An extension to the Alpha Factor method for enhanced common cause failure analysis

Mina Torabi[a,*], Marko Čepin[b]

[a] *National Centre for Nuclear Research (NCBJ), A. Sołtana 7, 05-400 Otwock, Poland*
[b] *University of Ljubljana, Faculty of Electrical Engineering, Tržaška 25, 1000 Ljubljana, Slovenia*

Abstract

Common cause failures occur when multiple components fail simultaneously due to a shared cause, and can significantly increase the overall probability of system failure. Therefore, it is essential to consider them in reliability and safety assessments, particularly for redundant systems in which components often share design, operational, or maintenance characteristics. The main objective of this work is to develop an advanced Alpha Factor method to enhance the assessment of common cause failures. One of the main drawbacks of the existing Alpha Factor method is that each component is limited to a single common cause failure group. The proposed method overcomes this limitation by allowing components to be assigned to multiple groups. The new method is applied to a simplified, yet representative, redundant safety system, and the corresponding results highlight the significant impact of common cause failures on system failure probability when analyzed through the proposed approach.

Keywords: Common cause failures, Alpha Factor method, Fault tree, Redundant systems, Containment spray system

1. Introduction

The safety and reliability assessment of nuclear power plants is a critical procedure during the design phase, licensing, and throughout their operational lifetime. This procedure can help to ensure a long term operation and to minimize severe damages during abnormal operating conditions. Additionally, due to the high safety demand standards in nuclear power plants, it is essential to implement a robust safety and reliability analysis procedure. Probabilistic safety assessment is one of the most widely used procedures for assessing and managing safety and reliability across various industries, particularly in nuclear power plants. This approach incorporates various techniques for modeling and quantifying potential failure scenarios and their consequences, including fault tree analysis, event tree analysis, and failure modes and effects analysis, among others [1, 2].

*Corresponding author.
Email addresses: mina.torabi@ncbj.gov.pl (Mina Torabi), marko.cepin@fe.uni-lj.si (Marko Čepin)

In this paper, the focus is on failure analysis of systems using the fault tree analysis technique, which is primarily used to systematically evaluate failure mechanisms at both the system and subsystem levels. It provides a structured graphical framework for identifying and evaluating the combinations of failures leading to undesired system or subsystem events. In the fault tree model, the components failures are often considered as independent events. However, in complex engineered systems, this assumption is frequently challenged due to the presence of common cause failures [3, 4].

Common cause failures represent a specific category of dependent failure events wherein multiple components fail simultaneously due to a shared cause. These failures can substantially reduce overall system reliability [4] and are particularly prevalent in redundant systems, where there exist multiple shared characteristics across identical components. Therefore, although redundancy is intended to enhance safety and ensure compliance with reliability standards in safety-critical industries (such as nuclear power, aerospace, and chemical processing), common cause events can undermine this advantage and significantly increase the overall probability of system failure [5, 6]. Detailed assessment of these failures is therefore essential for a comprehensive safety evaluation, especially in highly redundant systems [7–9]. Moreover, the recognition and detailed modeling of common cause failures are crucial for determining optimal system configurations [10], and can also influence the prioritization of components and systems based on importance measures [11].

There are several models for addressing common cause failures in safety and reliability studies. Among the most commonly used are the Beta Factor, Multiple Greek Letter, and Alpha Factor methods [12–14]. Notably, the Alpha Factor and Multiple Greek Letter methods provide a more detailed evaluation of common cause failures compared to the Beta Factor method. Some studies have proposed extensions to these methods to allow for more advanced analysis of common cause failures. For example, improved Beta Factor and Multiple Greek Letter methods that account for multiple shared causes were developed by Kančev and Čepin [15] and by Bricman Rejc and Čepin [16], respectively. The Partial Alpha Factor Model was introduced as an extension of the conventional Alpha Factor method for explicitly incorporating coupling factors (e.g., shared maintenance or location) between components [17]. The General Dependency Model enhances the parametric methods by introducing cause-specific parameters, such as cause condition probability, component fragility, and coupling factor strength, to model probabilistic dependencies among components using a Bayesian Network [18].

Despite advancements in common cause failure modeling, the Alpha Factor method retains certain limitations. One such limitation is the simplifying assumption that each component can be associated with only one common cause failure group. A common cause failure group is a set of components that fail together due to the same cause. This limitation prevents the modeling of scenarios in which a component may share multiple common characteristics with different groups of components. The aim of this work is to develop an advanced Alpha Factor method that allows a component to be associated with multiple common cause failure groups. The applicability of the new method is demonstrated through a case study on a safety system, namely the containment spray system of an advanced pressurized water reactor nuclear power plant. This example pertains to a single-unit reactor. However, the proposed approach features the flexibility to be applied to multi-unit reactors, where shared systems across units introduce the potential for inter-unit common cause failures [19, 20].

In addition to the proposed Alpha Factor method, we derive a general equation for calculating the failure probability of redundant systems affected by common cause failures, which is applicable to any redundancy level. We also perform a sensitivity analysis to investigate how variations in individual component failure probabilities and system redundancy levels influence the contribution of common cause failures.

The structure of this paper is as follows. Section 2 provides an overview of the relevant reference methods, including fault tree method, the common cause failures and their implementation within the fault tree model, and Alpha Factor method. Section 3 introduces a new formulation for quantifying the failure probability of redundant systems while accounting for common cause failures. Section 4 presents a sensitivity analysis to investigate how variations in component failure probability and redundancy level affect the contribution of common cause failures to the overall system failure probability. Section 5 presents the new Alpha Factor method as an enhanced approach to common cause failure analysis. Section 6 presents the results of a case study demonstrating the application and effectiveness of the proposed approach. Finally, the paper concludes in Section 7 with a summary of the key findings.

2. Background

2.1. Fault tree analysis

Fault tree analysis is a systematic and commonly used tool within Probabilistic Safety Assessment (PSA) to investigate component and system failures. The fault tree analysis is initiated by defining an undesired top event which represents a system failure. Then, the smallest failures that may lead to the top event, known as Basic Events (BEs), are identified. These BEs are connected to the top event through logical gates. In order to quantify system failure, component failure evaluation is performed by defining failure rates based on historical or empirical data. These rates are commonly calculated as the ratio of the number of failures to the total operational time, or as an inverse of mean time to failure.

Since each component may exhibit multiple failure modes, fault tree analysis focuses on identifying and modeling only those specific modes that contribute to the system failure. Each relevant failure mode is included in the model along with its associated probability. Consequently, the overall failure probability of a component is obtained by aggregating the probabilities of all considered failure modes.

Fault tree analysis provides both qualitative and quantitative failure assessments at the system, subsystem, and component levels. These assessments are derived from equivalent Boolean equations that represent the logical combinations of basic failure events leading to the top level system failure [1, 21]. In the qualitative phase, the analysis aims to identify Minimal Cut Sets (MCSs). Each MCS represents the smallest combination of component failures that, if they occur simultaneously, will result in system failure. These MCSs are identified using Boolean minimization technique which simplify the logical expression of the fault tree by eliminating redundant terms. An MCS consisting of a single BE is referred to as a single MCS; those with two, three, and four BEs are known as double, triple, and quadruple MCSs, respectively. As the number of BEs in an MCS increases, the probability of system failure decreases, since a larger number of events are required to cause the system failure. In the quantitative analysis of a fault tree, the probability of the top event is calculated by evaluating the probability of each MCS.

For complex systems, fault trees may contain a large number of MCSs, many of which contribute negligibly to the overall top event probability. In order to manage computational complexity and maintain practical applicability, a truncation limit is typically applied to exclude low probability MCSs. Selecting an appropriate truncation threshold is critical for ensuring the accuracy of the results. A too large threshold may neglect critical MCSs, which introduces errors on importance risk measures. On the other hand, a too small limit increases the computational effort without a significant gain in precision. Thus, adopting an optimized truncation limit can improve the accuracy of risk assessments [22]. With a suitable truncation limit in place, the top event probability is evaluated using the inclusion-exclusion principles, as outlined below.

Let us assume that the system failure is represented by a set of MCSs, $\{\mathrm{MCS}_1, \mathrm{MCS}_2, \ldots, \mathrm{MCS}_L\}$, where L denotes the total number of MCSs. Each MCS_i comprises n_i basic events, where the j-th basic event within MCS_i is denoted by BE_{ij}. The structure of each MCS_i is thus defined as follows.

$$\mathrm{MCS}_i = \{\mathrm{BE}_{i1}, \mathrm{BE}_{i2}, \ldots, \mathrm{BE}_{in_i}\}, \quad i = 1, 2, \ldots, L \tag{1}$$

Let $Q_{\mathrm{MCS}_i(\mathrm{BE}_{i1},\ldots,\mathrm{BE}_{in_i})}$ denote the probability of occurrence of MCS_i. The probability of the top event based on the inclusion-exclusion principle, is expressed as follows.

$$
\begin{aligned}
Q_{\mathrm{TOP}} = &\sum_{i=1}^{L} Q_{\mathrm{MCS}_i(\mathrm{BE}_{i1},\ldots,\mathrm{BE}_{in_i})} \\
&- \sum_{i<k} Q_{\mathrm{MCS}_i(\mathrm{BE}_{i1},\ldots,\mathrm{BE}_{in_i}) \cap \mathrm{MCS}_k(\mathrm{BE}_{k1},\ldots,\mathrm{BE}_{kn_k})} \\
&+ \sum_{i<k<l} Q_{\mathrm{MCS}_i(\mathrm{BE}_{i1},\ldots,\mathrm{BE}_{in_i}) \cap \mathrm{MCS}_k(\mathrm{BE}_{k1},\ldots,\mathrm{BE}_{kn_k}) \cap \mathrm{MCS}_l(\mathrm{BE}_{l1},\ldots,\mathrm{BE}_{ln_l})} \\
&- \cdots + (-1)^{L-1} Q_{\bigcap_{i=1}^{L} \mathrm{MCS}_i(\mathrm{BE}_{i1},\ldots,\mathrm{BE}_{in_i})}
\end{aligned}
\tag{2}
$$

Given the significantly low failure probability of the safety systems, they may be treated as rare event systems, where higher order terms in Eq. (2) can be neglected without significantly affecting accuracy. This rare event approximation enables simplified probability calculations while maintaining a high level of accuracy in the results.

