Facilitating β-Factor Estimation for Common Cause Failures of Safety-Related System

Sirisha Bai Govardhan Rao[1,2](✉)

[1] Alstom, Västerås, Sweden
[2] Mälardalen University, Västerås, Sweden
sirisha.bai.govardhan.rao@mdu.se

Abstract. Common Cause Failures (CCF) have the potential to make safety-related systems fail. Hence, the safety-critical industries identify and quantify the probability of CCF using different methodologies. For example, industries like railways rely on a β-factor methodology suggested by the IEC 61508 standard, in which defense measures are established against CCF and β-factor (used in the estimation of the probability of CCF) quantified based on the application of those measures. However, this methodology had two main research problems (RP) they are, RP1: The standard's inception was in 2010, and due to this the measures against the CCF that arose from the emerging new technologies were absent in the standard. Moreover, the methodology has not provided any means to permit new measures. RP2: The methodology is generalized and applicable to all safety-related systems using Electrical/Electronic/Programmable Electronic-based systems across different industries. However, the impact of CCF and the required defense measures against them would be distinct in each industry. Eventually, the negligence of these problems leads to conservative β estimations. Therefore this research aims to provide possible solutions for these two problems. For RP1, by proposing a methodology that enhances the IEC 61508 standard methodology in β-factor estimation and adopts a way that could consider new defense measures in addition to the existing measures. For RP2, we planned to demonstrate an approach to develop an industry-specific β-factor methodology focusing on railways. Later, the methodology is applied to a system i.e., Electro-dynamic braking of railway propulsion systems for β-factor estimation. This research would provide insights to industrial practitioners and researchers to develop industry-specific β-factor methodology to estimate more realistic β, by analyzing appropriate defense measures.

Keywords: IEC 61508 standard · β-factor · System Safety · Common Cause Failure · Redundancy · Railways · Safety-critical industries

A. Bertolino et al. (Eds.): QUATIC 2024, CCIS 2178, pp. 444–451, 2024.
https://doi.org/10.1007/978-3-031-70245-7_33

1 Introduction

Redundancy supports the reliability of safety systems in performing the needed safety functions despite a single failure. Hence, safety-critical industries adopt redundancy in the design of safety systems. However, common-cause failures (CCF) are a major threat to the redundancy of the systems, because CCF is an event leading to the failure of a component due to a cause and that cause has the potential to fail the other redundant components in the system. The failure of those multiple redundant components consecutively leads to system failure [7]. These CCF create a greater impact on the overall probability of system failure. Hence, they are identified and quantified in probabilistic risk assessments of safety systems using the CCF models. There are different varieties of models available for CCF quantification. Among these, the β-factor model [4] is one of the prominent CCF models and has been used by various safety-critical industries. The estimation of the β-factor (i.e., a factor used in the quantification of CCF) could be made following the quantitative or qualitative approaches available in the literature [13].

The IEC 61508 standard [2] suggested a qualitative β-factor estimation methodology for the CCF quantification. The methodology establishes certain defense measures against the CCF to minimize their probability of occurrence. The implementation of each measure leads to the reduction of the β-factor value. The defense measures are provided in the form of 37 checklist questions and each question has an associated value based on engineering judgment to quantify the β-factor value. There are two research problems (RP) with this methodology. The first problem (RP1) is the inability to include new measures to the pre-existed measures in the methodology. Since the methodology is from 2010, there is a need to add new measures against the probability of CCF emerging with the latest technological developments in the industry. In this context, a recent study [12] highlighted and considered the importance of including new measures related to the latest technologies, and developed a CCF score table on the IEC 61508 standard methodology. However, the values assigned to the measures in the proposed table are based on the failure data of the nuclear power plant.

The problem (RP2) is that many safety-critical industries such as railways comply with the IEC 61508 standard as a safety practice. However, the established defense measures in the IEC 61508 standard methodology apply to all industries using Electrical/Electronic/Programmable Electronic (E/E/PE) - based systems and not especially for any application/industry. Hence, there is a need to analyze the industry-specific factors and identify the essential defense measures against the CCF to derive more appropriate application-specific β. In this context, the standard IEC 62061 [3], highlighted that not all measures from the IEC 61508 standard apply to the machinery application. Therefore, a few measures are considered for the β-factor estimation. In the same way, the IEC 61131-6 standard [1] considered some specific defense measures for the programmable controllers. However, there is a lack of studies/standards that focus on the defense measures against the probability of occurrence of CCF in railway applications. Even though certain studies like [5] adopted a distinct method for the CCF analysis of railway applications. However, it is not specifically made for the railway systems. Moreover, it considers the same defense measures from the IEC 61508 standard method. Hence, these two problems (RP1 and RP2) could cause uncertainty in the estimated β, which leads to the adoption of inadequate/inessential safety requirements in the industry. Therefore, this research aims to provide possible solutions for these problems by proposing a methodology that enhances the IEC 61508 standard methodology which could consider additional defense measures and estimate β without the need for historical failure data. Then, we plan to demonstrate an approach to develop an industry-specific methodology focusing on one industry i.e., the railway industry, and perform a railway case study. The solution for RP1 is a demonstration of a generic method that applies to all safety-critical industries which could permit new measures. The solution for RP2 is not only useful for railways but also beneficial for those industries that intend to develop application-specific methodology by following our steps. In this research, we established five goals and adopted five research methodologies to achieve them.

