A Proposal for Enhancing IEC 61508 Methodology for the β-Factor Estimation

Sirisha Bai Govardhan Rao[1,2(✉)], Julieth Patricia Castellanos-Ardila[2], and Sasikumar Punnekkat[2]

[1] Alstom, Västerås, Sweden
sirisha.bai.govardhan.rao@mdu.se
[2] Mälardalen University, Västerås, Sweden
{julieth.castellanos,sasikumar.punnekkat}@mdu.se

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 evolution regarding both new technologies with an impact on the system dependency factors, as well as 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 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 CCF reduction. The rationale is that the more defenses are addressed, the more protection can be achieved against CCF.

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

1 Introduction

The common cause failure (CCF), i.e., simultaneous components failure resulting from a single cause [3], can lead to system failure in redundancy systems. In particular, dependency factors, i.e., factors due to the multiple interactions between systems and components, lead to CCF and can appear during the design and/or manufacturing of the components or the systems. Therefore, they must be quantified and mitigated during risk assessment of safety systems.

This Research has been supported by the Knowledge Foundation (KKS) in collaboration with Alstom and Mälardalen University.

M. Yilmaz et al. (Eds.): EuroSPI 2024, CCIS 2179, pp. 300–314, 2024.
https://doi.org/10.1007/978-3-031-71139-8_20

Several models have been proposed to quantify CCF. For example, the *Binomial Failure Rate model* [16], in which the occurrence of CCF is compared with the shock to the components and the failure rate due to this shock is assumed as random with binomial distribution. Another model is an *α-factor model* [12], where the α-factor is the fraction of events involving the failure of k out of m redundant components due to a shared cause. Even though there are many such CCF models, the most known and widely used model is the *β-factor model*, which can be estimated using qualitative or quantitative methodologies [13].

The β-factor in quantitative models is estimated using numerical data regarding CCF collected over the years. In fact, the first β-factor model, called BMF [7], was created considering such historical data. In the qualitative models, the β factor requires the assessment of defense measures, i.e., practices done to mitigate the CCF against system dependencies. The methodology adopted in the IEC 61508-6:2010 [3] (we called, *the core methodology*) is a qualitative model that contains 37 checklist questions covering 8 defense measures. Each question has assigned numerical values selected by the presence (or lack) of a diagnostic test, which is a test used to detect dangerous failures (i.e., failures that result in an unsafe and hazardous state). The values are collected once the questions are answered, and the β-factor is calculated using specific formulas. The core methodology has been used since the standard was released in 2010. However, different aspects leading to CCF have been studied and formulated in different contexts that also have relevance in calculating the β-factor.

In this paper, we propose a methodology to estimate the β-factor by adding 33 checklist questions to the already proposed core methodology. For this, we use the design science methodology for information systems and software engineering [17]. Such methodology is suitable for the design of artifacts that call for a change in the real world. In particular, we analyze the CCF problem and consider that the checklist provided in the core methodology is an artifact that can be complemented with a broader range of questions that can be used to reason about CCF's causes. Those questions (collected from state of the art, i.e., [1, 8–11, 15]) mostly relate to human dependency factors and programmable controllers, which are not considered in the core methodology. We also propose an approach for estimating the β-factor that makes inclusion of additional questions possible. The proposed estimation method includes two additional parameters, i.e., the level of defense support (low, medium, or high) from each defense measure and the impact of the safety culture (strong, moderate, or poor). Finally, we apply our developed β-factor methodology to a realistic system and discuss the findings. As a result, we can provide recommendations for those factors that are not fulfilled so the system can evolve safely, i.e., with less probability of CCF. The rationale is that the more defenses are addressed, the more protection can be reached against CCF.

The paper is structured as follows. In Sect. 2, we present essential background. In Sect. 3, we present our proposed methodology. In Sect. 4, we present an illustrative example. In Sect. 5, we discuss our findings. Finally, in Sect. 6, we present our conclusions and future remarks.

2 Background

In this section, we provide information regarding the estimation of β-factor and defense measures.

