ISA Transactions 118 (2021) 35–43

Contents lists available at ScienceDirect

ISA Transactions

journal homepage: www.elsevier.com/locate/isatrans

Research article

Performance assessment of K-out-of-N safety instrumented systems subject to cascading failures

Lin Xie [a], Mary Ann Lundteigen [b], Yiliu Liu [a,*]

[a] *Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, 7491, Trondheim, Norway*
[b] *Department of Engineering Cybernetics, Norwegian University of Science and Technology, 7491, Trondheim, Norway*

ARTICLE INFO

Article history:
Received 21 November 2018
Received in revised form 10 February 2021
Accepted 10 February 2021
Available online 15 February 2021

Keywords:
Safety instrumented systems
Cascading failures
K-out-of-N configuration
Performance assessment
Average probability of failure on demand

ABSTRACT

Safety instrumented systems often employ redundancy to enhance the ability to detect and respond to hazardous events. The use of redundancy increases the fault tolerance to single failure but remains vulnerable in case of dependent failures, including common cause failures and cascading failures. Reliability analysis of safety instrumented systems therefore involves the impact of dependent failures. The used approaches have primarily focused on common cause failures. In this paper, it is argued the need to consider the efforts of cascading failures that are caused by functional dependencies, hazardous events, and shared resources. A recursive aggregation-based approach is proposed for performance analyzing of K-out-of-N safety instrumented systems with consideration of cascading failures. General approximation formulas are developed for estimating the average probability of failures on demand of different configurations of safety instrumented systems. These formulas are compared with those for common cause failures. Then a case of fire water pump is studied to illustrate the effects of cascading failures on safety instrumented systems.

1. Introduction

Safety instrumented systems (SISs) are employed to prevent hazardous events and mitigate damages in diverse industries, including but not limited to process and nuclear power plants, and oil and gas facilities. A SIS is characterized as a system that relies on electrical/electronic/programmable electronic (E/E/PE) technologies to detect abnormal situations [1]. A SIS performs one or more safety instrumented functions (SIFs) to protect the equipment under control (EUC) [2]. It often consists of one or more components (such as sensors, gas detectors), logic solvers (such as programmable logic controller) and final elements (such as circuit breakers). Considering a process shutdown system as an example of SISs, it performs its safety function as following: In case of process upsets, the sensors of the SIS s detect possible abnormal situations. The sensors will send the alarm information to the logic solver(s), which can activate the final elements, shutdown valves, to stop production [3].

According to the standards IEC 61508 [1] and IEC 61511 [2], performance requirement on a SIS is often assigned to each SIF and reliability assessment is carried out to prove compliance to the requirement [1,2]. It is stated that the SIFs performed by a SIS must fulfill specified safety integrity levels (SILs). Four different SILs are defined in accordance with the average probability of failure on demands ($\mathrm{PFD}_{\mathrm{avg}}$), ranging the safety integrity from SIL 1 (the lowest level) to SIL4 (the highest level). $\mathrm{PFD}_{\mathrm{avg}}$ is the performance measure for SISs operating in the low-demand mode [1]. It can also be interpreted as a mean proportion of time that the item is not able to perform its specified SIF in a certain period or a long term [4]. $\mathrm{PFD}_{\mathrm{avg}}$ may be calculated on the basis of several methods: simplified formulas based on fault tree analysis (FTA) [4], IEC 61508 formulas [1], PDS method [5], and Markov methods [6].

To reduce $\mathrm{PFD}_{\mathrm{avg}}$, it is often effective to introduce redundancy, such as K-out-of-N (*KooN*) configurations, into a SIS subsystem. *KooN* means that the subsystem with N parallel components is available when at least K components are functioning. A typical SIS in the oil & gas industry, high-integrity pressure protection system (HIPPS), can comprise a *2oo3* configuration of pressure transmitters, a *1oo1* configuration of logic solver, and a *1oo2* configuration of shutdown valves. The HIPPS does not terminate its SIF until there are two or more failures on transmitters, one failure on the logic solver, or two failures on the valves. Such kind of configurations normally can increase the reliability and availability of systems. This redundancy often brings dependent failures, which occur on multiple components with functional dependencies and shared resources [7]. IEC 61508 [1], ISO/TR 12489 [8] and PDS ("Reliability of SIS" in Norwegian) handbook [5] have indicated that the effects of dependent failures on the performance of SISs should be considered. Biswal et al. have

[*] Corresponding author.
E-mail address: yiliu.liu@ntnu.no (Y. Liu).

https://doi.org/10.1016/j.isatra.2021.02.015

proposed approaches based on FTA for redundant structure in production systems like hydrogen cooling systems [9]. However, it is difficult to straightforwardly use by such traditional methods like FTA, IEC 61508 formulas and Markov to deal with dependent issues with SISs [10–12].

IEC 61508 and relevant literature focus primarily on common cause failures (CCFs) as dependent failures. CCFs are characterized by the failures of two or more components fail due to the same reasons [1]. They can be modeled by the standard and the multiple beta-factor model incorporated with FTA, PDS method and Markov model in $\mathrm{PFD}_{\mathrm{avg}}$ calculation [5,12]. Cascading failures (CAFs) are another type of dependent failures, reflecting the multiple failures that one component's failure results in chain reactions [12]. The differences between cascading and CCFs in interdependences and propagation mechanisms have been discussed in the previous work [13]. CCFs are the failures that are first in line and directly linked to the failure causes, while the propagation of CAFs follows a series of interactions. Therefore, the models for assessing performance of SISs with CCFs are not applicable for the SISs with CAFs.

