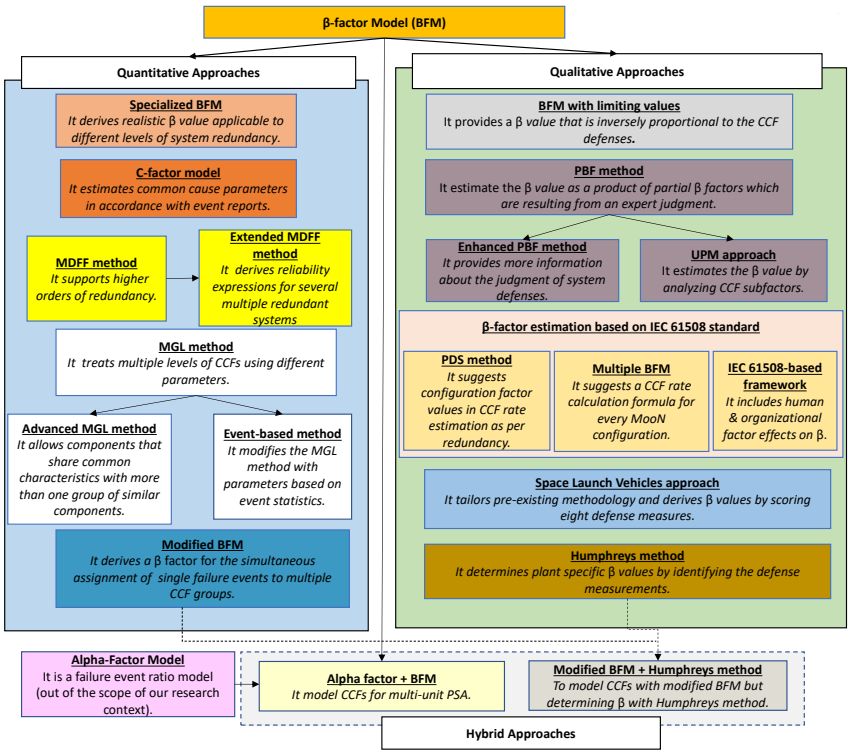

Figure 4.1. Models classification with distinguishing features and relationships

In quantitative models, the β value is estimated using historical CCF data. In qualitative models, the β value is derived through expert assessment of defense measures against CCF, as detailed in Table 4.1. Models that use a combination of both qualitative and quantitative approaches are known as hybrid models.
This research provides valuable insights into the application of these models across various industries offering a solid theoretical foundation for further development and practical implementation.
In particular, it supports the informed selection and application of β-factor

Table 4.1. β Estimation Factors for Qualitative Models

Type of factor	**Estimation Factor**
Design factors	Degree of component diversity
	Type of system
	Defense against CCF
	Degree of redundancy
	Design control
	Design review
	Functional diversity
	Equipment diversity
	Fail-safe design
	Operational interfaces
	Protection and segregation
	Derating and simplicity
	Separation of components
	Similarity in the components
	Complexity of the system
	Analysis of the components
	Isolation
	Understanding
	Evaluation
Construction factors	Construction and control
	Testing and commissioning
	Inspection
	Construction standards
Operation factors	Operational control
	Reliability monitoring
	Maintenance
	Proof test
	Operations
	Procedures
	Training
	Interface
Environment factors	Environmental control
	Environmental test
Condition factors	Control
	Experiment
Other factors	Design/application/maturity/experience
	Assessment and feedback of data
	Human interface
	Competence/training/safety culture

models. The β-factor classification enables practitioners to choose the most appropriate approach based on the availability of historical data and engineering judgment. Since safety-critical systems use different redundancy levels, choosing a β-factor model that matches the system's configuration is key to achieving accurate and less conservative results. Although all models claim to support every redundancy type, their performance varies; some deliver more precise and less conservative results than others. These findings help practitioners make informed model selections. Furthermore, the identified tools facilitate the practical application of these models to implement them effectively.