2.1 β-factor Estimation

The core methodology provided in the standard IEC 61508-6:2010 [3], includes 37 checklist questions, which are related to 8 dependency sub-factors (see in Sect. 2.2). Each checklist question has a set of assigned values, which practitioners choose by the presence or lack of a diagnostic test, i.e., the test that detects dangerous failures in a system. A dangerous failure is revealed and can be considered safe only if effective measures, automatic or manual, are taken. The user of the core methodology determines the β-factor, i.e., the fraction of unit failures that are common mode, by adding up overall gained values according to the answers to those checklist questions. The parameters considered in this equation are 'β' and 'λ'. 'λ' is the probability of system failure rate, given by the number of failures over a period of time (see Eq. (1)). 'λ' is a parameter that considers two different rates, 'λ_1', which is the rate related to independent failures, i.e., failures that do not affect other components in the system (see Eq. (2)), and 'λ_2', which is the rate related to the common cause failure (see Eq. (3)).

$$\lambda = \frac{\text{number of failures}}{\text{part - hours of operation}} \tag{1}$$

$$\lambda_1 = (1 - \beta)\lambda \tag{2}$$

$$\lambda_2 = \beta\lambda \tag{3}$$

As we saw, the core methodology considers diagnostic tests, which discover dangerous detected failures (DD). However, there are also dangerous undetected failures (DU), in which there is no diagnostic test. Therefore, the final CCF rate, called by the standard λ_{CC} is determined by considering the Eq. (4), which splits the β-factor (i.e., into β and β_D, where β is the CCF factor for undetectable dangerous failure and β_D is the CCF factor for detectable dangerous failure) according to the diagnostic test (i.e., λ_{DU} and λ_{DD}).

$$\lambda_{CC} = \lambda_{DU}\beta + \lambda_{DD}\beta_D \tag{4}$$

2.2 Defense Measures

The dependencies between the redundant components lead to a CCF event, which affects the system's redundancy. Hence to mitigate the CCF, different defense measures are considered in the literature (i.e., [1, 3, 6, 9, 11, 15]) which is listed below.

1. **Separation/Segregation:** It refers to the physical separation of redundant units, for example, two cameras sensing the same event are positioned in separated boxes in the system.

2. **Diversity/redundancy**: It refers to the different approaches used to address the replication of components in a safety system, for example, how the redundant units are managed during design and construction by considering different teams working on them or the technology used.
3. **Complexity/design/application/maturity/experience:** The adopted designs and techniques for redundant systems that have been used successfully for a longer time have less probability of CCF (*maturity*). A system with fewer inputs/outputs (*complexity*) and their protection from potential levels of over-voltage and current (*application*) will likely lead to a lower probability of CCF. The *experience* with the same hardware in similar environments would be an addition.
4. **Assessment/analysis and feedback of data:** It refers to the study of past failures and performing the present needed reviews. For example, having discussions with the designers to eliminate the CCF by adopting possible changes in the design and analyzing the field failures from previous projects.
5. **Procedures/human interface:** The sequence of tasks that refers to procedures should be properly written with details, for example, the installation instructions and maintenance procedures. The human interaction with the system also needs to be minimized or carefully done.
6. **Competence/training/safety culture:** The staff in the industry like operators, maintainers, and designers need to be properly trained regarding emergency operations and also to guide on CCF and their preventive measures. The competence refers to the stakeholders like operators, and designers' familiarity with the system.
7. **Environmental control:** The range of temperature, corrosion, vibration, and other crucial factors in which the system probably operates need to be tested to know if it is within the range and specification of environmental conditions during the system development.
8. **Environmental testing:** The system needs to be tested under environmental conditions like temperature, corrosion, dust, and other impacting factors to reveal common cause susceptibilities and withstand their environmental effects. For example, performing the type tests i.e., qualifying a component from the testing of one or more similar types of components.