SISs are vulnerable to CAFs that are originated from the reliance on shared loads, shared testing and maintenance resources, hazardous events, and dependent functions [13,14]. For example, several components are configured in parallel in a flow transmission system sharing maintenance resources. The failure of one component may occupy the maintenance resource, decrease the possibilities of maintenances on other components, and then trigger more failures [14]. Another example is a fire water supply system where the pumps are operating in a $K$oo$N$ configuration. When one of the pumps fails, the corresponding pipeline is closed, and other pumps must carry the whole loads. The probabilities of failures-to-start of the other pumps thereby increase. Many researchers analyze the impacts of CAFs on general systems based on different theory and models including but not limited to complex network [15–18], risk analysis [19–22], probabilistic analysis [23,24] and maintenance optimizations [25,26].

Nevertheless, performance assessment of SISs that are subject to CAFs is seldom explored. SISs are such a kind of systems whose SIFs are only be activated upon abnormal situations. Since SISs are not running all the time in the low demand operational mode, many failures cannot be detected immediately after their occurrences. These so-called hidden failures can be both independent- and dependent-failures. Periodical proof tests, such as once per year, are conducted in many process plants to reveal hidden failures of SISs, but with noticeable delays. Performance assessment of SISs thus needs specific measures, such as $\mathrm{PFD}_{\mathrm{avg}}$ for low demand mode of SISs. The value of $\mathrm{PFD}_{\mathrm{avg}}$ is not only related with the internal properties of a SIS, but also related with the frequency and effectiveness of proof tests (see [1,2] and [4]). These particularities distinguish SISs from production or general systems and impede the adaption of the existing approaches for CAF analysis to SISs.

Therefore, the objective of this paper is to introduce the approaches for incorporating CAFs into performance assessment of SISs: (1) A generalized approach based on recursive aggregation for reliability analysis of SISs subsystems voted *KooN*. (2) Approximation formulas for performance assessment of most common configuration SISs. The approximation formulas may be considered for the standards with respect to SISs, such as IEC 61508 and ISO TR 12489, as a complement to the existing formulas for performance assessment of SISs.

The rest of the paper is organized as follows: Section 2 discusses the considerations in SIS performance assessment and the basic analysis approaches for CAFs. Section 3 presents an approach based on recursive aggregations for reliability analysis of SISs that subject to CAFs, and Monto Carlo Simulation is adopted to verify the numerical results. Section 4 introduces approximation formulas for evaluating the performance of SISs with general configurations, and Section 5 illustrates the approach and the effects of CAFs with a case study. Finally, a discussion is presented, and further works are discussed in Section 6.

2. Considerations in assessing SISs with CAFs

It is important to clarify the characteristics of CAFs and SISs before quantitative analysis, in consideration that many arguments still exist.

2.1. Failures and performance measures of SISs

IEC 61508 splits the failures of SISs into two groups [1]: dangerous failures and safe failures. Owing to many automatic diagnosis functions in SISs, some dangerous failures can be found immediately when they occur, as dangerous detected (DD) failures, but some other failures are hidden after occurrence for some time, as dangerous undetected (DU) failures. DU failures are more of interests in many studies including this paper, because DU failures are the main contributors to the unavailability of SISs and only can be revealed by proof tests or when a demand/shock occurs [4]. A proof test is a periodic test performed to detect DU failures in SISs so that, if necessary, a repair can restore the system to an 'as-good-as-new' condition or as close as practical to this condition. In case of DU failures, the SISs cannot activate when a demand comes, and a disaster may therefore occur.

Performance of a SIS is often measured by $\mathrm{PFD}_{\mathrm{avg}}$ if the SIS is in low demand mode, namely the demand rate is less than once per year according to IEC 61508 [2]. $\mathrm{PFD}_{\mathrm{avg}}$ of subsystems (sensors, logical solvers, and final elements) is dependent on DU failure rates of components, system configurations, and frequency and effectiveness of tests and maintenances. The overall $\mathrm{PFD}_{\mathrm{avg}}$ of a SIS is a sum of the values of $\mathrm{PFD}_{\mathrm{avg}}$ of its three subsystems. The rest parts of this paper will be limited to the SIS subsystems in low-demand modes, concerning DU failures and $\mathrm{PFD}_{\mathrm{avg}}$ in the quantification of SILs. For the assessment of SISs in other demand modes and the applicability of $\mathrm{PFD}_{\mathrm{avg}}$, readers can find more information in [6,27].

2.2. CAFs analysis

CAFs appear in the current literatures with different names, including induced failures, domino failures, and propagating failures [19,25,28]. Rausand and Høyland [12] define CAFs as the multiple failures that the failure of one component result in a chain reaction. Murthy and Nguyen regard CAFs as the failures that affect the remaining components in a system [25]. Hauge et al. [9] view CAFs as the escalating failures that one or more components fail caused by failures of other components. Although there is no standard definition for CAFs, researchers have some common agreements that CAFs start from one component and spread to more in the system. On the contrary, there are some failures whose occurrence probabilities are irrelevant with other components [4], like, an age-related failure. In this paper, such failures are called as independent failures or self-failures, and their occurrences are irrelevant with other components.