Now, let $Q(\mathrm{BE}_{ij})$ denote the probability of occurrence of the j-th basic event within the MCS_i. Assuming that the BEs within each MCS are mutually independent, meaning that the joint probability of events equals the product of their individual probabilities, then the probability of MCS_i can be calculated as the product of the probabilities of its constituent BEs, as shown in Eq. (3).

$$
Q_{\mathrm{MCS}_i(\mathrm{BE}_{i1},\ldots,\mathrm{BE}_{in_i})} = \prod_{j=1}^{n_i} Q(\mathrm{BE}_{ij}) \tag{3}
$$

By substituting Eq. (3) into Eq. (2), and applying the rare event approximation, the top event probability can be simplified as in the following equation.

$$
Q_{\mathrm{TOP}} = \sum_{i=1}^{L} \prod_{j=1}^{n_i} Q(\mathrm{BE}_{ij}) \tag{4}
$$

2.2. Common cause failures

Common Cause Failure (CCF) represents a specific category of dependent failure events. Such failures occur when multiple components fail simultaneously due to single root cause, such as environmental conditions (e.g., high humidity or temperature), manufacturing defects, or maintenance errors. CCFs are typically induced by coupling factors among components including shared physical location, identical operational functions, common manufacturers, shared suppliers, or identical maintenance procedures. These coupling mechanisms violate the assumption of independent failures. As a result, in redundant systems where such shared attributes are more prevalent, CCFs can significantly compromise system reliability by simultaneously affecting multiple components, thereby undermining the effectiveness of redundancy as a risk mitigation strategy.

In complex systems, CCFs can be modeled using fault tree analysis. Neglecting CCFs in fault tree models results in a systematic underestimation of the top event probability. Accurate representation of CCFs is therefore a crucial step to achieve a more realistic and detailed assessment of system reliability.

There are basically two approaches for implementing CCFs into fault tree models: the implicit and explicit approach. In the implicit approach, while the logical structure of the fault tree remains unchanged, the basic event failure probabilities are adjusted to reflect the contribution of CCFs without explicitly modeling the underlying failure mechanism within the fault tree. This approach is preferred when the shared cause of failure is complex, uncertain, or when explicitly representing it would introduce excessive modeling complexity and computational burden. In the explicit approach, CCFs are modeled directly within the fault tree by defining specific CCF events. These events are then integrated into the fault tree using appropriate logical gates, such as OR gates feeding into the top event or directly connecting to the BEs representing individual component failures.

2.3. Alpha Factor method

There are various parametric models for quantifying CCF basic events. These parametric models are divided into two main categories: shock models and non-shock models. Shock models, such as the binomial failure rate model, assume that a single external event simultaneously affect multiple components at a certain rate. Non-shock models, such as the Beta Factor, Alpha Factor, and Multiple Greek Letter methods, represent dependent failures through probabilistic relationships among components based on predefined parameters [13]. These parameters are typically derived from historical failure data analysis and expert judgment [23, 24].

The Alpha Factor method is a multi-parameter approach, which enables modeling intermediate common cause failure events, where subsets of components fail simultaneously. It is particularly suitable for systems with high redundancy, where partial group failures can impact overall system performance. The associated parameters in the Alpha Factor method are derived from a set of failure ratios and the total component failure rate. In general, the CCF data are typically collected from periodic tests, which can either be staggered or non-staggered. In staggered test data, different redundant components are tested in different test episodes. On the other hand, in non-staggered test, the system failure data are collected from a testing scheme, where all redundant components are tested simultaneously in each test episode. When considering non-staggered test data, the probability of a CCF event involving the failure of k out of a group of m components, $Q_k^{(m)}$, is given by Eq. (5). Here, Q_t denotes the total failure probability of an individual component, α_t is a normalizing factor, and α_k is the conditional probability that, given a failure event, k components out of m components within the Common Cause Failure Groups (CCFGs) fail.

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad k = 1, \ldots, m \tag{5}$$

The normalizing factor α_t is given by the following equation.

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k \qquad \alpha_1 + \alpha_2 + \alpha_3 + ... + \alpha_m = 1 \tag{6}$$

The failure probability notation by Q_k, is widely adopted in standard CCF guidelines and in studies addressing CCF in risk evaluations [12–14], where the subscript k indicates the number of components involved in the failure. For instance, Q_1 is the probability of an independent failure of a single component, Q_2 is the probability of a common cause event failing two components, and so on, up to Q_m which reflects the failure of all m components at once. In CCF quantification, the definition of Q_k is based on a symmetry assumption which implies that all combinations of k components within a CCFG have the same probability of being affected by a shared cause. As a result, the analysis depends only on the number of failed components, rather than their specific identities. This significantly simplifies the estimation process for systems with a large number of components within a CCFG.

3. Failure probability quantification of redundant systems with CCFs

In this section, a formula is proposed for quantifying the failure probability of redundant systems considering CCFs. The formulation is developed in a general form, applicable to different levels of redundancy. To this end, we consider a system composed of m identical components arranged in parallel, where the system fails only if all components fail.

To illustrate how the system failure probability is constructed using the Q_k terms, we present the expressions for systems with small values of m such as m=2, 3, 4. The corresponding system failure probabilities based on CCF method, which are represented by $Q^{(2)}_{\text{Sys-CCF}}$, $Q^{(3)}_{\text{Sys-CCF}}$, and $Q^{(4)}_{\text{Sys-CCF}}$, respectively, can be expressed as follows. The equations include all relevant combinations of independent failures and CCFs probabilities [13].

$$Q^{(2)}_{\text{Sys-CCF}} = Q_1^2 + Q_2 \tag{7}$$

$$Q^{(3)}_{\text{Sys-CCF}} = Q_1^3 + 3Q_1Q_2 + Q_3 \tag{8}$$

$$Q^{(4)}_{\text{Sys-CCF}} = Q_1^4 + 6Q_1^2Q_2 + 4Q_1Q_3 + 3Q_2^2 + Q_4 \tag{9}$$

From the patterns identified in these cases, a general expression for the system failure probability with m components is derived as follows. Let n_k be the number of failure groups involving exactly k components. These values must satisfy the following constraint, ensuring that all components are accounted for.

$$\sum_{k=1}^{m} k\, n_k = m \tag{10}$$

The number of distinct ways to partition m components into non-overlapping groups of sizes k with exactly n_k groups is given by following equation.

$$C(n_1, \ldots, n_m) = \frac{m!}{\prod_{k=1}^{m} (k!)^{n_k} \, n_k!} \tag{11}$$

Then, the total system failure probability $Q^{(m)}_{\text{Sys-CCF}}$ is calculated as follows.

$$Q^{(m)}_{\text{Sys-CCF}} = \sum_{\substack{n_1+2n_2+\cdots+mn_m=m \\ n_k \geq 0}} \left(\frac{m!}{\prod_{k=1}^{m} (k!)^{n_k} \, n_k!} \right) \prod_{k=1}^{m} Q_k^{n_k} \tag{12}$$

The presented general formulation yields an exact expression of failure probability in the presence of CCFs for a system with m redundant components.

4. Sensitivity analysis of CCFs in redundant systems

In order to achieve more insights into the influence of CCFs on the reliability of redundant systems, a sensitivity analysis was performed by varying the failure probability of individual component (Q_t). Furthermore, the impact of system redundancy level was assessed by analyzing configurations with two, three, and four identical redundant components. For each discrete value of Q_t, the system failure probability was calculated using the fault tree method under two assumptions: (1) independent failures of components (no CCFs) and (2) failures including CCFs. In the case including CCFs, the probabilities of CCF events were determined using the Alpha Factor method. The α parameter values were adopted from the NRC 2020 [24] for a specific failure mode of a consistent component type across all three redundancy levels. In the case not including CCFs, each component was assumed to fail with probability Q_t.

Fig. 1 shows the system failure probability as a function of Q_t under both assumptions, across all redundancy level cases (different m). In all cases, as the failure probability of individual components increases, the system failure probabilities for different m, with and without CCFs, converge and eventually intersect. The intersection points occur at $Q_t = 0.43$ for $m = 2$, $Q_t = 0.50$ for $m = 3$, and $Q_t = 0.54$ for $m = 4$, indicating that systems with lower redundancy reach this point of convergence more rapidly. Beyond these intersection points, the model without CCFs predicts a slightly higher system failure probability than the one with CCFs.

This counter-intuitive behavior indicates that as Q_t approaches 1, the relative contribution of CCF events diminishes, and independent failures become dominant. As a result, the system failure probability in the cases with CCFs falls below those without CCFs in the high probability regime. On the other hand, for the lower values of Q_t, the contribution of CCFs becomes increasingly significant in determining the overall system reliability.

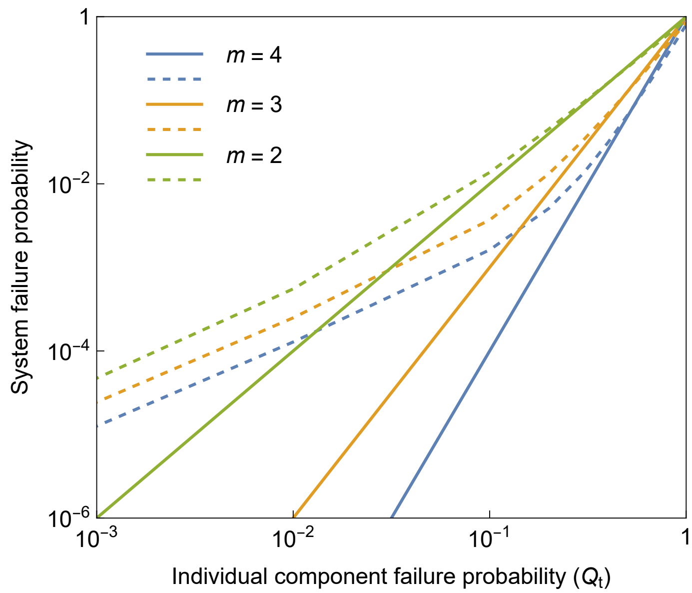

Fig. 1: System failure probability vs. component failure probability for systems with different levels of redundancy m. Solid lines: without CCFs; dashed lines: with CCFs.