2.3 A β-factor Methodology Focusing Industry's Safety Culture

The first step in this methodology [8] is the estimation of the Maximum Common Cause Value (MCCV) i.e., the maximum industry β-factor assumed based on judgment and experiences. The MCCV is estimated by considering factors related to the industry i.e., its safety culture, failure history, management effectiveness, maintenance program, training, budget, and schedule constraints. In particular, the MCCV is lowest at 10% if the industry has a strong safety culture. It is 20% for the industries with moderate safety culture practices, and it is highest at 30% for the industries with poor safety culture. The second step in this methodology is the calculation of the Common Cause Score (CCS). Each defense measure (called a sub-factor in this methodology) provides different levels of support and is categorized under low, medium, and high. Later, the total number of defenses under each level should be added and assumed as N_{low}, N_{medium}, and N_{high} which are multiplied by some pre-defined values. The total Common Cause Score (CCS)

is then calculated using the following equation:

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

The maximum possible CCS would be assumed as T in the equation. Then β in this methodology is estimated using the following equation:

$$\beta = \frac{\text{CCS}}{\text{T}} * MCCV \tag{6}$$

3 Proposed Methodology

In this section, we propose a methodology by enhancing the core methodology for estimating the β-factor by considering additional defense measures and checklist questions to the already existing ones. For this, we consider the Design Science Methodology for Information Systems and Software Engineering [17], which considers that a research problem (see Sect. 3.1) could be improved with the proposition of a design artifact (see Sect. 3.2).

3.1 Research Problem

The core methodology provides 8 defense measures in the form of 37 checklist questions with some predefined values. Based on the answers to those questions, the β-factor is estimated (see Sect. 2.1). Such methodology has been used since the standard was released in 2010. However, different aspects leading to CCF have been studied and formulated in different contexts (see Sect. 2.2) that also have relevance in estimating the β-factor. We consider that such aspects shall also be included. The problem with the core methodology is that there is no scope to include more questions to the checklist to extend defenses against the occurrence of CCF because there is no information on what basis the values are assigned to each question. Hence an estimation method that opens room for the inclusion of all different defense measures has to be provided. For doing this, we are using the same formula provided in Sect. 2.3 (see Eq. (6)). In addition, to make the calculation more easy to grasp for practitioners, we provide an assessment method for CCS.

3.2 Research Artifact

Our research artifact comprises two parts: an extended checklist and an applicable estimation method for the β-factor. We defined the goal for the artifact that follows the template of the Design Science Methodology (see [17]) as follows:

> *Improve* ***the handling of CCF***
> *by* ***enhancing the methodology for the β-factor estimation***
> *that is* ***flexible, up-to-date, and more comprehensible***
> *in order to* ***help practitioners to reason about a larger set of defense measures improving the estimation as well as development of industry-specific β-factor estimation methodologies.***

A. **Creation of the checklist** There are four steps in the checklist creation.
   1. **Collection of qualitative methodologies:** We collected qualitative β-factor methodologies found in the state of the art (See Sect. 2.2). All the collected information is maintained in Excel sheets[1].
   2. **Identification of dependency factors:** From the collected sources, we identify a total of 11 types of dependency factors. We removed the ones that were repeated and made groups with the related ones. As a result, we obtained a final set of 5 dependency factors, i.e., physical (which includes design and construction of the system), operational (which includes procedures), environmental, functional, and human dependency factors.

Table 1. 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

   3. **Identification of defense measures:** A total of 74 defense measures were identified from all the sources. After filtering and grouping, we obtained a total of 10 defense measures, i.e., separation, diversity, design control, experience, safety assessment, procedures, diagnostic testing, training, environmental control, and environmental testing, that were allocated to the dependency factors as presented in Table 1.
   4. **Identification of checklist questions:** Finally, the identified checklist questions from all the sources were gathered. The same type of questions, i.e., with the same content and different phrases, are removed. Later, they are grouped under the respective defense measures, as presented in Table 2.

B. **β-factor estimation** Fig. 1, presents the process required in the estimation of the β-factor, which are grounded on the methodology presented in Sect. 2.3.

Step 1: Identify Redundancies. Identify the system for which the CCF has to be assessed and find out the responsible stakeholders.

Step 2: Study the Safety Culture. The perceived safety culture is used to assign the MCCV value, i.e., poor (30%), moderate (20%), or strong (10%).