4.2 A Scalable Method for β-Factor Estimation

The β-factor estimation methodology outlined in the IEC 61508 standard (recalled in Section 2.8) estimates the β value based on scores derived from the evaluation of a fixed set of CCF defense measures. These dependency factors (see Section 2.6) and their associated checklist questions (as shown in Table 2.1) have remained unchanged since the introduction of the methodology more than a decade ago. However, with the rapid advancement of technology, modern safety-critical systems increasingly rely on shared software platforms, cloud infrastructure, and cybersecurity frameworks. These new forms of system inter-dependencies introduce shared vulnerabilities, significantly increasing the likelihood of CCF in diverse ways. Hence, this study aims to improve the handling of CCF by enhancing the methodology for β-factor estimation. The proposed approach introduces a more flexible, up-to-date, and comprehensible framework that enables practitioners to reason about a broader set of defense measures. By expanding the checklist and incorporating factors such as safety culture and emerging system dependencies, the methodology supports more accurate β-factor estimation. Ultimately, it lays the foundation for the development of industry-specific β-factor estimation methods tailored to diverse safety-critical contexts.

This research comprises two parts: an extended checklist and an applicable estimation method for the β factor.

The first part, namely the *creation of the checklist*, involved four key steps.

It started with the collection of relevant qualitative β-factor methodologies.

Next, we identified a comprehensive list of dependency factors, followed by the corresponding defense measures and checklist questions. This process resulted in the identification of 5 types of dependency factors with 10 categories of defense measures, as shown in Table 4.2.

Table 4.2. Dependency Factors and Defense Measures.

Dependency Factors	**Defense Measures**
Physical factors	Separation
	Diversity
	Design Control
Operational factors	Procedures
	Diagnostic testing
Functional factors	Safety assessment
Environmental factors	Environmental control
	Environmental testing
Human factors	Experience
	Training

We identified 33 new checklist questions in addition to the 37 existing ones from IEC 61508, resulting in a total of 70 questions categorized under 10 defense measures (see Table 4.2). In general, checklist questions related to human factors are not prioritized in IEC 61508; however, in our contribution, they are addressed under the defense categories of *training* and *experience*. Furthermore, we included a set of questions related to programmable controllers, which are not covered in the IEC 61508 standard. As an example, the checklist questions proposed in our methodology for the defense measures *design control* and *training* are presented in Table 4.3.

ID	Design Control
DC1	*Is the design based on techniques used in equipment that has been used successfully in the field for greater than 5 years?*
DC2	*Are the common cause failures considered in design reviews with the results fed back into the design?*
DC3	*Does the degree of redundancy more than dual redundancy?*
DC4	*Is the design proven, fail-safe, and follows standards?*
DC5	*If identical redundancy is employed, has the potential for CCF been adequately addressed?*
DC6	*Do I/O data buses have strong error detection?*
DC7	*Has the multi-channel design been thoroughly reviewed by competent staff, independent of the design team?*
DC8	*Were the channels designed by different designers without communication between them during the design activities?*
DC9	*Is the system simple, for example no more than 10 inputs or outputs per channel?*
DC10	*Does there is a construction control?*
ID	**Training**
T1	*Have the designers been trained (with training documentation) to understand the causes and consequences of common-cause failures?*
T2	*Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?*
T3	*Do the individuals involved in developing safety requirement specification been trained to understand the consequences of common cause failures?*
T4	*Do the individuals involved in developing the conceptual design been trained to understand the consequences of common-cause failures?*
T5	*Do the individuals involved in developing the application software been trained to understand the consequences of common-cause failures?*
T6	*Do the individuals performing the installation trained to understand the consequences of common-cause failures?*
T7	*Do the individuals performing the inspection trained to understand the consequences of common-cause failures?*
T8	*Is the individuals involved in testing been trained to understand the consequences of common-cause failures?*
T9	*Is the training updated relative to changes in operation and maintenance procedures?*

Table 4.3. Checklist Questions of *Design Control* and *Training*

The second part of this research is the β-factor estimation process. This process builds on the β-factor methodology described in [35], introducing notable differences in the defense measures considered and their scoring. Furthermore, this research provides a detailed description of each step. This second part

comprises six main steps, which are illustrated in Figure 4.2.