For subsystems in a SIS, especially for sensor- and final element subsystems, it is common that identical components are installed in a voting structure. These components can suffer from the same hazardous events and are monitored with the same mechanism. Thus, the dependency among these components, as the root cause of CAFs, is difficult to be avoided.

In this study on the performance assessment of SISs, the following assumptions are existing:

(1) All the components in a subsystem of SISs are identical and unrepairable.
(2) Only two states account for all the components: either functioning or failed.
(3) An independent/self-failure of a component is characterized by a distribution function $F(t)$, and the time to failures is assumed as an exponential distribution, namely the component has a constant failure rate λ. Other distributions, such as Weibull distribution for many mechanical systems can also be considered.

Considering the particulars of CAFs, additional assumptions are needed in analysis:

(1) Any component can lose its SIF due to a self-failure or the cascading impact of the failures of other components.
(2) Propagation duration of CAFs is rather short and can be ignored.

We use cascading intensity $\gamma_{ij}(t) \in (0,1]$ $(i \neq j)$ to reflect the easiness of failure propagation from component i to component j. In mathematics, the cascading intensity is expressed as the conditional failure probability of component j when component i fails by time t:

$$\gamma_{ij}(t) = \Pr(\text{comp. } j \text{ fails by } t \mid \text{comp. } i \text{ has failed by } t) \tag{1}$$

The value of cascading intensity $\gamma_{ij}(t)$ can be estimated by either parametric or nonparametric techniques based on historic data. It is not difficult to identify cascading failures that origin from a failure in another component from review of maintenance notifications in case of adequate and detailed failure causes descriptions. The probability $\gamma_{ij}(t)$ is arranged as a matrix $\boldsymbol{\gamma}$ that represents failure propagation between the components. The probabilities escaping from CAFs are $\delta_{ij}(t) = 1 - \gamma_{ij}(t)$. With the assumption of exponential distributions, $\gamma_{ij}(t)$ and $\delta_{ij}(t)$ can be simplified as two constants γ_{ij} and δ_{ij}, or even γ and δ for identical components in the rest parts of this paper.

3. SIS reliability analysis with CAFs

The performance assessment often starts from reliability analysis based on probabilistic theory and models [12]. This section suggests a system reliability analysis approach of *KooN* configurations subject to CAFs. Then, Monte Carlo simulation is used to check whether the analytical results are appropriate or not.

3.1. The recursive aggression-based approach

The reliability of the systems in parallel and in series that are affected by CAFs has been discussed in [26]. For many traditional reliability methods, such as fault tree, they are not effective in dealing with failures with dependencies. In this section, we extend the research to SISs, and to more general configurations, namely *KooN* voting structures. A recursive aggregation-based approach proposed can be applicable for analyzing systems with several components and many CAFs propagation paths. Recursive aggregation means that evaluation is repeated for each combination of the components in the systems.

Let $F_\Omega(t_a, t)$ express a probability that the system Ω ($\Omega = [1, 2 \ldots \mathrm{n}]$) fails by time t, conditioned on that all the component in the system Ω is functioning by time t_a. Let $\mathrm{G}_\Omega(t_i, t)$ denote the probability that the system Ω fails in $[t_i, t]$ given that component i fails at time t_i. The failure probability of the system Ω is obtained:

$$F_\Omega(t_\mathrm{a}, t) = \sum_{i\in\Omega} \int_{t_\mathrm{a}}^{t} \mathrm{G}_\Omega(t_i, t) \prod_{\mathrm{j}\neq\mathrm{i}, \mathrm{j}\in\Omega} \mathrm{R}_{\mathrm{jm}}(\mathrm{t}) \Big/ \prod_{\mathrm{j}\in\Omega} \mathrm{R}_\mathrm{j}(\mathrm{t_a})\, \mathrm{d}F_i(t_i) \tag{2}$$

where R_{j_m} (t) denotes the reliability of component $j_m(\forall j_m \in \Omega - \mathrm{i}, m \in [1, 2, \ldots, n-k-1])$ at time t. $F_i(t_i)$ denotes the failure probability because of independent /self-failures. $G_\Omega(t_i, t)$ is given by:

$$\begin{aligned} G_\Omega(t_i, t) = {} & \Pr(n_c = 0) F_{\Omega-\{\mathrm{i}\}}(t_i, t) \\ & + \sum_{j_1 \in \Omega - \{\mathrm{i}\}} \Pr(n_c = 1) F_{\Omega - \{\mathrm{i}, j_1\}}(t_i, t) \\ & + \sum_{j_1, j_2 \in \Omega - \{\mathrm{i}\}} \Pr(n_c = 2) F_{\Omega - \{\mathrm{i}, j_1, j_2\}}(t_i, t) \ldots \\ & + \sum_{j_1, j_2 .. j_{n-k-1} \in \Omega - \{\mathrm{i}\}} \Pr(n_c = n-k-1) \\ & \times F_{\Omega - \{\mathrm{i}, j_1, j_2 .. j_{n-k-1}\}}(t_i, t) + \Pr(n_c \geq n-k) \end{aligned} \tag{3}$$