In this paper, Sect. 2 presents our research plan which includes the research goals, research contributions, and the adopted research methods. Section 3 discusses the state-of-art. Section 4 presents our time plan, preliminary results, expected results, and our future work.

2 Research Plan

In this section, we present our research plan including the research goals, research contributions, and research methods. This research aims to provide possible solutions for the two main research problems (see Sect. 1) by making five main research goals (*RG*). The *RG1* is to do an in-depth study of the β-factor methodology and its evolution for a strong background knowledge and academic contribution. The *RG2* is to propose a β-factor methodology built over the IEC 61508 standard methodology, that could adopt additional defense measures and estimate β without the need for historical failure data. For *RG3*, we plan to demonstrate a way to develop industry-specific β-factor methodology focusing on the railway industry, by analyzing the needed defense measures from the insights of railway practitioners. In *RG4*, we planned to do a railway case study by adopting the developed railway-specific β-factor methodology and IEC 61508 standard methodology and compare their β-factor estimations. In *RG5*, we plan to study the Electro-dynamic braking of a railway-propulsion system, the CCF analysis of the system, and how the β-factor estimation is performed by the industry and conduct an experimental study using our developed methodology.

2.1 Research Goals

In this research, we made five main research goals (RG), and we discussed each goal in this section.

- **RG1 - Systematic study of β-factor methodology:** The industries like nuclear and railways adopted the β-factor methodology for CCF analysis. However, there is a lack of studies in the literature focusing entirely on this methodology. Hence, we aim to do an in-depth analysis of the evolution of the β-factor methodology (see Sect. 2.3).
- **RG2 - Proposal of a new generic β-factor methodology:** The IEC 61508 standard suggested a β-factor methodology which estimates β based on the applied CCF defense measures. However, the challenge is that the methodology was from 2010, and the measures concerning newly evolved technologies are not included. Moreover, there is no way to permit them. Hence, to overcome this challenge we proposed a new generic methodology.
- **RG3 - Approach to develop industry-specific β-factor methodology:** We plan to develop a railway-specific β-factor methodology by conducting a survey and getting insights from the railway practitioners about the needed defense measures. Since there are no known existing railway-specific β-factor methodologies, this methodology would support practitioners in estimating appropriate railway-specific β-factor value.
- **RG4 - Evaluation and comparison of two β-factor estimation methods:** We plan to compare the developed railway-specific β-factor estimation method in RG3 with the already existing methodology at the industry[1] by doing a case study of a railway sub-system. The goal is to demonstrate the positives and negatives of using both methodologies.
- **RG5 - Study of Electro-dynamic braking of railway propulsion system:** The electro-dynamic braking of railway propulsion system has the probability of CCF. Hence practitioners performed the CCF analysis and estimated the β-factor using the β-factor methodology from the IEC 61508 standard. However, the methodology has been in use for more than a decade, and practitioners determined to do a re-evaluation of this β estimation. For this purpose, we plan to do an experimental study of this system to estimate the β value using the railway-specific β-factor methodology.

2.2 Research Contributions

In this section, we present our Research contributions (RC) so far in achieving the research goals RG1 and RG2.

- **RC1:** We conducted a systematic literature review (see Sect. 2.3) for RG1 and identified 20 different qualitative and quantitative β-factor estimation methods. Our findings are published in the SEAA[2] conference [13].
- **RC2.** We proposed an enhanced IEC 61508 methodology for β-factor estimation to achieve RG2. We submitted our work for the Euro SPI conference[3] and the paper was accepted for publication in the conference proceedings.

[1] https://www.alstom.com/.
[2] https://dsd-seaa2023.com/.
[3] https://conference.eurospi.net/index.php/en/.

- We prepared PhD symposium paper for the Quatic conference[4]. Our research problem comes under the software quality concepts under the *Reliability* topic mentioned in the SWEBOK guide[5] because the research problem is all about a CCF methodology which is used as a part of the reliability assessment of safety systems including hardware and software.