Step 3: Fill the checklist. The checklist questionnaire is filled. Every question has three choices, i.e., *yes* if the question is applied in the system, *no* if the question is not

[1] https://rb.gy/qwev3k

Table 2. Checklist Questions

ID	Checklist question
S	**Separation**
S1	*Are all signal cables for the channels routed separately at all positions?*
S2	*Are the logic subsystem channels on separate printed circuit boards?*
S3	*Are the logic subsystems physically separated effectively?*
S4	*Does the sensors/final elements have dedicated control electronics, are the electronics for each channel on separate printed-circuit boards?*
S5	*Do the sensors/final elements have dedicated control electronics, are the electronics for each channel indoors and in separate cabinets?*
S6	*Are all power cables separate at all positions?*
S7	*Do the redundant components are physically separated?*
S8	*Are all channel elements enclosed in separate shielded enclosures?*
S9	*Are separate and independent I/O data buses used for each channel?*
S10	*Are redundant sensors adequately physically separated?*
S11	*Is there sufficient independence of hardware manufacturer?*
S12	*Do the redundant systems develop from separate requirements by distinctly different design groups with independent testing and design verification teams?*
S13	*Is the maintenance on each channel carried out by different people at different times?*
S14	*Does there is full independence of supplies?*
S15	*Does there is full independence of maintenance?*
D	**Diversity**
D1	*Do the channels employ different electrical technologies? for example, one electronic or programmable electronic and the other relay?*
D2	*Do the channels employ different electronic technologies? for example, one electronic, the other programmable electronic?*
D3	*Do the devices employ different physical principles for the sensing elements? for example, pressure and temperature, vane anemometer and doppler transducer, etc?*
D4	*Do the devices employ different electrical principles/designs? for example, digital and analog, different manufacturers (not re-badged), or different technology?*
D5	*Is medium diversity used, for example, hardware diagnostic tests using different technology?*
D6	*Is low diversity used for example hardware diagnostic tests using the same technology?*
D7	*Do the channels employ deliberate temporal differences in functional operation (temporal diversity) to reduce the risk of coincident failures?*
D8	*Is different separately developed embedded software employed in different channels?*
D9	*Does the industry ensure diversity in maintenance procedures?*
D10	*Are separate test methods used for each channel during commissioning?*
D11	*Are separate people used for each channel during commissioning?*
DC	**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?*

(*continued*)

Table 2. (*continued*)

ID	checklist question
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?*
P	**Procedures**
P1	*Are the procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?*
P2	*Does the documented maintenance specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?*
P3	*Is the industry subject to strict government oversight and regulation?*
P4	*Do the procedures meet exceedingly well-defined standards?*
P5	*Does it follow construction standards?*
P6	*Is personnel access limited (for example locked cabinets, inaccessible position)?*
P7	*Does there is a written system of work to ensure that all compon ent failures (or degradation) are detected, the root causes established, and other similar items inspected for similar potential?*
P8	*Does there is an active problem reporting and analysis program for the system?*
P9	*Is the analyzed data effectively communicated to the design engineers and managers, where the insights used to make appropriate changes in the design, operational procedures, and training programs?*
E	**Experience**
E1	*Does the operator have more than 10 years of operating experience with the system?*
E2	*Does the designer have a variety of technical background and experience?*
E3	*Do the FS-PLC designers have previous experience in eliminating common-cause failures?*
SA	**Safety Assessment**
SA1	*Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?*

(*continued*)

Table 2. (*continued*)

ID	checklist question
SA2	*Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?*
SA3	*Do the field failures fully analyze with feedback into the design? (Documentary evidence of the the procedure is required.)*
SA4	*Are all devices/components conservatively rated (for example, by a factor of 2 or more)?*
DT	**Diagnostic Testing**
DT1	*Does the maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair center, and have all the repaired items gone through full pre-installation testing?*
DT2	*Do the system diagnostic tests report failures to the level of a field-replaceable module?*
DT3	*Are inputs and outputs protected from potential levels of over-voltage and over-current?*
DT4	*Are the diagnostic tests of one channel independent of the operation of another channel?*
DT5	*Does the system have diagnostic coverage and report failures to the level of a field-replaceable module?*
T	**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?*
EC	**Environmental Control**
EC1	*Is the same hardware used in similar environments for more than 5 years?*
EC2	*Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?*
ET	**Environmental Testing**
ET1	*Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?*
ET2	*Have external causes of CCF been identified (e.g. fire, vehicle impact, lightning, etc.)?*