where n_c denotes the number of CAFs. $\mathrm{P_r}(n_c)(m \in [0, 1, 2, \ldots, n-k-1])$ denotes the probability that the system is subject to CAFs with number of n_c. All the components in the SIS subsystem are identical and $\mathrm{P_r}(n_c)$ can be expressed as:

$$\Pr(n_c) = \binom{n_c}{n-1} \delta^{n-n_c-1} \gamma^{n_c} \tag{4}$$

In consideration of the exponential distribution assumption, the starting point of the study, t_a, can be regarded as zero when the system like $\Omega - \{i\}$, $\Omega - \{i, j_m\}$ is regarded as a new system Ω. $F_s(t)$ denotes failure probability of system Ω, and $F_s(t) = F_\Omega(t) = F_\Omega(0, t)$.

The failure rates for all the components are λ. Hence, the system failure probability $F_s(t)$ can be obtained by using Eqs. (3) and (4) when $t_a = 0$:

$$\begin{aligned} F_s(t) = F_\Omega(t) = n \Bigg[& \delta^{n-1} F_{\Omega-1}(t) + \binom{1}{n-1} \delta^{n-2} \gamma F_{\Omega-2}(t) \\ & + \binom{2}{n-1} \delta^{n-3} \gamma^2 F_{\Omega-2}(t) + \cdots \\ & + \binom{n-k-1}{n-1} \delta^k \gamma^{n-k-1} F_{\Omega-(n-k-1)}(t) \\ & + \left(\binom{n-k}{n-1} \delta^{k-1} \gamma^{n-k} \right. \\ & + \binom{n-k-1}{n-1} \delta^{k-2} \gamma^{n-k+1} \ldots \\ & \left. + \binom{n-1}{n-1} \gamma^{n-1} \right) \Bigg] \end{aligned} \tag{5}$$

The failure probability $F_{\Omega_m}(t_m, t)$ for any subsystem Ω_m is obtained in a similar way by using Eqs. (4) and (5). This aggregation stops when there are more than *N-K*-1 failures in Ω_m. Then, the failure probability of this subsystem is $F_{\Omega-(n-k-1)}(t) = 1 - e^{-k\lambda t}$.

The convolution and Laplace transformation is used to facilitate integration of system failure probabilities in Eq. (2) [12]. We obtained:

$$\mathcal{L}[F_S(t)] = \mathcal{L}[G_\Omega(t)]\, \lambda/(S + n\lambda) \tag{6}$$

......

$$\mathcal{L}\left[F_{\Omega-(n-k-1)}(t)\right] = \frac{1}{S} - \frac{1}{S + k\lambda} \tag{7}$$

Then, the system failure probability $F_s(t)$ and system reliability $R(t)$ can be obtained by inverting Laplace transforms.

3.2. Verification with Monte Carlo simulations

To examine whether the analytical algorithms are appropriate, Monte Carlo (MC) simulations are conducted in MATLAB in this

Table 1
Inputs parameters for the models.

Parameter	Values
γ	0.1, 0.2 and 0.5
λ	2.0×10^{-6} per hour
t	2.5×10^4 hours

section. Two typical configurations of SIS subsystems, *2oo3* and 1oo3 voting structures, have been chosen as examples for formula verification. For a *2oo3* configuration, its reliability can be obtained by Eqs. (3)–(7) as:

$$R(t) = 3\delta^2 e^{-2\lambda t} + (1 - 3\delta^2)e^{-3\lambda t} \tag{8}$$

Similarly, the reliability of a 1oo3 configuration can be obtained as:

$$\begin{aligned} R(t) = {} & 3\delta(1 - \delta\gamma)\, e^{-\lambda t} + 3\delta^2(2\gamma - 1)e^{-2\lambda t} \\ & + (1 - 3\delta(1 - \delta\gamma) - 3\delta^2(2\gamma - 1))e^{-3\lambda t} \end{aligned} \tag{9}$$

Fig. 1 shows the flowchart of MC simulation for CAFs propagation. $T_i(\lambda)$ denotes random exponential variables. They are the time to failure of component i with λ failure rate. Let P_{ij} denote a random variable that is generated from a uniform distribution in [0, 1]. It is limited by γ_{ij} that represents the propagated probability from component i to component j. $T_s(t)$ denotes the simulated time to system failures.

To verify the proposed algorithms, without losing generality, it is assumed that γ_{ij} has fixed values of 0.1, 0.2 and 0.5 respectively for all cascades between components. The time to independent/self-failures $F_i(t)$ is exponentially distributed with a constant failure rate of 2.1×10^{-6} per hour. We run Monte Carlo simulations over a period of 2.5×10^4 hours with 10^5 iterations. Inputs of the parameters are summarized in Table 1.

The results of system reliability for *2oo3* and *1oo3* configurations using analytical approach and MC simulation are presented in Figs. 2 and 3.

As seen, the results using analytical formulas give the almost same results as the MC simulations of *2oo3* and *1oo3* configurations. That gives the confidence on the proposed approach for further reliability analysis of *KooN* SISs subject to CAFs.