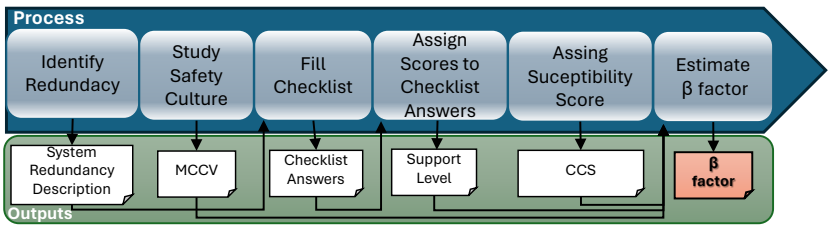

Figure 4.2. β-factor Estimation Process

- **Step 1:** It involves the study of the system and identification of system redundancies for which the CCF has to be assessed.

- **Step 2:** The Maximum Common Cause Value (MCCV) reflects the industry's safety culture and is used to estimate the maximum β-factor based on expert judgment and experience. It is determined by considering factors such as safety culture, failure history, management effectiveness, maintenance practices, and resource constraints like budget and schedule. The MCCV is set at 10% for industries with a strong safety culture, 20% for those with moderate safety practices, and 30% for industries with a poor safety culture, limited training, and constrained resources.

- **Step 3:** In this step, the checklist questionnaire is filled out by selecting one of three response options for each question: Yes (value = 1), No (value = 0), and Not Applicable (value = 1, same as Yes, as it does not affect the common cause susceptibility score (CCS)). An exception is question DT5 under *diagnostic testing*, which offers four options: low coverage (60–90%, value = 0.25), medium coverage (90–99%, value = 0.50), high coverage (>99%, value = 1), and Not Applicable (value = 1).

- **Step 4:** The scores are assigned based on the previous step. Each defense measure's maximum score equals its number of questions. The support level is classified as *low* (score < 50%), *medium* (50% to <100%), or *high* (score = 100%) based on the total score achieved.

- **Step 5:** A susceptibility score of 1, 5, or 10 is assigned to each defense measure according to its support level (high, medium, or low). The total Common Cause Susceptibility (CCS) score is calculated as the sum of the products of the number of measures at each level and their respective scores, as shown in the equation 4.1.

$$CCS = 10.N_{low} + 5.\ N_{medium} + 1.\ N_{high} \tag{4.1}$$

- **Step 6:** The maximum Common Cause Susceptibility (CCS) score, denoted as T, occurs when all defense measures are rated with the lowest support level, each assigned a susceptibility score of 10. In our methodology with 10 defenses, the maximum T is 100 (10 × 10). This value increases if more defenses are included in the methodology. The β-factor is then estimated using this score in the corresponding equation 4.2.

$$\beta = \frac{\text{CCS}}{\text{T}} * MCCV \tag{4.2}$$

This research contributes to improving the handling of CCF by enhancing the methodology for β-factor estimation. The proposed approach is flexible and supports practitioners in adopting a greater number of defenses, taking into account the CCF risks associated with technological advancements. The methodological insights provided in this research emphasize adaptability, simplicity, comprehensibility, flexibility, and adequacy.

4.3 Evaluating IEC 61508 Defenses in Railways

This research contribution primarily serves the railway industry, as well as other sectors that rely on the IEC 61508 standard to evaluate the CCF (recalled in Section 2.4). The main objective of this research is to evaluate the applicability of IEC 61508 defenses (recalled in Section 2.8) to the CCF in railway systems. The research process consists of four main steps, illustrated in Figure 4.3. These steps are explained below:

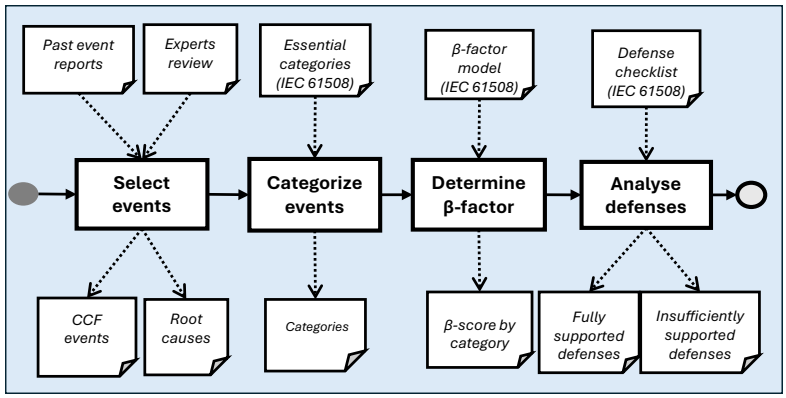

Figure 4.3. Steps in our evaluation process

In step 1, CCF events are selected from historical event reports provided by Alstom[1], which maintains records of accidents identified during validation, installation, testing, or operational phases. Events are selected based on two criteria: (1) *events in which two or more components failed due to the same root cause*, and (2) *sets of events that, although occurring separately, share a common root cause*. This step results in a curated list of CCF events along with their corresponding root causes (see Table 4.4).
The CCF dataset[2], collected in this step, provides a focused and well-defined collection of CCF events that establishes a strong foundation for building more comprehensive repositories in future studies in the railway domain.