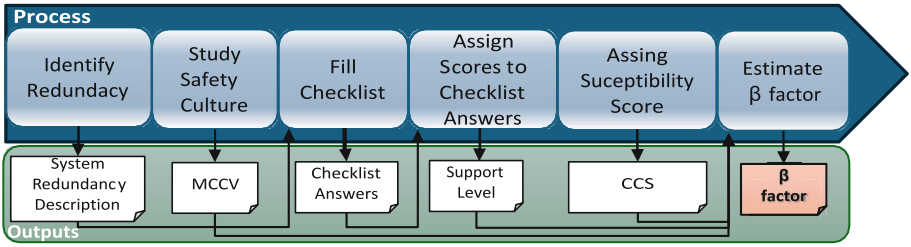

Fig. 1. β-factor Estimation Process

applied in the system, and *not applicable* if the question is not applicable for the system). The values assigned to the answers are 1 for *yes*, 0 for *no*, and 1 for *not applicable*. The value assigned to the not applicable option is the same as the answer yes because such values do not make any difference for the CCS score. As an exception, we have question DT5 (see Table 2 under Diagnostic Testing), which has four different options. First, *low diagnostic coverage* (60% to 90%), whose value is 0.25. Second, *medium diagnostic coverage* (90% to 99%), whose value is 0.50. Third, *high diagnostic coverage* (>99%), the value is 1. For not applicable, the value is 1.

Step 4: Assign Scores to Checklist Answers. We assign scores to answers according to the previous step. The maximum score of each defense measure is the number of questions it possesses. The support level can be *low* (the score is less than half of the maximum score), *medium* (the score is between half of the maximum score and the maximum score), or *high* (the score is equal to maximum score) based on the total score gained from the answers.

Step 5: Assign the Susceptibility Score. We assign a susceptibility score of 1, 5, or 10 for the total assessed level of defense support (high, medium, low) identified in the previous step. The total common cause susceptibility score (CCS) is a sum of the product of the total number (N) of defense measures from each level and the assigned susceptibility score (see Eq. (7)).

$$CCS = 10.N_{low} + 5.N_{medium} + 1.N_{high} \tag{7}$$

Step 6: Estimate β-factor. The maximum CCS, called T, can occur if all defense measures provide low support. In our methodology, which provides 10 defenses, the maximum T equals 100 (10 defenses multiplied by 10, which is the susceptibility score for the lowest support). This value changes if more defense measures are included in the methodology. The β-factor value is estimated using Eq. (8).

$$\beta = \frac{\text{CCS}}{\text{T}} * MCCV \tag{8}$$

4 Illustrative Example

We consider a fictitious but realistic system called a High-integrity Pressure Protection System (HIPPS) and use it to illustrate our methodology (See Fig. 1). This system is used, for example, in petrochemicals to protect from overpressure.

4.1 Identify Redundancy

There are mainly three subsystems in HIPPS [14]. One of them is pressure sensors which is redundant and configured with 2oo3 redundancy (see Fig. 2). However, the CCF event may affect the redundancy and cause overall system failure. Hence, there is a need to evaluate the probability of CCF for this system.

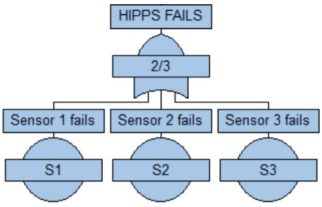

Fig. 2. Fault Tree of HIPPS

4.2 Study of Safety Culture

The industry's safety culture in which this system has been in use is perceived as following a strong safety culture. Hence, the assigned MCCV is 10%.

4.3 Fill Checklist

The checklist questions provided in Table 2 for each defense measure have to be filled. However, in this example, we are filling the answers of only one defense measure i.e., *separation*. It is shown in Table 3.

4.4 Assigning Scores to Checklist Answers

In this step, we are assigning scores to the answers. Here, we considered only one defense measure and their answers (see Table 3). For the remaining defense measures, we are taking half of the maximum scores of their sensor-related questions. For the questions related to the logic sub-system, we assume the answer is not applicable. The score gained for the defense measure separation is 15, which is equal to its maximum score. Hence the defense support provided by separation is high. The support from each defense measure is shown in Table 4.