5. Enhanced Alpha Factor method

In the Alpha Factor method described in Section 2.3, it is assumed that each component can belong to only one group of similar components, which represents a key limitation of the current approach. Here, an enhanced method is proposed to overcome this limitation by allowing a component to be shared across multiple common cause failure groups.

In order to demonstrate the proposed enhanced Alpha Factor method, the failure probability of a hypothetical redundant system is evaluated. The system consists of four parallel trains (A, B, C, and D), each train comprises four components arranged in series. The reliability block diagram of the system is shown in Fig. 2. The system is considered to have failed only if all four trains fail simultaneously. Accordingly, the success criterion is defined as at least one out of four trains functioning, while the failure criterion is defined as the simultaneous failure of all four trains. The failure of a single component within a train results in the failure of the entire train.

The system failure analysis assuming only independent failures is first presented as a baseline assessment. In the next step, the analysis is extended by incorporating CCFs to introduce the proposed enhanced Alpha Factor method. The system failure probability in both cases is evaluated using the fault tree model.

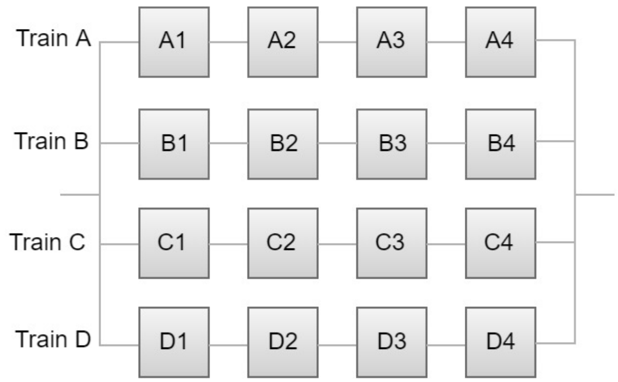

Fig. 2: Reliability block diagram of the system with four parallel trains.

5.1. System failure analysis without CCFs

Fig. 3 presents the fault tree of the system without CCFs implementation. The logical relationships between train failures and their associated components are modeled using standard AND and OR gates. An AND gate is applied at the top level (system) failure event indicating that the system fails only when all four trains fail simultaneously. Each train failure event (A,B, C, D) is linked to its associated component failures through an OR gate, signifying that the failure of a single component causes the failure of the entire corresponding train. To simplify the fault tree structure, transfer symbols are used to represent the OR gate sub-trees for B, C, and D.

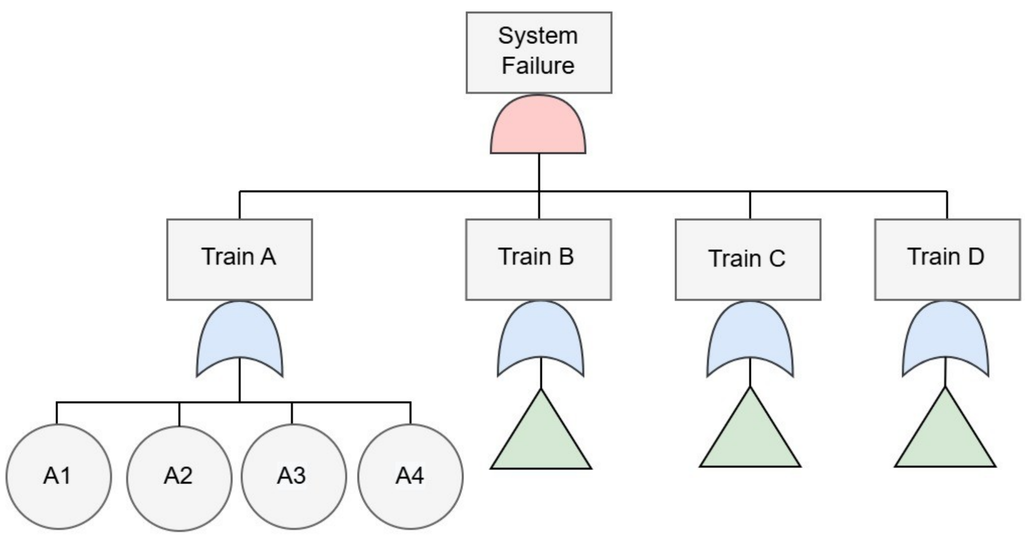

Fig. 3: Fault tree of the system with four parallel trains without CCF events.

Accordingly, the system failure event S can be expressed based on the logical AND for the failure events A, B, C, and D.

$$S = A \times B \times C \times D \tag{13}$$

In the above expression, each failure event is represented by a logical OR of the failures of its individual components, as shown in Eqs. (14)–(17). Here, $A1$ to $A4$ represent BEs corresponding to the failures of individual components in train A; the notation follows analogously for trains B, C, and D.

$$A = A1 + A2 + A3 + A4 \tag{14}$$

$$B = B1 + B2 + B3 + B4 \tag{15}$$

$$C = C1 + C2 + C3 + C4 \tag{16}$$

$$D = D1 + D2 + D3 + D4 \tag{17}$$

Substituting Eqs. (14)–(17) into Eq. (13) and applying distributive laws yields the system failure expressed in terms of MCSs.

$$S = A1 \times B1 \times C1 \times D1 + A1 \times B1 \times C1 \times D2 + \cdots + A4 \times B4 \times C4 \times D4 \tag{18}$$

For quantitative analysis, let Q_{A1}, Q_{A2}, Q_{A3}, etc., represent the failure probabilities of the BEs $A1$, $A2$, $A3$ and so on. By using the first order approximation, the system failure probability $Q_{\text{Sys-MCS}}$ is expressed as the sum of probabilities of all MCSs.

$$Q^{(1)}_{\text{Sys-MCS}} = Q_{A1}\,Q_{B1}\,Q_{C1}\,Q_{D1} + Q_{A1}\,Q_{B1}\,Q_{C1}\,Q_{D2} + \cdots + Q_{A4}\,Q_{B4}\,Q_{C4}\,Q_{D4} \tag{19}$$

In the next section, the system failure assessment in fault tree model described by Eqs. (13)–(19) is further extended by modifying the assumption of independent failures and introducing an enhanced Alpha Factor method to account for CCFs.

5.2. System failure analysis with CCFs

In order to include CCFs into the system failure model, the initial step involves identifying CCFGs. This step is particularly important in complex systems, such as those with multiple redundant trains comprising numerous identical components which may share common failure mechanisms due to their similar characteristics. Components are therefore grouped into CCFGs based on their susceptibility to the same common causes. Once these groups are established, the Alpha Factor method can be applied to quantify the probabilities of CCF events within each group.

In conventional Alpha Factor method, it is assumed that each component is associated with only a single CCFG. This simplification significantly limits the ability of the method to accurately represent real system behavior, as components may, in practice, have multiple common characteristics with different groups of components. Therefore, to achieve realistic system failure modeling, it is essential to account for such overlapping CCFs.

To demonstrate the proposed method, two distinct CCFGs are considered within the analyzed system. The components A1, B1, C1, and D1 are assumed to belong to CCFG1 and are associated with failures resulting from common mechanism 1. This group is represented by the red dashed line in Fig. 4. The components A1, B2, C3, and D3 are assumed to belong to CCFG2 and are associated with failures resulting from common mechanism 2. This group is represented by the blue dashed line in Fig. 4. Accordingly, the component A1 is shared between both CCFGs.

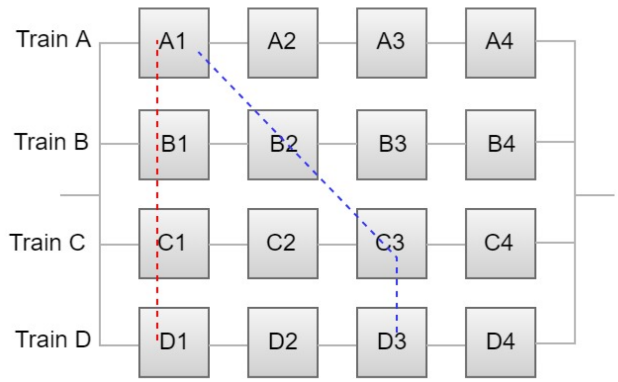

Fig. 4: System with four parallel trains and two CCFGs: CCFG1 = $\{\boldsymbol{A1}, B1, C1, D1\}$ and CCFG2 = $\{\boldsymbol{A1}, B2, C3, D3\}$.

According to the Alpha Factor method, for the CCFG1 = $\{\boldsymbol{A1}, B1, C1, D1\}$, the probability of BEs are defined based on Eqs. (20)–(23). These equations specify the failure probabilities associated with common cause events within group 1. The notation Q_{ij} used here follows the conventional format used in CCF modeling, where the first index i indicates the number of components affected by the CCF, and the second index j indicates the corresponding CCFG. Accordingly, Q_{11} represents the independent failure probability of components B1, C1, and D1 within CCFG1. Q_{21} represents the probability of a CCF affecting two components, Q_{31} corresponds to a failure involving three components, and Q_{41} represents the probability of all four components failing simultaneously due to a single common cause within CCFG1. For consistency, the same indexing convention is adopted here for the α_{ij} parameters. The parameters α_{11}, α_{21}, α_{31} and α_{41} denote the probabilities that, given a failure event, exactly one, two, three, and all four components within CCFG1 will fail due to a common cause, respectively.

$$Q_{11} = Q_{B1i} = Q_{C1i} = Q_{D1i} = \frac{\alpha_{11}}{\alpha_{t,1}} Q_t \tag{20}$$

$$Q_{21} = Q_{A1B1\_CC} = Q_{A1C1\_CC} = Q_{A1D1\_CC} = Q_{B1C1\_CC} = Q_{B1D1\_CC} = Q_{C1D1\_CC} = \frac{2}{3} \frac{\alpha_{21}}{\alpha_{t,1}} Q_t \tag{21}$$

$$Q_{31} = Q_{A1B1C1\_CC} = Q_{A1B1D1\_CC} = Q_{A1C1D1\_CC} = Q_{B1C1D1\_CC} = \frac{\alpha_{31}}{\alpha_{t,1}} Q_t \tag{22}$$

$$Q_{41} = Q_{A1B1C1D1\_CC} = 4 \frac{\alpha_{41}}{\alpha_{t,1}} Q_t \tag{23}$$

The term $\alpha_{t,1}$ represents the normalizing factor for CCFG1 and is defined by Eq. (24).