[1]https://www.alstom.com/alstom-sweden
[2]https://rb.gy/lukc3r

Table 4.4. Identified root causes of CCF in railways

Root Cause Category	Source
Design	Engineering - Others Material - Others Material - Supplier Process Management (2) Material - Design Issue Procurement - Supplier material issue Procurement - Supplier - Others Procurement - Supplier - Design non conformity Material - Not Conform to specifications Industrialization/manufacturing issue
Operation	Operations - Manufacturing Manpower issue Manpower - Self-inspection inefficient (2) Operations - Others Train Operation - Training and Competencies Documentation - not detailed enough (5) Manpower - Training Manpower - Error / Identification (2) Maintenance - Documentation Method - Other (2) Maintenance - Others Documentation - mistake Method - Process Management
Environmental	Environment - Others

In step 2, the selected events are classified based on the root cause categories (see Section 2.5). The overall distribution of root causes of CCF events in railways is shown in Figure 4.4.

In step 3, we analyze the β-factor estimation in IEC 61508. For this, we study the defense measures (see Section 2.8.1) and their score distribution across each root cause category: design, operational, and environmental. This analysis concludes that within the IEC 61508 standard, the overall β-factor is primarily shaped by design-related defenses, with environmental and operational defenses

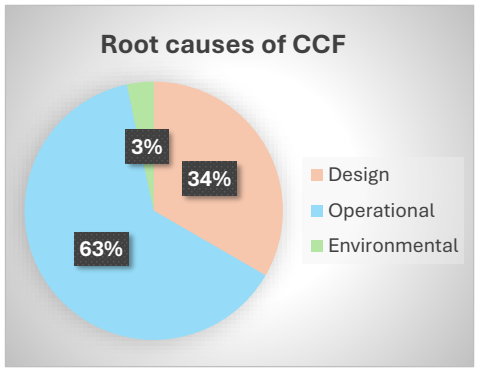

Figure 4.4. Root cause distribution of CCF in railways

playing progressively smaller roles. This is based on the weighting criteria used in the β-factor estimation process, as depicted in Figure 4.5.

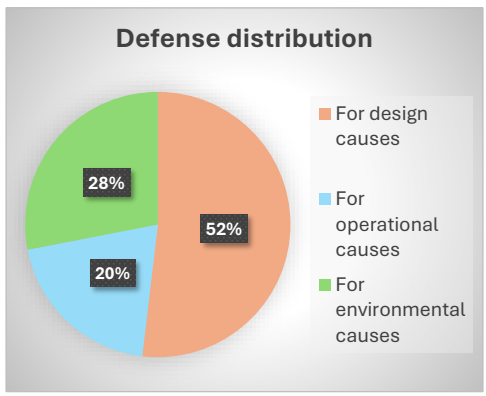

Figure 4.5. Defense contribution to overall β-factor in IEC 61508

In the final step, we analyze the defense support provided by IEC 61508 against the identified CCF in railways. We conclude that operational root causes are the most prevalent in railway CCF, but the IEC 61508 standard predominantly emphasizes design-related defenses. Despite the absence of defenses that address

operational root causes, IEC 61508 still yields a β-value of 1% for the logic subsystem and 2% for sensors and final elements. This results in a misalignment between the standard's defense measures and the actual root causes observed in the railway systems, leading to an inaccurate β-factor. Therefore, this research concludes that the standard should more effectively estimate CCF risks in railway contexts.