2.3 Research Methods

The research methods (RM) that we planned to adopt to achieve our research goals are discussed in this section.

- **RM1 - Systematic Literature Review:** We conducted the *Systematic Literature Review* proposed by Kitchenham and Charters [9] to achieve RG1. This methodology supports identifying the existing β-factor estimation methods in the literature studies.
- **RM2 - Design Science Methodology:** We proposed a methodology for enhancing the β-factor methodology of the IEC 61508 standard following the guidelines of *Design Science Methodology* [15].
- **RM3 - Survey:** We plan to conduct *Survey Methodology* in the process of achieving RG3, by following the survey guidelines in software engineering [11] to get insights from the railway practitioners regarding the applicable defense measures against the CCF.
- **RM4 - Case Study:** We plan to perform *Case Study Research* to achieve the RG4 by following the guidelines of conducting and reporting case study research in software engineering [14]. This case study planned to analyze the applicability of two different β-factor methodologies.
- **RM5 - Experimental Study:** The research method chosen for achieving the RG5 is the *Experimentation* following the guidelines proposed in [16]. Experimentation is planned for the Electro-dynamic braking of the railway propulsion system to analyze their CCF and β-factor estimation.

3 State-of-the-Art

In the literature, many studies discussed the β-factor estimation using qualitative approaches. These approaches are based on the analysis of the defense measures and the β-factor quantification is made by assigning the values to the defense measures. For example in the [8], the values are assigned to the defense measures based on experiences from the past. In [6], the defense measures are weighted with five different values, and the β-factor is estimated based on the applicability of those measures. In the [2], defense measures are analyzed by establishing 37 checklist questions and assigning values based on the engineering judgment to estimate the β. All these studies evolved between 1987–2010, and the defense measures considered in the studies are assigned with certain pre-defined values

[4] https://2024.quatic.org/phd-symposium-sedes.

[5] https://www.computer.org/education/bodies-of-knowledge/software-engineering.

based on the engineering judgment to use in the quantification of β. For this reason, we are incapable of including/excluding needed defense measures as per the industry-specific requirement. In this context, a recent study [12] evolved based on the IEC 61508 standard which considered the additional defense measures considering the latest technologies. However, the scores assigned for the measures in this methodology are based on past nuclear power plant failure data. In contrast to these studies, in our research, we assigned the values to the defense measures in a simpler way according to their applicability in the system by making a checklist questionnaire, and no historical failure data was used. This would be beneficial in including additional defense measures against the CCF. This is also useful for industries that lack historical failure data and intend to develop domain-specific β-factor methodology.

4 Time Plan

The time plan is made for the entire PhD considering the spring term and autumn terms of each year between 2022 and 2026. We made a brief time plan (see Table 1) with the conducted and planned research activities. The spring term refers to the time between mid-January to the beginning of June and the autumn term refers to the time between the beginning of September to mid-January. The research work has been funded by the Knowledge Foundation[6] within the framework of INDTECH Graduate School.

4.1 Preliminary Results

The preliminary results of our research are identified in RC1 and RC2 (see Sect. 2.2). Our main research revolves around the β-factor methodology identified in the IEC 61508 standard. However, proper background details of the β-factor methodology are absent in the standard and there is also a lack of research studies that explicitly focus on this methodology. Hence, we aim to conduct a systematic literature review of β-factor models and identify 20 types of β-factor models that provide us with a strong background knowledge to achieve the research goals and contribute to RC1. Based on the knowledge gained from RC1 about the historical evolution of the β-factor methodology and the pros & cons of different identified methodologies. We proposed a methodology that enhances the IEC 61508 standard β-factor methodology and serves as a generic method that could adopt new defense measures easily and contribute to RC2. This RC2 provides a solution to our RP1 (see Sect. 1).

4.2 Future Work and Expected Results

Expected Results: The expected results would be our expected contributions RC3, RC4 and RC5.

[6] https://www.kks.se/en/start-en/.