$$\alpha_{t1} = \alpha_{11} + 2\alpha_{21} + 3\alpha_{31} + 4\alpha_{41} \tag{24}$$

Additionally, the α parameters must satisfy the following condition to ensure that the total probability across all CCFs within CCFG1 is equal to one.

$$\alpha_{11} + \alpha_{21} + \alpha_{31} + \alpha_{41} = 1 \tag{25}$$

Similarly, for CCFG2 $= \{\boldsymbol{A1}, B2, C3, D3\}$, the probability of BEs are defined based on Eqs. (26)–(29). Here, Q_{12} represents the independent failure probability of components B2, C3, and D3 within CCFG2. The terms Q_{22}, Q_{32}, and Q_{42} denote the probabilities of common cause failures affecting two, three, and all four components within CCFG2, respectively. Parameters α_{12}, α_{22}, α_{32} and α_{42} represent the probabilities that, given a failure event, exactly one, two, three, and all four components within CCFG2 will fail due to a common cause, respectively.

$$Q_{12} = Q_{B2i} = Q_{C3i} = Q_{D3i} = \frac{\alpha_{12}}{\alpha_{t,2}} Q_t \tag{26}$$

$$Q_{22} = Q_{A1B2\_CC} = Q_{A1C3\_CC} = Q_{A1D3\_CC} = Q_{B2C3\_CC} = Q_{B2D3\_CC} = Q_{C3D3\_CC} = \frac{2}{3}\frac{\alpha_{22}}{\alpha_{t,2}} Q_t \tag{27}$$

$$Q_{32} = Q_{A1B2C3\_CC} = Q_{A1B2D3\_CC} = Q_{A1C3D3\_CC} = Q_{B2C3D3\_CC} = \frac{\alpha_{32}}{\alpha_{t,2}} Q_t \tag{28}$$

$$Q_{42} = Q_{A1B2C3D3\_CC} = 4\frac{\alpha_{42}}{\alpha_{t,2}} Q_t \tag{29}$$

The normalizing factor $\alpha_{t,2}$ for CCFG2 is calculated as shown in Eq. (30).

$$\alpha_{t,2} = \alpha_{12} + 2\alpha_{22} + 3\alpha_{32} + 4\alpha_{42} \tag{30}$$

As with CCFG1, the α parameters associated with CCFG2 must also satisfy the following condition.

$$\alpha_{12} + \alpha_{22} + \alpha_{32} + \alpha_{42} = 1 \tag{31}$$

The failure space of component A1, which is divided into independent and CCF affected portions, is influenced by its inclusion in two CCFGs. According to the definition of CCF, the independent failure probability of component A1, is reduced due to the increased impact of CCF events. Consequently, the total failure probability of component A1 can be expressed by the following equation, in which the CCF portion arises from both CCFGs.

$$Q_t = \underbrace{Q_{A1i}}_{\text{independent portion}} + \underbrace{Q_{CCFG1} + Q_{CCFG2}}_{\text{CCF portion}} \tag{32}$$

In the CCF portion, the common cause contributions involving $A1$ within each CCFG are taken into account.

Based on Eqs. (21), (22), and (23), various BEs contribute to the CCF of $A1$ in conjunction with other components in CCFG1. The contributions from these events are represented by the following equations.

$$3Q_{21} = 3\frac{2}{3}\frac{\alpha_{21}}{\alpha_{t,1}}Q_t \tag{33}$$

$$3Q_{31} = 3\frac{\alpha_{31}}{\alpha_{t,1}}Q_t \tag{34}$$

$$1Q_{41} = 4\frac{\alpha_{41}}{\alpha_{t,1}}Q_t \tag{35}$$

According to Eqs. (27)–(29), the BEs in which $A1$ is affected within CCFG2 are defined by the following expressions.

$$3Q_{22} = 3\frac{2}{3}\frac{\alpha_{22}}{\alpha_{t,2}}Q_t \tag{36}$$

$$3Q_{32} = 3\frac{\alpha_{32}}{\alpha_{t,2}}Q_t \tag{37}$$

$$1Q_{42} = 4\frac{\alpha_{42}}{\alpha_{t,2}}Q_t \tag{38}$$

Therefore, the total contribution from common cause failures $Q_{\text{CCF},A1}$ is given by the sum of the contributions from both CCFGs affecting component A1.

$$Q_{\text{CCF},A1} = \left(2\frac{\alpha_{21}}{\alpha_{t,1}} + 3\frac{\alpha_{31}}{\alpha_{t,1}} + 4\frac{\alpha_{41}}{\alpha_{t,1}}\right)Q_t + \left(2\frac{\alpha_{22}}{\alpha_{t,2}} + 3\frac{\alpha_{32}}{\alpha_{t,2}} + 4\frac{\alpha_{42}}{\alpha_{t,2}}\right)Q_t \tag{39}$$

Consequently, the independent failure probability of component A1 is determined by subtracting the total CCF contribution from its overall failure probability.

$$Q_{A1i} = Q_t\left[1 - \left(2\frac{\alpha_{21}}{\alpha_{t,1}} + 3\frac{\alpha_{31}}{\alpha_{t,1}} + 4\frac{\alpha_{41}}{\alpha_{t,1}} + 2\frac{\alpha_{22}}{\alpha_{t,2}} + 3\frac{\alpha_{32}}{\alpha_{t,2}} + 4\frac{\alpha_{42}}{\alpha_{t,2}}\right)\right] \tag{40}$$

The general expression for Q_{A1i}, when component A1 is shared among n CCFGs of size four, is derived as follows.

$$Q_{A1i} = Q_t\left[1 - \sum_{j=1}^{n}\left(2\frac{\alpha_{2j}}{\alpha_{t,j}} + 3\frac{\alpha_{3j}}{\alpha_{t,j}} + 4\frac{\alpha_{4j}}{\alpha_{t,j}}\right)\right] \tag{41}$$

For a more general case where component A1 participates in n CCFGs, each of size m, the independent failure probability of component A1 can be expressed as in Eq. (42). In this expression, α_{pj} denotes the alpha factor representing the probability that exactly p components fail simultaneously due to a common cause event in the j-th CCFG. The term $\alpha_{t,j}$ is the normalizing factor for the j-th CCFG, defined as in Eq. (43). Note that the sum of the alpha factors for each group must equal one, see Eq. (44).

$$Q_{A1i} = Q_t\left[1 - \sum_{j=1}^{n}\sum_{p=2}^{m} p\frac{\alpha_{pj}}{\alpha_{t,j}}\right] \tag{42}$$

$$\alpha_{t,j} = \sum_{k=1}^{m} k\alpha_{kj} \tag{43}$$

$$\sum_{k=1}^{m} \alpha_{kj} = 1 \tag{44}$$

Once CCFs are incorporated into the system failure analysis, the fault tree must be further extended to account for these CCFs contribution. To achieve this, each BE within a CCFG is modified in accordance with the definition of CCF. An example of the extended basic event of $A1$ is illustrated in Fig. 5.

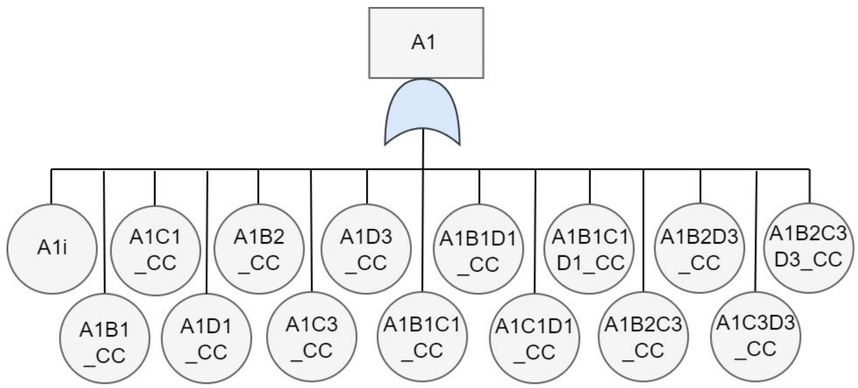

Fig. 5: Extended basic event $A1$ with CCFs contributions.

In accordance with the definition of CCFs, the component A1 may either fail independently, where the related BE is denoted as $A1i$, or participate in CCF scenarios with other components. Depending on the number of components affected, different levels of CCFs can occur. For example, $A1$ may fail simultaneously with one other component, representing a two component CCF, such as $A1B1\_CC$, $A1C1\_CC$, $A1D1\_CC$, $A1B2\_CC$, $A1C3\_CC$, or $A1D3\_CC$. It may also be involved in a CCF with two additional components, corresponding to a three component CCF, such as $A1B1C1\_CC$, $A1B1D1\_CC$, $A1C1D1\_CC$, $A1B2C3\_CC$, $A1B2D3\_CC$, or $A1C3D3\_CC$. Furthermore, A1 can participate in a four component CCF, such as $A1B1C1D1\_CC$, or $A1B2C3D3\_CC$. This modeling strategy is similarly applied to other BEs within both CCFGs, including $B1$, $C1$, $D1$, $B2$, $C3$, and $D3$. On the other hand, BEs such as $A2$, $A3$, $A4$, $B3$, $B4$, $C2$, $C4$, $D2$, and $D4$, which do not participate in any CCFG, are modeled exclusively as independent failure events.

The basic fault tree (Fig. 3) must then be extended with additional BEs. Fig. 6 presents the extended fault tree by properly including the extended BEs.