Chapter 5

Related Work

The β-factor model has been in use for many years [36], and several distinct estimation methodologies are described in the literature. For example, the IEC 61508 standard estimates the β-factor by assigning and quantifying values for 37 checklist questions across 8 defense measures. Several studies [8], [37], and [38] discuss common cause failure (CCF) methodologies, including the β-factor model. However, the existing literature is fragmented, and there are no state-of-the-art studies that focus exclusively on the β-factor model and its characteristics. To address this gap, this research conducted a systematic literature review and provided a comprehensive overview of β-factor models. As a result, 20 distinct β-factor models were identified (recalled in Section 4.1).

The study [39] proposed a framework that incorporates the human and organizational factors (HOFs) influencing CCF during the operational phase. Since the β-factor in IEC 61508 is typically determined using checklist questions focused on the design phase, this study highlights that several factors during the operational phase can significantly affect the actual β-factor. To address this, the framework integrates HOFs into β-factor estimation, enabling dynamic monitoring and management of operational changes. However, this approach primarily targets operational variability and is distinct from our study, which is designed to be adaptable to emerging technologies and industry-specific requirements.

A recent study [40] aimed to enhance the β-factor estimation methodology of IEC 61508 by incorporating additional defense measures relevant to modern technologies such as digital transformation systems in process safety. However, the values assigned to these defense measures were derived from historical failure data from nuclear power plants. In contrast, our research (recalled in Section 4.2) introduces a methodology that allows the inclusion of additional defense measures, with values assigned to checklist questions based on their applicability rather than historical data. This makes our approach particularly suitable for industries that lack historical failure records.

Studies such as [41] have focused on estimating the β-factor for railway systems using a methodology that employs the same checklist questions as those in the IEC 61508 standard. In [42], the β-factor estimation methodology suggested by IEC 61508 is adopted for fire safety systems in the railway industry. Similarly, [43] applies the IEC 61508-based methodology to estimate the β-factor in train operation control systems. However, the defense measures and associated checklist questions provided in the IEC 61508 standard are designed to be broadly applicable across all industries utilizing E/E/PE systems, rather than being tailored to the specific characteristics of railway applications.

Hence, in our research (recalled in Section 4.3), we focus specifically on the railway industry to identify root causes that lead to multiple component or system failures due to dependency factors. This targeted approach supports future efforts to develop a railway-specific β-factor estimation methodology by tailoring defense measures and checklist questions to better reflect the unique characteristics and operational contexts of railway systems.

Chapter 6

Conclusions and Future work

This chapter presents the overall conclusions of the thesis in Section 6.1 and the details of the future work in Section 6.2.

6.1 Conclusions

This thesis has provided an approach to adapt the β-factor estimation methodology outlined in IEC 61508 to enhance its applicability within the context of the railway industry. In particular:

1. A systematic literature review was conducted that offered in-depth insights into the β-factor model landscape. This review identified 20 distinct β-factor models, and provided additional understanding of their historical development, classification, industrial applications, and tool support. These findings contribute to building the theoretical foundation necessary to support both practical implementation and methodological innovation.

2. We proposed a methodology that allows the inclusion of additional measures. In our proposed methodology, 33 new checklist questions were introduced in addition to the 37 questions suggested by the standard, using a structured scoring approach for β-factor estimation. Thus, we address this limitation by developing a flexible and adaptable β-factor estimation methodology.

3. We implemented a four-step methodology for investigating the applicability of IEC 61508 defense measures to railway-specific CCF. To identify CCF events from historical safety event reports provided by railway company Alstom[1]. The methodology was also used to assess the adequacy and coverage of the standard's defenses in addressing the identified CCF within the railway context. In this study, we identified 30 CCF events in the railway domain, with the majority linked to operational root causes. However, the β-factor values in the standard are predominantly influenced by design-related defenses. Despite the absence of defenses targeting operational root causes, the standard still yields a β-factor of 1% for the logic subsystem and 2% for sensors and final elements. This highlights a discrepancy between the actual root causes of CCF in railway systems and the defense measures supported by IEC 61508. Thus, we address the third limitation by evaluating the applicability of IEC 61508 defenses for CCF in the railway industry.

These findings underscore the need for industry-specific strategies and support the development of a more context-aware β-factor methodology, by identifying and addressing key constraints such as generalized assumptions, lack of domain-specific adaptability, and limited flexibility to accommodate emerging technologies.