Table 1. Timeline

Timeline		
Year	Research Activities - Spring term (ST) and Autumn term (AT)	Research Contributions and Expected outcomes
2022	ST. Setting the research goals AT. Research Planning and the start of writing the research paper A	Finalized research goals and initiated research paper A to do a systematic literature review of β-factor models
2023	ST. Writing and submitting paper A for the SEAA conference AT. Presented Paper A at the conference and it was published in IEEE Xplore Digital Library	Presented paper A at the SEAA conference in Albania Publication of paper A "A Systematic Review of β-factor Models in the Quantification of Common Cause Failures"
2024	ST. For RG2, worked on paper B and submitted it for the EuroSPI conference and submitted PhD symposium paper for Quatic conference AT. Plan to present paper B and symposium paper at conferences, plan to work on paper C for RG3, and prepare the Licentiate proposal	Submitted paper B "A Proposal for Enhancing IEC 61508 Methodology for the β-Factor Estimation" for Euro SPI conference and got accepted Submitted PhD symposium paper "Facilitating β-factor estimation for Common Cause Failures of safety-related system" to Quatic 2024 conference Submission of paper C "Development of railway-specific β-factor methodology"
2025	ST. Writing Licentiate thesis and preparing paper D for RG4 AT. Writing paper E for RG5 and preparation for the licentiate defense seminar	Submission of paper D - "Evaluation and comparative analysis of two β-factor estimation methodologies - A case study" The public defence of my Licentiate thesis
2026	ST. Writing paper E and submitting it to a conference, preparing PhD proposal AT. Completion of writing PhD thesis, making the future goals, and presentation of PhD defense seminar	Submission of paper E - "β-factor estimation of electro-dynamic braking in railway-propulsion system" Completion of writing the PhD thesis The public defense of Doctoral thesis work

- **RC3 -** In this, we would propose a railway-specific β-factor methodology by analyzing the needed defense measures for railway applications from the insights of railway practitioners by conducting a survey.
- **RC4 -** In this, we would do a comparison of the developed railway-specific methodology in RG3 with the already existing methodology in the industry through a railway case study and demonstrate the results.
- **RC5 -** In this, we would do an experimental study of the Electro-dynamic braking of a railway-propulsion system and its β-factor estimation by adopting our developed railway-specific β-factor methodology.

Future Goals: Two main future goals would add benefit to our research and be beneficial, especially for the railway industry.

- **FG1 - Project on CCF data collection focusing railways:** The collection of CCF data of railway sub-systems and maintaining its database would be beneficial in estimating more accurate β-factor values. Industries like nuclear plants have sources like [10] that provide information on how the

CCF data is gathered and evaluated. The nuclear industry also has support from an ongoing project called the International Common Cause Failure Data Exchange Project, where they are collecting CCF data from different countries and analyzing methods to prevent CCF in nuclear plants. The railway industry lacks this kind of support, hence the initiation of a project for CCF data collection would be the first future goal.

- **FG2 - Development of a tool to facilitate our β- factor methodology:** The methodology we developed in RG2 facilitated by a tool would be an add-on benefit. Hence we plan to develop a tool as our second future goal.

References

1. IEC 61131-6:2012 programmable controllers - part 6: functional safety. https://webstore.iec.ch/publication/4555. Accessed 16 June 2024
2. 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 31 Mar 2024
3. IEC 62061: Safety of machinery - functional safety of safety-related control systems. https://webstore.iec.ch/publication/59927. Accessed 16 June 2024
4. Fleming, K.N.: Reliability model for common mode failures in redundant safety systems. Technical report, General Atomics, San Diego, CA, United States (1974)
5. Hokstad, P., Håbrekke, S., Lundteigen, M.A., Onshus, T.: Use of the PDS method for railway applications. SINTEF Technol. Soc. **15**, 5–23 (2009)
6. Humphreys, R.: Assigning a numerical value to the beta factor common cause evaluation. In: Reliability 1987 (1987)
7. Jin, H., Lundteigen, M.A., Rausand, M.: Common-cause failures in safety-instrumented systems. In: PSAM, vol. 11, pp. 6121–6131
8. Johnston, B.: A structured procedure for dependent failure analysis (DFA). Reliab. Eng. **19**(2), 125–136 (1987)
9. Kitchenham, B., Charters, S., et al.: Guidelines for performing systematic literature reviews in software engineering (2007)
10. MarshaU, F.U.: Common-cause failure database and analysis system: overview (1998)
11. Molléri, J.S., Petersen, K., Mendes, E.: Survey guidelines in software engineering: an annotated review. In: Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, pp. 1–6 (2016)
12. Park, J., Park, K., Lee, C.J.: The development of a common cause factor score table on IEC 61508 Part 6 Edition 2.0. J. Loss Prev. Process Ind. **68**, 105270 (2024)
13. Rao, S.B.G., Castellanos-Ardila, J.P., Punnekkat, S.: 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), pp. 262–269. IEEE (2023)
14. Runeson, P., Höst, M.: Guidelines for conducting and reporting case study research in software engineering. Empir. Softw. Eng. **14**, 131–164 (2009)
15. Wieringa, R.J.: Design Science Methodology for Information Systems and Software Engineering. Springer, Heidelberg (2014)
16. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in Software Engineering. Springer, Heidelberg (2012)