Table 3. Checklist question & answers

S	Seperation	Answer
S1	Are all signal cables for the channels routed separately at all positions?	Yes
S2	Are the logic subsystem channels on separate printed circuit boards?	NA
S3	Are the logic subsystems physically separated effectively?	NA
S4	Do the sensors/final elements have dedicated control electronics, are the electronics for each channel on separate printed circuit boards?	Yes
S5	Do the sensors/final elements have dedicated control electronics, are the electronics for each channel indoors and in separate cabinets?	Yes
S6	Are all power cables separate at all positions?	Yes
S7	Do the redundant components are physically separated?	Yes
S8	Are all channel elements enclosed in separate shielded enclosures?	NA
S9	Are separate and independent I/O data buses used for each channel?	NA
S10	Are redundant sensors adequately physically separated?	Yes
S11	Is there sufficient independence of the hardware manufacturer?	Yes
S12	Do the redundant systems develop from separate requirements by distinctly different design groups with independent testing and design verification teams?	Yes
S13	Is the maintenance on each channel carried out by different people at different times?	Yes
S14	Does there is full independence of supplies?	Yes
S15	Does there is full independence of maintenance?	Yes

4.5 Assign Susceptibility Scores

In this step, we are assigning susceptibility scores for total identified low, medium, and high defense supports from all defense measures (see Table 4). We are assigning a low susceptibility score for high defense support i.e., 1. For medium defense support, we are assigning a score of 5 and for low defense support, we are assigning a score as 10. We then calculate the CCS using the Eq. (7).

$$CCS = 10.2 + 5.7 + 1.1 = 56 \tag{9}$$

4.6 Estimate β-factor

Finally, the β-factor is calculated in this step following the Eq. (8).

$$\beta\% = \frac{56}{100} * 10 = 5.6\% \tag{10}$$

5 Discussion

In this section, we discuss our insights from the applications of the methodology in Sect. 5.1 and the relation of our work with the SPI Manifesto in Sect. 5.2.

Table 4. Common cause scoring

Defense measure	Low	Medium	High
Separation			x
Diversity		x	
Design Control		x	
Experience		x	
Safety Assessment		x	
Procedures	x		
Diagnostic Testing		x	
Training	x		
Environmental Control		x	
Environmental Testing		x	
Sum of x	2	7	1
Scoring	10	5	1
X score (sum of x * scoring)	20	35	1
CCS (Sum of X score)			56

5.1 Methodology Insights

The insights provided in this section are mainly with the adaptability, simplicity, comprehensibility, flexibility, and adequacy provided by our methodology. In addition, we discussed the importance of safety culture and the stakeholder's involvement in our methodology.

Adaptability: Recent emerging technologies such as Artificial Intelligence, the internet of things, virtual reality, and augmented reality are creating a greater impact in all safety-critical industries. Even new rules and regulations are established for the proper adoption of these technologies concerning safety for example, a new EU Artificial Intelligence Act [2] for comprehensive regulation of AI was recently introduced by the European Union (EU). In this regard, practitioners require the adoption of additional defense measures against the probability of CCF arising from emerging technologies. For this, we provided the logic behind our scoring method to support the practitioners in adopting additional defense measures against the latest technologies.

Complexity in the β estimation: The core methodology derives two types of β, the β and β_D by considering the frequency and coverage of diagnostic tests. Whereas our methodology does not differentiate β and maintains a single β to make it less complex. However, we didn't neglect the diagnostic testing and coverage, the defense measure *DT* (see Table 2) covers checklist questions related to it and which has an impact on the estimated β value.

Comprehensibility: The core methodology considered 37 questions grouped under 8 defense measures for β estimation. However, it has not provided the details on how and why it chooses those particular number of measures. They just stated that the methodology was developed based on two sources [5, 9]. However, providing the background details would help the practitioners to develop their industry-specific methodology.

Hence in our methodology, we gave clear information on the steps (see Sect. 3.2) involved in considering the 10 defense measures and 70 checklist questions.

Adequacy of checklist questionnaire: The core methodology has not proposed many questions against human-related dependency factors. Whereas our methodology considered 12 questions (that includes training & experience-related questions). In addition, we considered a set of questions focusing on programmable controllers which are missing in the core methodology.