6.2 Future Work

Future work will involve *structuring CCF-related knowledge into domain-specific ontologies* to support consistent assessments and reasoning in β-factor estimation. Furthermore, research will *investigate how software-related CCF are identified, modeled, and mitigated across industries*, contributing to the development of software-specific defense strategies. To ensure practical relevance, we plan to *conduct surveys and interviews with safety practitioners* to capture challenges in CCF evaluation and guide iterative improvements to the methodology. As a next step, *a pilot study will be conducted* to apply and assess the proposed methodology in the railway context.

[1] `https://www.alstom.com/alstom-sweden`

Bibliography

[1] Marvin Rausand. *Reliability of safety-critical systems: theory and applications*. John Wiley & Sons, 2014.

[2] 179 dead in South Korea's worst plane crash in decades. `https://edition.cnn.com/world/live-news/south-korea-plane-crash-12-29-24-intl-hnk/index.html`. [Accessed: 2025-01-10].

[3] Michael Stamatelatos. Probabilistic risk assessment: what is it and why is it worth performing it. *NASA Office of Safety and Mission Assurance*, 4(05):00, 2000.

[4] Jose Antonio Bogarin Geymayr and Nelson Francisco Favilla Ebecken. Fault-tree analysis: a knowledge-engineering approach. *IEEE Transactions on Reliability*, 44(1):37–45, 1995.

[5] DOE Guideline. Root cause analysis guidance document. *US Department of Energy: Washington*, 1992.

[6] Siqi Qiu and Xinguo Ming. Explicit and implicit bayesian network-based methods for the risk assessment of systems subject to probabilistic common-cause failures. *Computers in Industry*, 123:103319, 2020.

[7] Jussi K Vaurio. An implicit method for incorporating common-cause failures in system analysis. *IEEE Transactions on Reliability*, 47(2):173–180, 2002.

[8] Per Hokstad and Marvin Rausand. Common cause failure modeling: status and trends. *Handbook of performability engineering*, pages 621–640, 2008.

[9] Ali Mosleh. A multi-parameter, eventbased common-cause failure model. *SMiRT9 Paper No. M7/3*, 1987.

[10] WE Vesely. Estimating common cause failure probabilities in reliability and risk analysis: Marshall-olkin specializations. *Nuclear systems reliability engineering and risk assessment*, 2(314-341), 1977.

[11] Karl N Fleming. Reliability model for common mode failures in redundant safety systems. Technical report, General Atomics, San Diego, CA (United States), 1974.

[12] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – part 6: Guidelines on the application of parts 2 and 3. `https://webstore.iec.ch/publication/5520`. [Accessed: 2024-03-21].

[13] EN 50126: Railway applications. the specification and demonstration of reliability, availability, maintainability and safety (RAMS) generic RAMS process. `https://rb.gy/pij444`. [Accessed: 2025-09-22].

[14] EN 50128: Railway applications - communication, signalling and processing systems - software for railway control and protection systems. `https://www.en-standard.eu/search/?q=EN+50128`. [Accessed: 2025-09-22].

[15] EN 50129: Railway applications - communication, signalling and processing systems - safety related electronic systems for signalling. `https://short-url.org/1fGgU`. [Accessed: 2025-09-22].

[16] IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems – part 3: Software requirements. `https://webstore.iec.ch/publication/62902`. [Accessed: 2024-03-21].

[17] Kevin Warwick. *Artificial intelligence: the basics*. Routledge, 2013.

[18] ISO (2015). ASTM 52900:2015 Additive manufacturing — general principles — terminology. `https://www.iso.org/obp/ui/#iso:std:iso-astm:52900:ed-2:v1:en`. [Accessed: 2025-01-17].

[19] Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila, and Sasikumar Punnekkat. A systematic review of β-factor models in the quantification of common cause failures. In *2023 49th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, pages 262–269. IEEE, 2023.

[20] Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila, and Sasikumar Punnekkat. A proposal for enhancing IEC 61508 methodology for the β-factor estimation. In *European Conference on Software Process Improvement*, pages 300–314. Springer, 2024.

[21] Sirisha Bai Govardhan Rao, Julieth Patricia Castellanos-Ardila, and Sasikumar Punnekkat. Evaluation of IEC 61508 defenses for common cause failures in railway industry. In *European Conference on Software Process Improvement*, pages 325–338. Springer, 2025.

[22] Nancy G Leveson. Software safety: Why, what, and how. *ACM computing surveys (CSUR)*, 18(2):125–163, 1986.