4. Analysis for PFD$_{\text{avg}}$ and approximation formulas

In this section, the reliability analysis results can be transformed to PFD$_{\text{avg}}$. Moreover, to simplify the calculations and analyses in practices, approximation formulas for PFD$_{\text{avg}}$ of a SIS subsystem with consideration of CAFs are summarized. Then, we have compared of these approximation formulas for CAFs with those for CCFs.

4.1. PFD$_{\text{avg}}$ *With CAFs*

PFD$_{\text{avg}}$ is the average probability that the component is not able to react and perform its safety function in response to the demand. Such a measure relates to the time dependent unavailability (PFD (t)) in a proof test interval, denoted by τ. PFD (t) can be expressed as in [4]:

$$\begin{aligned} \text{PFD}(t) &= \Pr(\text{a DU failure has occurred at or before time } t) \\ &= \Pr(T \le t) = F(t) \end{aligned} \tag{10}$$

The long-run average PFD$_{\text{avg}}$ is equal to the average value of PFD (t) in the first proof test interval $(0, \tau)$:

$$\text{PFD}_{\text{avg}} = \frac{1}{\tau}\int_0^\tau \text{PFD}(t)dt = \frac{1}{\tau}\int_0^\tau F(t)dt = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt \tag{11}$$

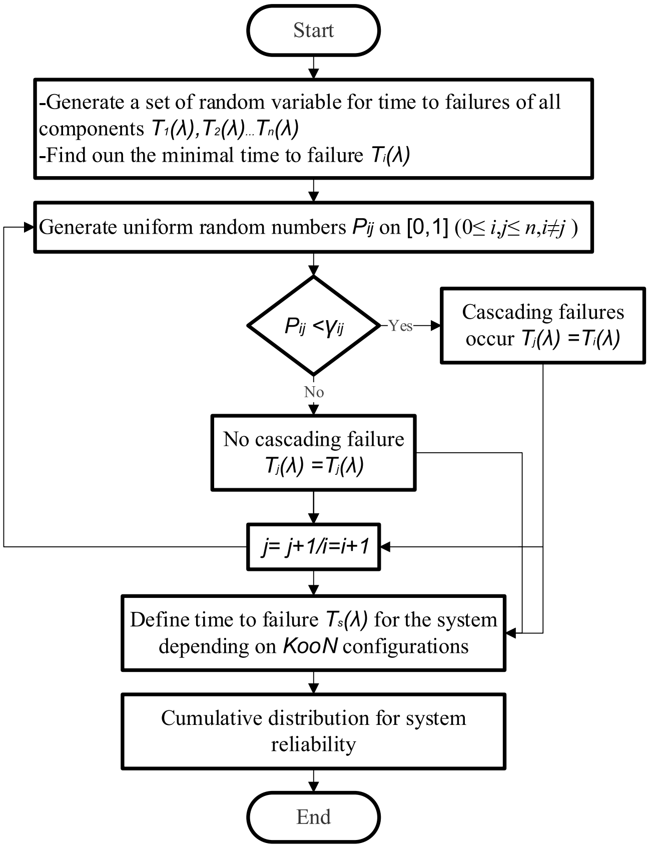
Start
-Generate a set of random variable for time to failures of all components $T_1(\lambda),T_2(\lambda)...T_n(\lambda)$
-Find oun the minimal time to failure $T_i(\lambda)$
Generate uniform random numbers P_{ij} on [0,1] ($0\le i,j\le n,i\neq j$)
$P_{ij} <\gamma_{ij}$
Yes
Cascading failures occur $T_j(\lambda) =T_i(\lambda)$
No
No cascading failure $T_j(\lambda) =T_j(\lambda)$
$j= j+1/i=i+1$
Define time to failure $T_s(\lambda)$ for the system depending on KooN configurations
Cumulative distribution for system reliability
End

Fig. 1. Flowchart of MC simulation of CAFs propagation.

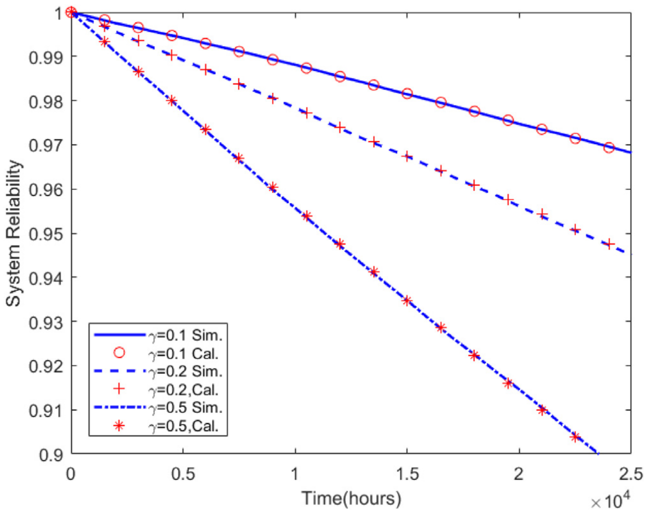

Fig. 2. Simulated and analytical system reliability for 2oo3 configuration.

where τ denotes the length of proof test interval.