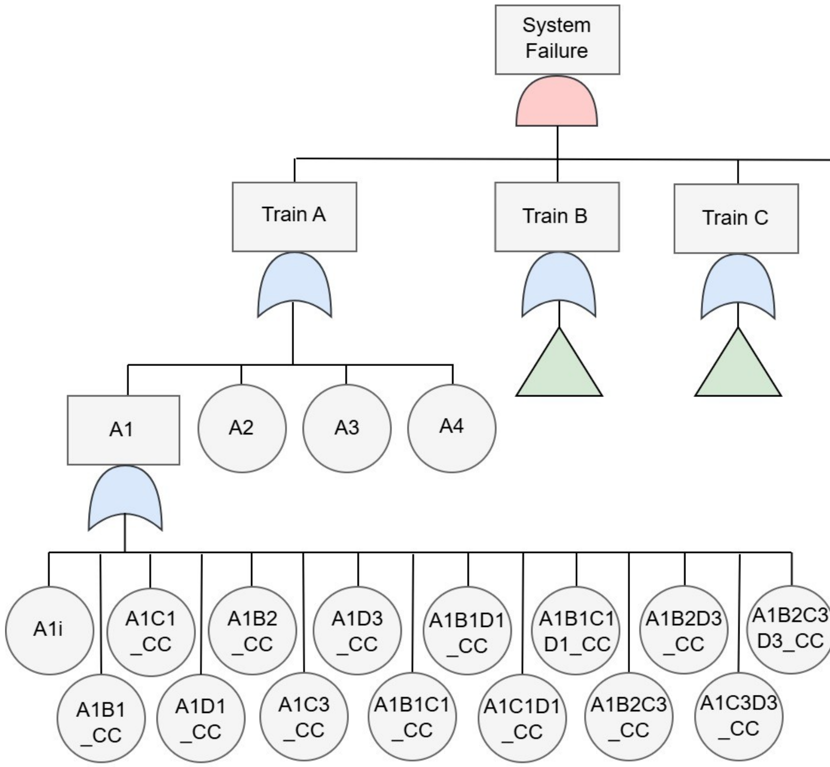

Fig. 6: Extended fault tree with CCF-related basic events.

The system failure S was initially described using Eq. (13). However, to account for CCF events, the failure logic of each train is updated by incorporating extended BEs into the fault tree structure.

$$\begin{aligned} A = A1i + A1B1\_CC + A1C1\_CC + A1D1\_CC + A1B2\_CC + A1C3\_CC + A1D3\_CC \\ + A1B1C1\_CC + A1B1D1\_CC + A1C1D1\_CC + A1B2C3\_CC + A1B2D3\_CC \\ + A1C3D3\_CC + A1B1C1D1\_CC + A1B2C3D3\_CC + A2 + A3 + A4 \end{aligned} \tag{45}$$

$$\begin{aligned} B = B1i + A1B1\_CC + B1C1\_CC + B1D1\_CC + A1B1C1\_CC + A1B1D1\_CC \\ + B1C1D1\_CC + A1B1C1D1\_CC + B2i + A1B2\_CC + B2C3\_CC + B2D3\_CC \\ + A1B2C3\_CC + A1B2D3\_CC + B2C3D3\_CC + A1B2C3D3\_CC + B3 + B4 \end{aligned} \tag{46}$$

$$\begin{aligned} C = C1i + A1C1\_CC + B1C1\_CC + C1D1\_CC + A1B1C1\_CC + B1C1D1\_CC \\ + A1C1D1\_CC + A1B1C1D1\_CC + C2 + C3i + A1C3\_CC + B2C3\_CC + C3D3\_CC \\ + A1B2C3\_CC + B2C3D3\_CC + A1C3D3\_CC + A1B2C3D3\_CC + C4 \end{aligned} \tag{47}$$

$$D = D1i + A1D1\_CC + B1D1\_CC + C1D1\_CC + A1B1D1\_CC + B1C1D1\_CC \\ + A1C1D1\_CC + A1B1C1D1\_CC + D2 + D3i + A1D3\_CC + B2D3\_CC + C3D3\_CC \\ + A1B2D3\_CC + B2C3D3\_CC + A1C3D3\_CC + A1B2C3D3\_CC + D4 \tag{48}$$

By substituting Eqs. (45)–(48) into Eq. (13), the Boolean expression for the system failure can be presented as shown in Eq. (49) which incorporates a large number of MCSs.

$$S = A1i \times B1i \times C1i \times D1i + A1i \times B1i \times C1i \times D2 + A1B1\_CC \times C1i \times D1i \\ + A1i \times B2C3D3\_CC + A1B1C1D1\_CC + A1B2C3D3\_CC + \cdots \tag{49}$$

The system failure probability can now be expressed using the derived MCSs. To simplify the formulation, four auxiliary variables are introduced to represent the failure probabilities of trains A, B, C, and D, assuming only independent component failures of the associated components.

$$Q_A = Q_{A1i} + Q_{A2} + Q_{A3} + Q_{A4} \tag{50}$$

$$Q_B = Q_{B1i} + Q_{B2i} + Q_{B3} + Q_{B4} \tag{51}$$

$$Q_C = Q_{C1i} + Q_{C2} + Q_{C3i} + Q_{C4} \tag{52}$$

$$Q_D = Q_{D1i} + Q_{D2} + Q_{D3i} + Q_{D4} \tag{53}$$

Now, the probability of system failure with a component shared among total n number of CCFGs (here $n = 2$) is defined as in Eq. (54). Here, $Q_{Sys-MCS-ccf}^{\text{AFM}(1)}$ represents the total failure probability of the system under the rare event approximation based on Alpha Factor method, and parameter l represents the number of BEs in which two components fail simultaneously within each CCFG (here $l = 6$).

$$Q_{Sys-MCS-ccf}^{\text{AFM}(1)} = (Q_A \cdot Q_B \cdot Q_C \cdot Q_D) + (Q_A \cdot (Q_B + Q_C + Q_D) + Q_B \cdot (Q_C + Q_D) \\ + Q_C . Q_D) \sum_{i=1}^{n} Q_{2i} + l(\frac{1}{2} \sum_{i=1}^{n} Q_{2i}^2 + \sum_{i=1}^{n} \sum_{j=i+1}^{n} Q_{2i} Q_{2j}) + (Q_A + Q_B + Q_C + Q_D) \sum_{i=1}^{n} Q_{3i} \\ + \sum_{i=1}^{n} Q_{4i} \tag{54}$$

6. Case study

The applicability of the proposed approach is here demonstrated for a simplified model of the emergency core cooling system, i.e., the Containment Spray System (CSS) of the U.S. Advanced Pressurized Water Reactor (US-APWR) [25], as illustrated in Fig. 7. The CSS is designed to maintain the integrity of the containment building, which serves as the final barrier to prevent the release of radioactive fission products to the environment. The CSS is a subsystem of the Residual

Heat Removal System (RHRS) and functions by spraying borated water into the containment atmosphere following a loss of coolant accident or a main steam line break. This function helps to ensure that containment pressure and temperature stay within their specified design limits.

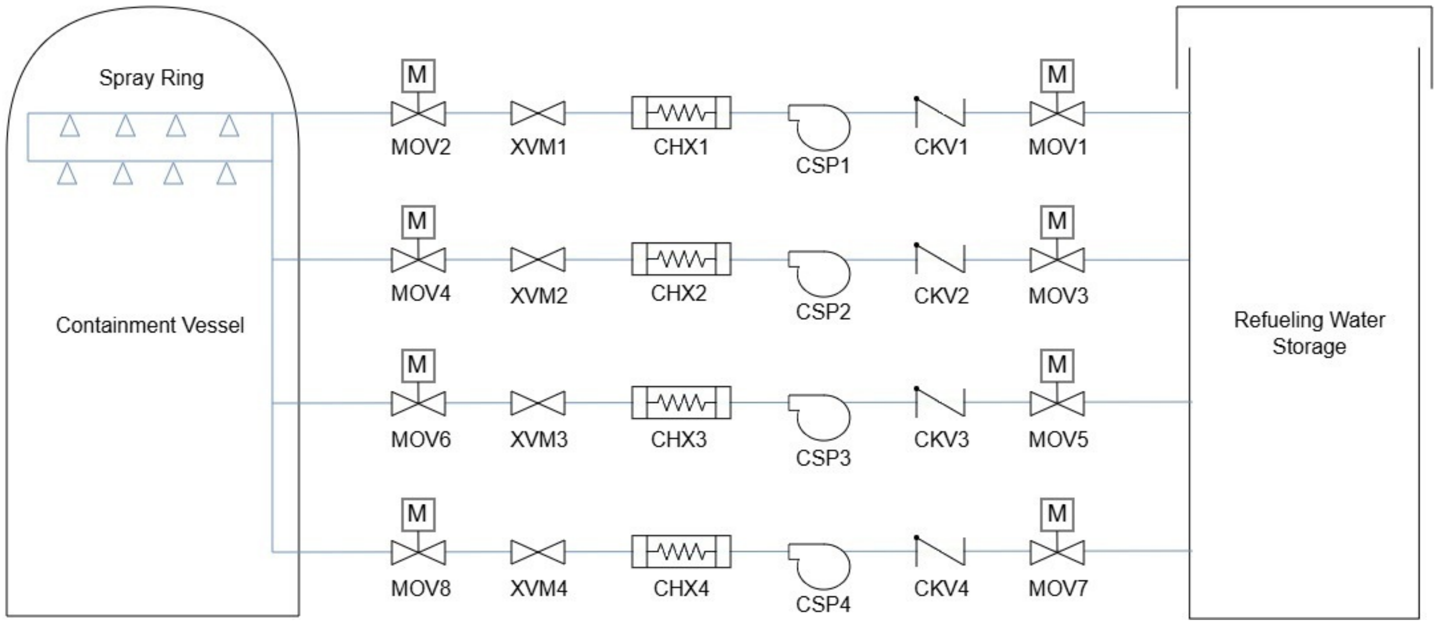

Fig. 7: Schematic diagram of containment spray system.

The CSS consists of four parallel trains, which form a redundant configuration to enhance the reliability of the system. The actual success criterion of the system is two out of four operational trains, meaning that the system can still fulfill its safety function as long as at least two trains are available. For example, continuous operation is maintained when a single component fails following an accident, and at the same time, one train is out of service due to maintenance. Each train includes two normally-open motor-operated isolation valves (MOVs), one gate valve (XVM), one check valve (CKV), one containment spray/residual heat removal (CS/RHR) heat exchanger (CHX), and one CS/RHR pump (CSP).

The CSS system automatically activates upon receiving a containment spray signal. Once activated, the outlet valves of the CS/RHR heat exchangers open, and the CS/RHR pumps begin operation. These pumps draw water from the refueling water storage tank, and circulate it through the heat exchangers for cooling. The cooled water is then delivered to the spray headers located at the top of the containment vessel to mitigate the rise in pressure and temperature.

In the present study, the operation of the CSS system is modeled using a fault tree, assuming one out of four success criteria. The failure probabilities of individual components were primarily derived from the 2020 update on U.S. commercial nuclear power plant data [26]. To supplement this dataset, additional reliability data were obtained from the IAEA reliability database [27].