[23] G Thompson, JS Liu, and L Hollaway. An approach to design for reliability. *Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering*, 213(1):61–67, 1999.

[24] Rudolph Frederick Stapelberg. *Handbook of reliability, availability, maintainability and safety in engineering design*. Springer, 2009.

[25] Alena Breznická, Marcel Kohutiar, Michal Krbat'a, Maroš Eckert, and Pavol Mikuš. Reliability analysis during the life cycle of a technical system and the monitoring of reliability properties. *Systems*, 11(12):556, 2023.

[26] Alejandro Carlos Torres-Echeverría, Sebastián Martorell, and Haydn A Thompson. Modeling safety instrumented systems with MooN voting

architectures addressing system reconfiguration for testing. *Reliability Engineering & System Safety*, 96(5):545–563, 2011.

[27] A J Bourne, G T Edwards, D M Hunns, D R Poulter, and I A Watson. Defences against common-mode failures in redundancy systems. *SRD R-196 January*, 1981.

[28] John L. Crooks. *Diesel generator operating experience at nuclear power plants*. Office of Operations Evaluation, Directorate of Regulatory Operations, 1974.

[29] Thomas E. Wierman, Dale M. Rasmuson, and Ali Mosleh. Common-cause failure database and analysis system: Event data collection, classification, and coding (nureg/cr-6268, inel/ext-07-12969, revision 1), 2007. [Accessed: 2025-10-01].

[30] OECD Nuclear Energy Agency. International common-cause failure data exchange (ICDE) project. `http://tiny.cc/usat001`, 2020. [Accessed: 2025-10-01].

[31] Margaret-Anne Storey, Rashina Hoda, Alessandra Maciel Paz Milani, and Maria Teresa Baldassarre. Guidelines for using mixed and multi methods research in software engineering. *arXiv preprint arXiv:2404.06011*, 2024.

[32] Barbara Kitchenham and Stuart Charters. Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report, July 9 2007. Technical Report, EBSE 2007-001.

[33] Roel J Wieringa. *Design science methodology for information systems and software engineering*. Springer, 2014.

[34] Mauri Myllyaho, Outi Salo, Jukka Kääriäinen, Jarkko Hyysalo, and Juha Koskela. A review of small and large post-mortem analysis methods. *Proceedings of the ICSSEA, Paris*, pages 1–8, 2004.

[35] Frank Hark, Rob Ring, Steven D Novack, and Paul Britton. Common cause failure modeling in space launch vehicles. In *International Association for*

the Advancement of Space Safety (IAASS) Conference, number M16-5258, 2015.

[36] BS Dhillon and OC Anude. Common-cause failures in engineering systems: A review. *International Journal of Reliability, Quality and Safety Engineering*, 1(01):103–129, 1994.

[37] Torbjørn Lilleheier. Analysis of commom cause failures in complex safety instrumented systems. Master's thesis, Institutt for matematiske fag, 2008.

[38] Per Hokstad. Common cause and dependent failure modeling. In *Fundamental Studies in Engineering*, volume 16, pages 411–444. Elsevier, 1993.

[39] Maryam Rahimi and Marvin Rausand. Monitoring human and organizational factors influencing common-cause failures of safety-instrumented system during the operational phase. *Reliability Engineering & System Safety*, 120:10–17, 2013.

[40] Jinhyung Park, Kyoshik Park, and Chang Jun Lee. The development of a common cause factor score table on IEC 61508 part 6 edition 2.0. *Journal of Loss Prevention in the Process Industries*, 88:105270, 2024.

[41] Per Hokstad, Solfrid Håbrekke, Mary Ann Lundteigen, and Tor Onshus. Use of the PDS method for railway applications. *Norway: SINTEF Technology and Society*, 15:5–23, 2009.

[42] Ozgur Turay Kaymakci, Ilker Ustoglu, and Ender Divriklioglu. Reliability assessment of fire safety systems in railway industry: a case study. *Journal of the Chinese Institute of Engineers*, 38(3):286–296, 2015.

[43] Weiqing Xue, Yan Zhao, Jiwen Xiao, and Mack Zhang. The research and application of fail-safe technologies in rail transit train operation control system. In *2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS)*, pages 1100–1104. IEEE, 2014.