Reconsider the two systems, namely *2oo3* and *1oo3* configurations, with all components having a constant DU failure rate λ and cascaded failure probability γ $(\delta = 1 - \gamma)$ between any two components. Based on system reliability obtained in Section 3, PFD$_{\text{avg}}$ of the *2oo3* configuration can be expressed as:

$$\text{PFD}_{\text{avg}}{}^{(2oo3)} = 1 - \frac{1}{\tau}\int_0^\tau R(t)\,dt$$

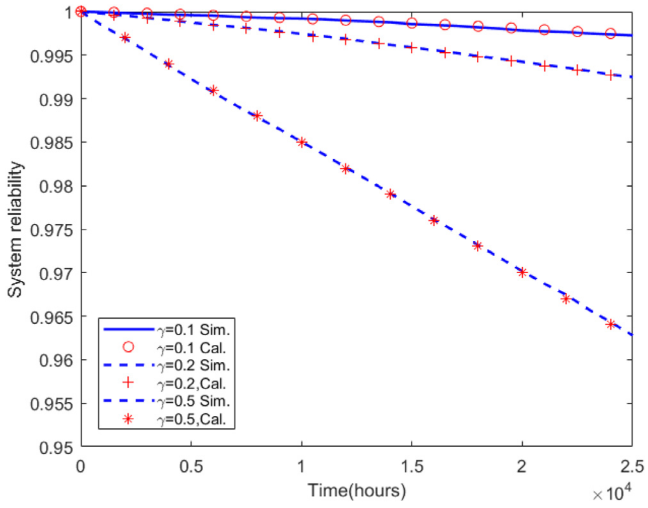

Fig. 3. Simulated and analytical system reliability for *1oo3* configuration.

Table 2
Approximation formulas for PFD$_{avg}$ with CAFs.

K/N	$N=1$	$N=2$	$N=3$	$N=4$
$K=1$	$\lambda\tau/2$	$2\gamma\cdot\lambda\tau/2$	$3\gamma^2\cdot\lambda\tau/2$	$4\gamma^3\cdot\lambda\tau/2$
$K=2$	–	$\lambda\tau$	$3\gamma(2-\gamma)\cdot\lambda\tau/2$	$4\gamma^2(3-2\gamma)\cdot\lambda\tau/2$
$K=3$	–	–	$3\lambda\tau/2$	$4\gamma(3-3\gamma+\gamma^2)\cdot\lambda\tau/2$
$K=4$	–	–	–	$2\lambda\tau$

$$= 1 - \int_0^\tau (3\delta^2 e^{-2\lambda t} + (1-3\delta^2)e^{-3\lambda t})dt$$

$$= 1 - \frac{3\delta^2}{2\lambda\tau}\left(1-e^{-2\lambda t}\right) - \frac{(1-3\delta^2)}{3\lambda\tau}\left(1-e^{-3\lambda t}\right) \quad (12)$$

Since SIS components are always highly reliable, λ is a rather small number. Given that $\lambda\tau$ is small (<0.1), we can replace $e^{-2\lambda t}$ and $e^{-3\lambda t}$ by using Taylor series deployment:

$$\mathrm{PFD_{avg}}^{(2oo3)} = 1 - 3\delta^2\left(1 - \frac{2\lambda\tau}{2} + \frac{(2\lambda\tau)^2}{3!}\ldots\right) - \left(1-3\delta^2\right)\left(1 - \frac{3\lambda\tau}{2} + \frac{(3\lambda\tau)^2}{3!}\ldots\right) \approx 3\left(1-\delta^2\right)\frac{\lambda\tau}{2} \quad (13)$$

While for the 1oo3 configuration, the PFD$_{\text{avg}}$ can be obtained as:

$$\mathrm{PFD_{avg}}^{(1oo3)} \approx 3\gamma^2\frac{\lambda\tau}{2} \quad (14)$$

4.2. Generalized formulas for PFD$_{\text{avg}}$ with CAFs

With the same approach, PFD$_{\text{avg}}$ for other *KooN* systems can be obtained. PFD$_{\text{avg}}$ of some simple *KooN* (n ≤ 4) systems are listed in Table 2.

When cascaded failure probability γ is small (for example when $\gamma \le 0.2$), $\gamma^2, \gamma^3, \gamma^4 \ldots$ are negligible. Therefore, simplified formulas for *PFD$_{avg}$* is presented in Table 3.

By observing the values in Table 3, a general approximation formula for PFD$_{\text{avg}}$ of any *KooN* configurations is summarized as:

$$\mathrm{PFD_{avg}}^{(KooN)} = \left(\begin{array}{c} N-1 \\ K-1 \end{array}\right) N\gamma^{N-K}\frac{\lambda\tau}{2} \quad (15)$$

The general formula is more meaningful for practitioners of SISs, because it can provide enough information only with some simple input numbers.

Table 3
Approximation formulas for PFD$_{avg}$ with CAFs after simplification.

K/N	$N=1$	$N=2$	$N=3$	$N=4$
$K=1$	$\lambda\tau/2$	$2\gamma\cdot\lambda\tau/2$	$3\gamma^2\cdot\lambda\tau/2$	$4\gamma^3\cdot\lambda\tau/2$
$K=2$	–	$\lambda\tau$	$6\gamma\cdot\lambda\tau/2$	$12\gamma^2\cdot\lambda\tau/2$
$K=3$	–	–	$3\lambda\tau/2$	$12\gamma\cdot\lambda\tau/2$
$K=4$	–	–	–	$2\lambda\tau$

Table 4
Factors σ_{KooN} for different configurations.