6.1. Case study without implementation of CCFs

Initially, the system failure analysis was conducted using a fault tree model without accounting for CCFs. Fig. 8 shows the reliability block diagram of the system. The system is considered to fail only when all four trains fail simultaneously.

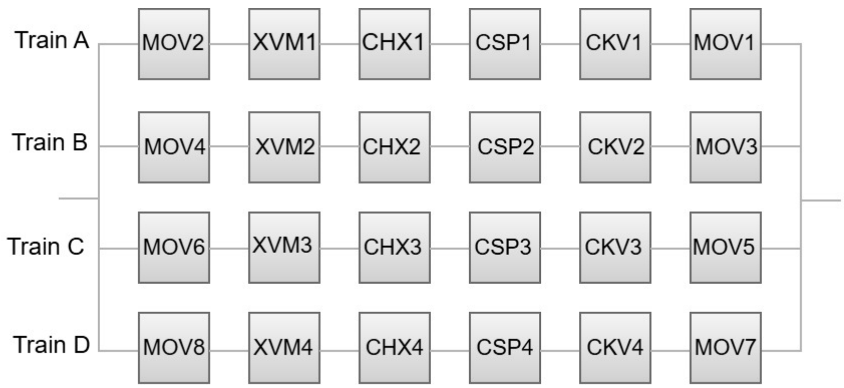

Fig. 8: Reliability block diagram of CSS system with four parallel trains.

The fault tree model of the system is presented in Fig. 9. An AND gate is used at the top of the fault tree for the system failure event, indicating that the system fails only when all trains fail simultaneously. The failure of Each train is connected to its associated components through an OR gate, signifying that the failure of a single component leads to the failure of the corresponding train.

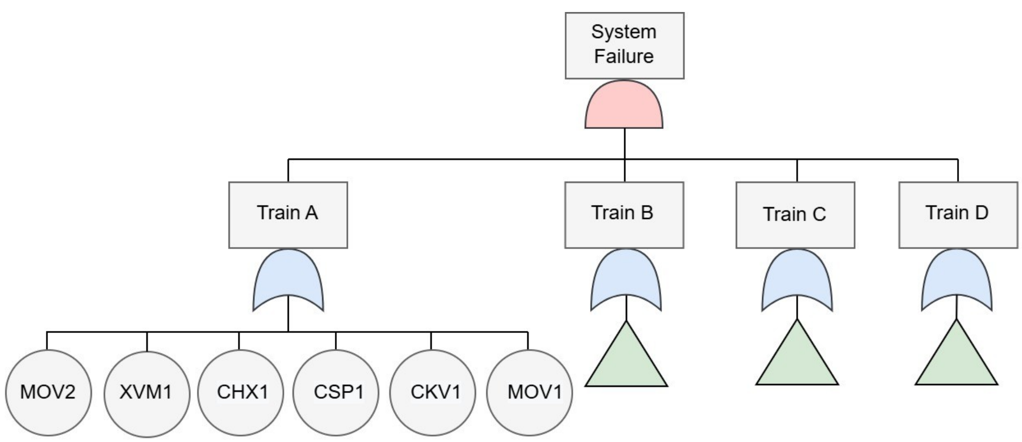

Fig. 9: Fault tree of the CSS system without CCF events.

Here, the system failure S is also initially described by Eq. (13), where the failure logic of the associated events is defined as follows.

$$A = MOV2 + XVM1 + CHX1 + CSP1 + CKV1 + MOV1 \tag{55}$$

$$B = MOV4 + XVM2 + CHX2 + CSP2 + CKV2 + MOV3 \tag{56}$$

$$C = MOV6 + XVM3 + CHX3 + CSP3 + CKV3 + MOV5 \tag{57}$$

$$D = MOV8 + XVM4 + CHX1 + CSP4 + CKV4 + MOV7 \tag{58}$$

By substituting these expressions into Eq. (13), the Boolean expression of the system failure can be obtained as follows.

$$S = MOV2 \times MOV4 \times MOV6 \times MOV8 + MOV2 \times MOV4 \times MOV6 \times XVM4 + \cdots \tag{59}$$

The probability of system failure, based on the identified MCSs and using the first order approximation, is given by the following expression.

$$Q^{(1)}_{\text{Sys(CSS)-MCS}} = Q_{MOV2}Q_{MOV4}Q_{MOV6}Q_{MOV8} + Q_{MOV2}Q_{MOV4}Q_{MOV6}Q_{XVM4} + \cdots \tag{60}$$

By substituting the failure probabilities of the BEs, the probability of system failure is achieved as 2.32×10^{-13} under the first order approximation. This result closely aligns with the exact value computed by the commercial PSA software.

In order to achieve more detailed insights, the significance of MCSs is also investigated. The eight most significant MCSs have been identified and presented in Tab. 1. The most significant MCS corresponds to the simultaneous failure of all four CSP pumps to start, i.e., CSP1, CSP2, CSP3, and CSP4. This MCS contributes approximately 51.72% to the total failure probability. The remaining MCSs involve various combinations of failure modes (start or run failure modes) across the CSP components, and also rank among the most significant contributors. Among these, each of the MCSs ranked from 2 to 5 contribute 8.02% , and each of the last three MCSs (ranks 6 to 8) contribute 1.24% to the system failure probability.

The analysis shows that independent failures of CSP components across trains are the dominant contributors to system failure when CCFs are not considered.

Tab. 1: The most significant MCSs without consideration of CCFs.

No.	MCS	%
1	$CSP1$ (fails to start) $CSP2$ (fails to start) $CSP3$ (fails to start) $CSP4$ (fails to start)	51.72
2	$CSP1$ (fails to start) $CSP2$ (fails to run) $CSP3$ (fails to start) $CSP4$ (fails to start)	8.02
3	$CSP1$ (fails to start) $CSP2$ (fails to start) $CSP3$ (fails to start) $CSP4$ (fails to run)	8.02
4	$CSP1$ (fails to run) $CSP2$ (fails to start) $CSP3$ (fails to start) $CSP4$ (fails to start)	8.02
5	$CSP1$ (fails to run) $CSP2$ (fails to start) $CSP3$ (fails to run) $CSP4$ (fails to run)	8.02
6	$CSP1$ (fails to start) $CSP2$ (fails to run) $CSP3$ (fails to start) $CSP4$ (fails to run)	1.24
7	$CSP1$ (fails to start) $CSP2$ (fails to run) $CSP3$ (fails to run) $CSP4$ (fails to start)	1.24
8	$CSP1$ (fails to run) $CSP2$ (fails to start) $CSP3$ (fails to start) $CSP4$ (fails to run)	1.24

6.2. Case study with application of the new method

Now, the system failure probability is recalculated by incorporating CCFs using the proposed new method. Two distinct CCFGs were defined within the system, as presented in Tab. 2. The isolation valve MOV2 is assumed to be shared between both CCFG1 and CCFG2, and is therefore analyzed according to the new method. The components MOV2, MOV4, MOV6, and MOV8 are assigned to CCFG1, represented by the red dashed line in Fig. 10, while the components MOV2, MOV3, MOV5, and MOV7 are assumed to take part in the CCFG2, indicated by the blue dashed line. These groups were categorized based on the following coupling mechanisms: operational-related and manufacturer-related factors, respectively.

Tab. 2: Defined CCFGs with associated components.

Group	Components	Coupling mechanism
CCFG1	{**MOV2**, MOV4, MOV6, MOV8}	Operational-related
CCFG2	{**MOV2**, MOV3, MOV5, MOV7}	Manufacturer-related

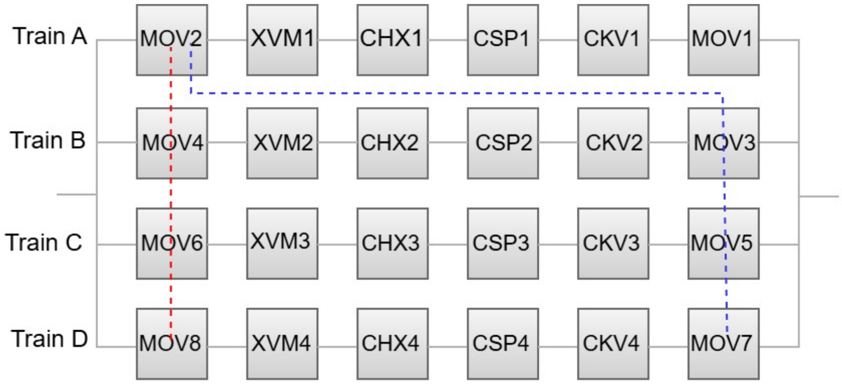

Fig. 10: Reliability block diagram of the CSS system with four parallel trains and two CCFGs: CCFG1 = $\{\boldsymbol{MOV2}, MOV4, MOV6, MOV8\}$ and CCFG2 = $\{\boldsymbol{MOV2}, MOV3, MOV5, MOV7\}$.

In order to extend the fault tree, each basic event within each CCFG is modified according to the CCF definition. An example of the extended basic event for component MOV2 is illustrated in Fig. 11.

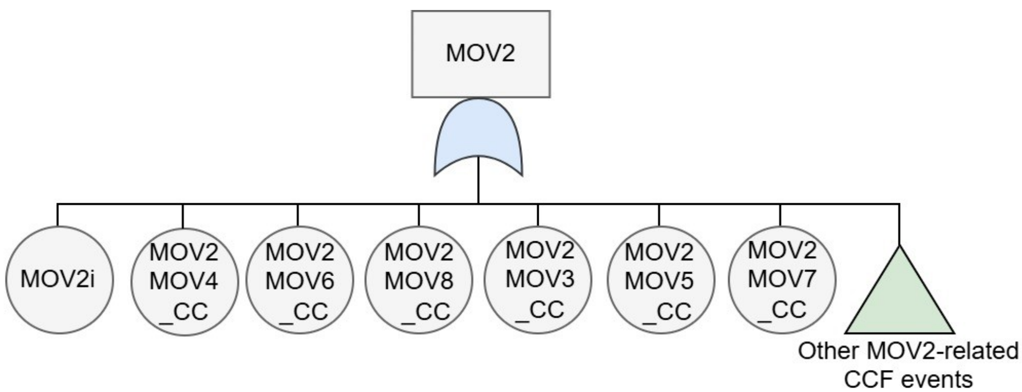

Fig. 11: Extended basic event MOV2 with CCFs contribution.