Safety culture: The industry's safety culture is prioritized and has an impact on the estimation of β in our methodology, whereas it is not prioritized in the core methodology.

Flexibility: In our β-factor methodology, the checklist questions have an ID (see Table 2), which facilitates flexibility in tracing them. After acquiring the answers to the checklist questions, we could tabulate the measures according to their applicability and review the questions that were not applied. This analysis provides suggestions on measures that could decrease CCF.

Involvement of stakeholders: In our β-factor methodology, we suggest the involvement of respective stakeholders (such as the designers, operators, and safety engineers) who worked with the system to answer the checklist questions that support obtaining accurate estimation.

5.2 Correspondence to SPI Manifesto

Our methodology suggested sharing checklist questions with the respective industrial practitioners to involve them for better results. This addresses principle 2 of the SPI Manifesto [4] i.e., *Motivate all people involved.* Our paper exhibits an extended checklist questionnaire and broadens the knowledge of practitioners to learn about new measures. This addresses principle 4 of the SPI Manifesto [4] i.e., *create a learning organization.* Our methodology was made in such a way that it is easily adaptable and could be modified to develop further as per the industry concerns. This addresses principle 6 of the SPI Manifesto [4] i.e., *use dynamic and adaptable models as needed.*

6 Conclusion & Future Work

In this paper, we proposed a methodology for enhancing the β-factor estimation proposed in the standard IEC 61508-6:2010. In particular, we added more defense measures and a new formulae for the estimation method. Such a method opens room for the inclusion of more questions that cover new defense measures, which can arise in different contexts, especially when technology evolves. Our methodology would serve as a base for developing industry-specific β-factor methodologies, which have their specific dependency factors.

In the future, we plan to evaluate the proposed methodology by considering case studies from different industries and comparative studies that include different β-factor methodologies. We will also consider practitioners' opinions regarding the current state of our methodology, which will help us evolve it in different directions, e.g., context-specific applications as well as the introduction of CCF from emerging technologies. Tools for supporting practitioners in the use of our methodology are planned to be investigated.

References

1. EN 61131: Programmable controllers – part 6: Functional safety. http://tinyurl.com/422tnhz8. Accessed 27 January 2024
2. EU Artificial Intelligent Act. https://rb.gy/8tsmgm. Accessed 04 June 2024
3. 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 21 March 2024
4. The SPI Manifesto. https://conference.eurospi.net/images/eurospi/spi_manifesto.pdf. Accessed 11 March 2024
5. Brand, V.: UPM 3.1: a pragmatic approach to dependent failures assessment for standard systems. AEA Technology (1996)
6. Evans, M., Parry, G., Wreathall, J.: On the treatment of common-cause failures in system analysis. Reliab. Eng. **9**(2), 107–115 (1984)
7. Fleming, K.N.: Reliability model for common mode failures in redundant safety systems. Tech. rep. General Atomics, San Diego, CA (United States) (1974)
8. Hark, F., Ring, R., Novack, S.D., Britton, P.: Common cause failure modeling in space launch vehicles. In: International Association for the Advancement of Space Safety (IAASS) Conference No. M16-5258 (2015)
9. Humphreys, R.: Assigning a numerical value to the beta factor common cause evaluation. Reliability (1987)
10. Johnston, B.: A structured procedure for dependent failure analysis (DFA). Reliab. Eng. **19**(2), 125–136 (1987)
11. Martin, B., Wright, R.: A practical method of common cause failure modeling. Reliab. Eng. **19**(3), 185–199 (1987)
12. Mosleh, A.: A multi-parameter, event-based common-cause failure model. SMiRT9 Paper No. M7/3 (1987)
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. Sotoodeh, K.: High integrity pressure protection system (HIPPS) usage justification from safety and reliability point of views. Saf. Extreme Environ. **3**, 43–50 (2021)
15. Summers, A.E., Ford, K.A., Raney, G., et al.: Estimation and evaluation of common cause failures in SIS. Chemical Engineering Progress (1999)
16. Vesely, W.: Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specializations. Nucl. Syst. Reliab. Eng. Risk Assess. **2**, 314–341 (1977)
17. Wieringa, R.J.: Design Science Methodology for Information Systems and Software Engineering. Springer (2014)