K/N	$N=2$	$N=3$	$N=4$	$N=5$
$K=1$	2γ	$3\gamma^2$	$4\gamma^3$	$5\gamma^4$
$K=2$	–	6γ	$12\gamma^2$	$20\gamma^3$
$K=3$	–	–	12γ	$30\gamma^2$
$K=4$	–	–	–	20γ

Table 5
$\sigma_{koon}(\gamma = 0.05)$ for CAFs in different configurations.

σ_{koon}	$N=2$	$N=3$	$N=4$	$N=5$
$K=1$	1.0×10^{-1}	7.5×10^{-3}	5.0×10^{-4}	3.1×10^{-5}
$K=2$	–	3.0×10^{-1}	3.0×10^{-2}	2.5×10^{-3}
$K=3$	–	–	6.0×10^{-1}	7.5×10^{-2}
$K=4$	–	–	–	10.0×10^{-1}

The validity of such a general formula needs to be examined. A more complicate system of *3oo5* configuration is concerned. The system reliability of the 3oo5 configuration subject to CAFs can be expressed as:

$$R(t) = (10\delta^3\gamma + 10\delta^7)e^{-3\lambda t} + (5\delta^4 - 20\delta^7)e^{-4\lambda t} + \left[1 - (10\delta^3\gamma + 10\delta^7) - (5\delta^4 - 20\delta^7)\right]e^{-5\lambda t} \quad (16)$$

PFD$_{\text{avg}}$ of 3oo5 configuration is found to be:

$$\mathrm{PFD_{avg}}^{(3oo5)} = 1 - \frac{1}{\tau}\int_0^\tau R(t)\,\mathrm{d}t = 5\gamma^2\left(6 - 8\gamma + 3\gamma^2\right)\frac{\lambda\tau}{2} \approx 30\gamma^2 * \frac{\lambda\tau}{2} = \left(\begin{array}{c} 5-1 \\ 3-1 \end{array}\right) 5\gamma^{5-3}\frac{\lambda\tau}{2} \quad (17)$$

The result matches the general formula Eq. (15) that is proposed in this subsection.

4.3. Comparisons of formulas for CCFs and CAFs

In the PDS handbook [5], PFD$_{\text{avg}}$ of SISs subject to CCFs have also been summarized to be approximation formulas relevant with configurations. Here we compare the formulas for PFD$_{\text{avg}}$ considering CCFs and CAFs. A factor σ_{KooN} is introduced to distinguish the effects of CAFs on the value of PFD$_{\text{avg}}$ among various configurations. Based on Eq. (15), the factors σ_{KooN} for CAFs in different configurations are summarized in Table 4.

PFD$_{\text{avg}}$ of the *KooN* configurations subject to CAFs is therefore calculated as:

$$\mathrm{PFD}_{\mathrm{avg(CAF)}}^{KooN} = \sigma_{KooN}\frac{\lambda\tau}{2} \quad (18)$$

The factor C_{KooN} is used to describe the effects of CCFs [5]. The general formula for PFD$_{\text{avg}}$ is expressed as [5]:

$$\mathrm{PFD}_{\mathrm{avg(CCF)}}^{KooN} = C_{KooN}\beta\frac{\lambda\tau}{2} \quad (19)$$

To compare the effects of two factors, γ and β are assigned as 0.05 as an example. The factors σ_{KooN} and C$_{KooN}\beta$ for different configurations are illustrated in Tables 5 and 6.

Table 6
$C_{koon}\beta(\beta = 0.05)$ for CCFs in different configurations.

$C_{\mathrm{MooN}}\beta$	$N = 2$	$N = 3$	$N = 4$	$N = 5$
$K = 1$	5×10^{-2}	2.5×10^{-2}	1.5×10^{-2}	1.0×10^{-2}
$K = 2$	–	1.0×10^{-1}	5.5×10^{-2}	4.0×10^{-2}
$K = 3$	–	–	1.4×10^{-1}	8.0×10^{-2}
$K = 4$	–	–	–	1.8×10^{-1}

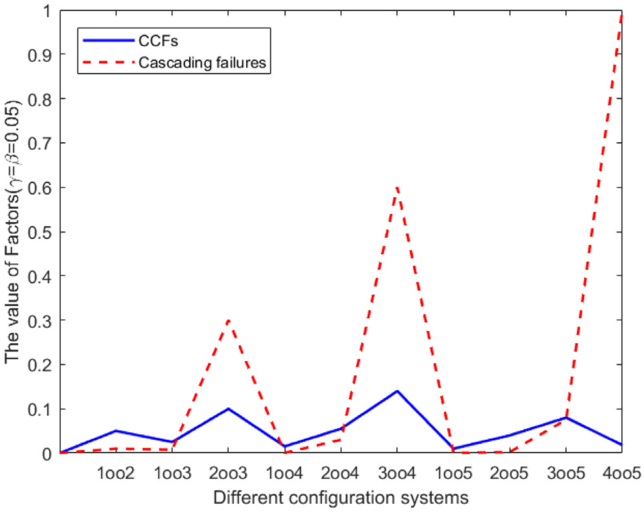

Fig. 4. Comparison of the factors for CCFs and CAFs.