In accordance with the definition of CCFs, the MOV2 component may either fail independently, denoted as $MOV2i$, or participate in CCF events with other components. Depending on the number of components affected, different levels of CCFs can occur. For example, MOV2 may fail simultaneously with one other component, representing a two component CCF such as $MOV2MOV4\_CC$, $MOV2MOV6\_CC$, $MOV2MOV8\_CC$, $MOV2MOV3\_CC$, $MOV2MOV5\_CC$, and $MOV2MOV7\_CC$. It may also participate in a CCF involving two additional components, corresponding to a three component CCF, such as $MOV2MOV4MOV6\_CC$, $MOV2MOV4MOV8\_CC$, $MOV2MOV6MOV8\_CC$, $MOV2MOV3MOV5\_CC$, $MOV2MOV5MOV7\_CC$, and $MOV2MOV3MOV7\_CC$. Furthermore, it can be involved in three other components, corresponding to a four component CCF such as $MOV2MOV4MOV6MOV8\_CC$, and $MOV2MOV3MOV5MOV7\_CC$. This modeling strategy is similarly applied to other BEs within all CCFGs, including $MOV4$, $MOV6$, $MOV8$, $MOV3$, $MOV5$, and $MOV7$. On the other hand, events such as $XVM1$, $CHX1$, $CSP1$, $CKV1$, $XVM2$, etc., which are not included in any CCFG, are modeled exclusively as independent failure events.

The basic fault tree of the system (Fig. 9) is subsequently extended to include additional BEs. The updated fault tree structure is illustrated in Fig. 12.

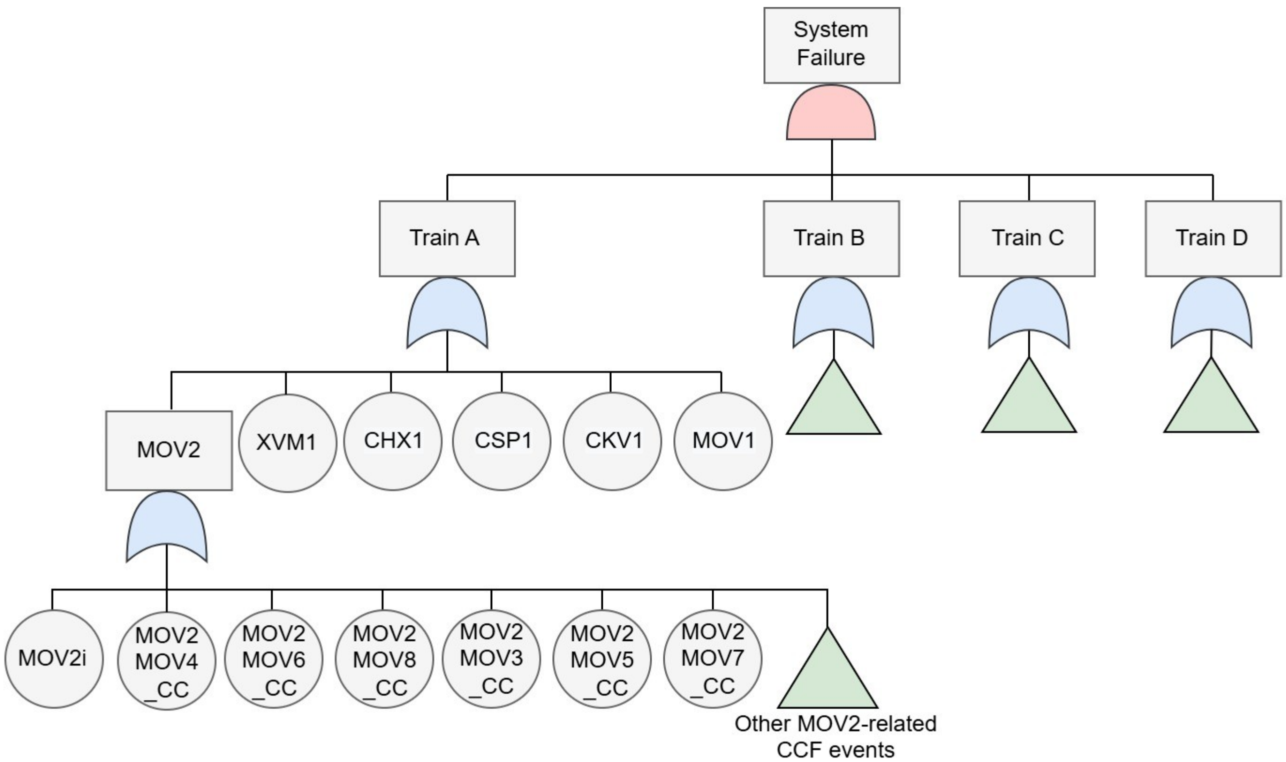

Fig. 12: Extended fault tree of the CSS system with contribution of CCF events.

Subsequently, the updated failure logic of each train can be derived as follows.

$$A = MOV2i + MOV2MOV4\_CC + MOV2MOV6\_CC + MOV2MOV8\_CC + \cdots \quad (61)$$

$$B = MOV4i + MOV2MOV4\_CC + MOV4MOV6\_CC + MOV4MOV8\_CC + \cdots \quad (62)$$

$$C = MOV6i + MOV2MOV6\_CC + MOV4MOV6\_CC + MOV6MOV8\_CC + \cdots \quad (63)$$

$$D = MOV8i + MOV2MOV8\_CC + MOV4MOV8\_CC + MOV6MOV8\_CC + \cdots \quad (64)$$

These equations are then substituted into Eq. (13), to define the system failure expression.

$$S = MOV2i \times MOV4i \times MOV6i \times MOV8i + MOV2i \times MOV4i \times MOV6i \times MOV7i + \cdots \quad (65)$$

Therefore, the failure probability of the CSS system with the first order approximation can be expressed using the qualitative failure analysis of the system.

$$Q^{(1)}_{Sys(CSS)-MCS-ccf} = Q_{MOV2i}Q_{MOV4i}Q_{MOV6i}Q_{MOV8i} + Q_{MOV2i}Q_{MOV4i}Q_{MOV6i}Q_{MOV7i} + \cdots \tag{66}$$

By applying the Alpha Factor method, Eq. (66) can be rewritten based on the proper application of the new formulation presented in Eq. (54).

The analysis is performed using Alpha Factor values corresponding to the MOV component under the spurious operation failure mode for both CCFGs. Additionally, the sensitivity of the results to the α values is evaluated using two different data sources. In order to enable a clear assessment of the impact of α variations without introducing other influencing factors, two versions of the NRC CCF parameter data were used: the latest version, NRC 2020 [24], and an earlier version, NRC 2009 [28], each providing different estimates. The parameters $l = 6$ and $n = 2$ within the equation remain unchanged as in the earlier simple example.

Based on the calculation using NRC 2020 data, the failure probability is achieved as 1.91×10^{-9} which is approximately four orders of magnitude higher than the probability calculated without CCFs and without the application of the new method. Based on the calculation using NRC 2009 data, the failure probability is achieved as 7.59×10^{-10}. Although the differences between the α values from two datasets are relatively small, they resulted in a variation of nearly one order of magnitude in the failure probability of the system. This outcome highlights the sensitivity of the system reliability results to the selected α factors. To verify the result, the failure probability was recalculated using the implemented MCS approach and commercial PSA software. The results confirmed consistency with the proposed equation.

The significance of MCSs and their contribution to system failure are also investigated for both cases. The corresponding results are presented in Tabs. 3 and 4. The results show that the MCSs involving simultaneous failure of multiple MOVs, caused by a common cause failure in spurious operation failure mode, dominate the system failure probability in both cases. In particular, the minimal cut sets $MOV2MOV4MOV6MOV8\_CC$ and $MOV2MOV3MOV5MOV7\_CC$ each contribute approximately 50% of the total system failure within both cases. Furthermore, the contribution of CSP components in system failure has significantly decreased under the new method.

The remaining MCSs, listed in the lower ranks of Tabs. 3 and 4, contribute only marginally to the overall failure probability. Most of these involve k-out-of-n common cause failure events involving MOVs along with the failure of one CSP component. Although these MCSs have a low contribution to the overall system failure probability, they still represent credible, yet less critical, failure scenarios that may gain importance under alternative parameter values or system configurations.

The results also indicate that, under both NRC datasets, the overall structure of the most significant MCSs remains broadly similar. However, slight variations in α values lead to shifts in the relative contribution of less dominant MCSs. For instance, the contribution of MCSs composed of MOVs and a CSP is slightly higher under the 2009 dataset compared to 2020, due to relatively larger α factors used for three-component group failures. Additionally, the NRC 2020 results include a CSP-only minimal cut set ($CSP1\,CSP2\,CSP3\,CSP4$) among the top-ranked contributors, which does not appear in the NRC 2009 table.

Tab. 3: The most significant MCSs with consideration of the new method with α values based on NRC 2020 data [24].

No.	**MCS**	**%**
1	$MOV2MOV4MOV6MOV8\_CC$ (Spurious operation)	49.98
2	$MOV2MOV3MOV5MOV7\_CC$ (Spurious operation)	49.98
3	$CSP1\,CSP2\,CSP3\,CSP4$ (Fails to start)	0.01
4	$MOV2MOV4MOV6\_CC$ (Spurious operation) $CSP4$ (Fails to start)	0.002
5	$MOV2MOV4MOV8\_CC$ (Spurious operation) $CSP3$ (Fails to start)	0.002
6	$MOV4MOV6MOV8\_CC$ (Spurious operation) $CSP1$ (Fails to start)	0.002
7	$MOV2MOV5MOV7\_CC$ (Spurious operation) $CSP2$ (Fails to start)	0.002
8	$MOV4MOV5MOV7\_CC$ (Spurious operation) $CSP1$ (Fails to start)	0.002

Tab. 4: The most significant MCSs with consideration of the new method with α values based on NRC 2009 data [28].

No.	**MCS**	**%**
1	$MOV2MOV4MOV6MOV8\_CC$ (Spurious operation)	49.89
2	$MOV2MOV3MOV5MOV7\_CC$ (Spurious operation)	49.89
3	$MOV2MOV3MOV5\_CC$(Spurious operation) $CSP4$ (Fails to start)	0.02
4	$MOV2MOV5MOV7\_CC$ (Spurious operation) $CSP2$ (Fails to start)	0.02
5	$MOV2MOV6MOV8\_CC$ (Spurious operation) $CSP2$ (Fails to start)	0.02
6	$MOV4MOV6MOV8\_CC$ (Spurious operation) $CSP1$ (Fails to start)	0.02
7	$MOV4MOV5MOV7\_CC$ (Spurious operation) $CSP1$ (Fails to start)	0.02
8	$MOV4MOV4MOV8\_CC$ (Spurious operation) $CSP3$ (Fails to start)	0.02

6.3. Discussion

The results demonstrate that introducing the new CCF modeling approach significantly increases the overall system failure probability compared to models without CCFs. Although the observed increase in system failure probability reflects the inclusion of CCF events, it is primarily attributed to the enhanced modeling of the proposed method. This improved approach enables the identification of failure mechanisms that are typically overlooked by conventional Alpha factor method. As a result, even when the results are compared against system failure probabilities that include other CCF events modeled using conventional methods, the proposed approach still yields higher failure probabilities. This difference arises from the limited capability of conventional methods to represent the additional failure mechanisms identified by the improved modeling technique.

Beyond its influence on failure probability, the proposed method also substantially alters the structure and ranking of the most critical MCSs by identifying high contribution failure combinations which may not be captured by conventional modeling approach. Although incorporating additional CCFGs or other CCF scenarios could further influence these outcomes, the current results clearly demonstrate the effectiveness of the method in revealing critical failure mechanisms that would otherwise remain unrecognized or be incorrectly dismissed as low contribution events.

Moreover, the results show that in CCF estimation using the Alpha Factor method, the selected α values have a direct and measurable impact on overall system reliability. Even small variations in the selected α values can lead to noticeable changes in the calculated failure probability. Larger discrepancies, such as those stemming from different data sources or estimation approaches, can result in more substantial shifts in overall system reliability. These variations not only alter the ranking of individual MCSs but can also reveal alternative failure pathways that may become dominant under different CCF parameter assumptions. These findings highlight that both system reliability and MCS prioritization are sensitive to the assumed CCF parameters. This underscores the importance of careful dataset selection in reliability assessments.

7. Conclusion

The main objective of this work is to introduce an advanced Alpha Factor method with the aim to improve the evaluation of common cause failures in system failure models such as fault tree analysis. In the standard Alpha Factor method, each component can be associated with only a single common cause failure group. The proposed method overcomes this limitation by allowing components to be assigned to multiple common cause failure groups. This enhancement captures a broader range of coupling mechanisms and thereby enables a more detailed evaluation of system reliability. The new method has been developed through a simple example, in which a single component is assumed to take part in two distinct common cause failure groups.

The practical application of the proposed method has been demonstrated through a simplified yet representative redundant safety system in a nuclear power plant. The system failure probabilities have been evaluated both without common cause failures and with their inclusion using the new method. The results proved that implementing the common cause failures using the new method led to a considerable increase in system failure probability compared to the case without considering common cause failures. However, this increase is attributed to the proposed method which enables a more detailed representation of common cause failure mechanisms that cannot be captured by the conventional Alpha Factor method. Additionally, application of the proposed method enables the identification of the most critical components within high priority minimal cut set combinations, which might otherwise be underestimated or overlooked when using conventional Alpha Factor method. These insights contribute to a more accurate characterization of critical failure scenarios and support more informed design and safety decisions.

Moreover, the analysis showed that system reliability and minimal cut set ranking are sensitive to the selected α values in the Alpha Factor method, which is particularly effective for mid- and lower-ranked minimal cut sets. This was confirmed through comparisons using different datasets, and highlights the importance of careful selection of Alpha Factor inputs in reliability assessments.

To further investigate the effect of common cause failures, a separate sensitivity analysis was performed across a wide range of individual component failure probabilities for systems with varying levels of redundancy. The results showed that as individual failure probabilities increases, the contribution of common cause failures decreases, and individual failure probability become the more dominant contributors in determining system failure. The impact of common cause failures diminishes more rapidly in systems with lower redundancy. This highlights the import of accurately modeling system failure by taking into account both the individual failure probabilities and redundancy levels. As neglecting either may result in underestimating the overall system failure probability.

In general, the application of the new approach is particularly relevant for highly redundant systems which include many identical components, such as those in safety-related systems of nuclear power plants. Further improvement of the new approach may depend on acquiring more detailed data related to the common cause factors, i.e., the underlying root causes and coupling mechanisms, beyond what is captured by the failure mode alone.

Acknowledgment

This work was supported by the National Science Centre (NCN) in Poland through the Grant No. DEC-2024/08/X/ST8/00283. Partial support was also provided by the Slovenian Research Agency under the research program P2-0356. The first author gratefully acknowledges the opportunity to carry out this research during a three month stay at the Faculty of Electrical Engineering, University of Ljubljana.

References

[1] W. E. Vesely, F. F. Goldberg, N. H. Roberts, D. F. Haasl, Fault tree handbook, Technical Report NUREG-0492, US Nuclear Regulatory Commission, Washington, DC (1981).

[2] M. Čepin, Assessment of power system reliability: methods and applications, Springer Science & Business Media, 2011.

[3] A. Mosleh, Common cause failures: an analysis methodology and examples, Reliab Eng Syst Saf 34 (3) (1991) 249–292.

[4] K. C. Chae, G. M. Clark, System reliability in the presence of common-cause failures, IEEE Trans Reliab 35 (1) (1986) 32–35.

[5] H. Jones, Common cause failures and ultra reliability, in: 42nd International Conference on Environmental Systems, 2012, p. 3602.

[6] H. Bao, H. Zhang, T. Shorthill, E. Chen, S. Lawrence, Quantitative evaluation of common cause failures in high safety-significant safety-related digital instrumentation and control systems in nuclear power plants, Reliab Eng Syst Saf 230 (2023) 108973.

[7] J. K. Vaurio, The probabilistic modeling of external common cause failure shocks in redundant systems, Reliab Eng Syst Saf 49 (1) (1995) 15–22.

[8] J. K. Vaurio, Common cause failure probabilities in standby safety system fault tree analysis with testing—scheme and timing dependencies, Reliab Eng Syst Saf 79 (1) (2003) 43–57.

[9] J. K. Vaurio, Availability of redundant safety systems with common-mode and undetected failures, Nucl Eng Des 58 (3) (1980) 415–424.

[10] J. E. Ramirez-Marquez, D. W. Coit, Optimization of system reliability in the presence of common cause failures, Reliab Eng Syst Saf 92 (10) (2007) 1421–1434.

[11] C. Tanguy, Importance measures and common-cause failures in network reliability, in: G. Bérenguer, G. Soares (Eds.), Advances in safety, reliability and risk management, Taylor & Francis Group, London, 2012, pp. 1052–1059.

[12] A. Mosleh, G. W. Parry, H. M. Paula, D. H. Worledge, D. M. Rasmuson, Procedures for treating common cause failures in safety and reliability studies, Tech. Rep. NUREG/CR-4780, Vol.1, US NRC, Washington, DC (1981).

[13] A. Mosleh, G. W. Parry, H. M. Paula, D. H. Worledge, D. M. Rasmuson, Procedures for treating common cause failures in safety and reliability studies, Tech. Rep. NUREG/CR-4780, Vol.2, US NRC, Washington, DC (1989).

[14] A. Mosleh, D. M. Rasmuson, F. M. Marshall, Guidelines on modelling common-cause failures in pra, Tech. Rep. NUREG/CR-5485, US NRC, Washington, DC (1998).

[15] D. Kančev, M. Čepin, A new method for explicit modelling of single failure event within different common cause failure groups, Reliab Eng Syst Saf 103 (2012) 84–93.

[16] Ž. Bricman Rejc, M. Čepin, An extension of multiple greek letter method for common cause failures modeling, in: J Loss Prevent Proc, Vol. 29, 2014, pp. 144–154.

[17] A. O'Connor, A. Mosleh, Extending the alpha factor model for cause based treatment of common cause failure events in pra and event assessment, in: Proceedings of the 12th probabilistic safety assessment & management conference (PSAM12), 2014.

[18] A. O'Connor, A. Mosleh, A general cause based methodology for analysis of common cause and dependent failures in system risk and reliability assessments, Reliab Eng Syst Saf 145 (2016) 341–350.

[19] T. D. Le Duy, D. Vasseur, A practical methodology for modeling and estimation of common cause failure parameters in multi-unit nuclear psa model, Reliab Eng Syst Saf 170 (2018) 159–174.

[20] D.-S. Kim, J. H. Park, H.-G. Lim, A pragmatic approach to modeling common cause failures in multi-unit psa for nuclear power plant sites with a large number of units, Reliability Engineering & System Safety 195 (2020) 106739.

[21] M. Čepin, B. Mavko, A dynamic fault tree, Reliab Eng Syst Saf 75 (1) (2002) 83–91.

[22] M. Čepin, Analysis of truncation limit in probabilistic safety assessment, Reliab Eng Syst Saf 87 (3) (2005) 395–403.

[23] T. Wierman, D. Rasmuson, A. Mosleh, Common cause failure database and analysis system: event data collection, classification, and coding, Tech. Rep. NUREG/CR-6268, US NRC, Washington, DC (2007).

[24] U. NRC, CCF parameter estimations, 2020 update, Inl/ext-21-62940 revision 1 (Novemer 2021).

[25] US-APWR design description, mitsubishi Heavy Industries, Ltd. (October 2006).

[26] Z. Ma, T. E. Wierman, K. J. Kvarfordt, Industry-average performance for components and initiating events at U.S. commercial nuclear power plants: 2020 update, Tech. Rep. INL/EXT-21-65055, Idaho National Laboratory (November 2021).

[27] IAEA, Reliability data for research reactor probabilistic safety assessment: final results of a coordinated research project, Tech. Rep. IAEA-TECDOC-1922, Vienna, Austria (2020).

[28] U.S. NRC, CCF parameter estimations, 2009 Update, Tech. rep. (April 2011).