Apparently, the value of factor σ_{KooN} for CAFs is higher than that of $C_{KooN}\beta$ for CCFs, when K is close to N, for example N-K is equal to 1, as shown in Fig. 4. This deviation can be explained that the value of $C_{KooN}\beta$ for CCFs is constant, whereas σ_{KooN} for CAFs relies on γ^{N-K}. Fig. 4 indicates that the curve of CAFs fluctuates much more than that of CCFs, in other words the effects of CAFs towards $\mathrm{PFD_{avg}}$ are more likely to rely on configurations. Such a phenomenon with case studies is explored in the next section.

5. Case studies

The purpose of case studies is to investigate the changing trend of SIS performance related to CAFs and then to examine the relevant operational strategies. We consider a fire water supply system, with the focus on the subsystem of final elements, namely firewater pumps.

5.1. System description

The fire water supply system consists of three parts: sensors (for example fire and gas (F&G) detectors, signal from ESD system), logic solver (for example F&G logic solver) and final elements (for example fire water pumps, deluge valves). Our study here is limited to firewater pumps that are structured in a *KooN* configuration and are subject to CAFs, as shown in Fig. 5. In this case study, some situations like the system lose power and the logic solver fails, are beyond the delimitation.

The fire pump subsystem is a load-sharing system, where the pumps share common loads, such as water pressure. If one pump fails, the other pumps must carry the whole loads, and thus their failure rates can increase. Such failures are referred to as CAFs in the SIS.

5.2. PFD(t) and $\mathrm{PFD_{avg}}$ with CAFs

Two configurations of such a SIS subsystem: *2oo3* and *1oo3* are considered in this subsection. The time to self-failures $F_i(t)$ for all the pumps is assumed to be distributed exponentially with constant failure rates of 2.1×10^{-6} per hour. The cascaded failure probability γ of each pump is set as a fixed value of 0.05. The relevant PFD(t) over time within three proof test intervals is calculated by Eqs. (8) and (9).

Figs. 6 and 7 illustrate PFD(t) with and without CAFs for *2oo3* and *1oo3* configurations, respectively. It is found that the effects of CAFs on *2oo3* configuration are more obvious than those on *1oo3* configuration. For the *2oo3* configuration, $\mathrm{PFD_{avg}}$ increase dramatically from 3.4×10^{-4} to 2.7×10^{-3}, while $\mathrm{PFD_{avg}}$ of the *1oo3* configuration rises from 1.6×10^{-6} to 6.9×10^{-5}. The absolute difference of $\mathrm{PFD_{avg}}$ for *2oo3* configuration that are caused

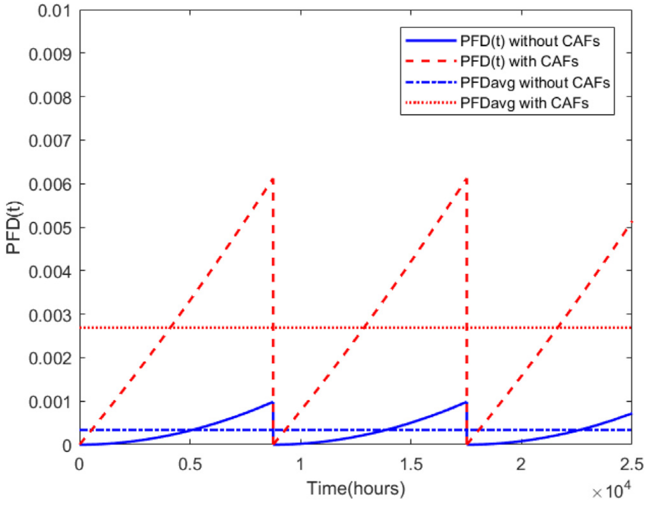

Fig. 6. PFD(t) without and with CAFs for *2oo3* system.

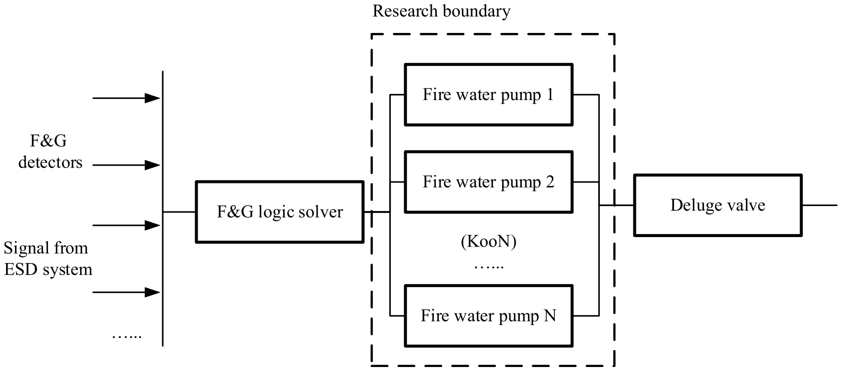

Fig. 5. Research boundary in fire water supply system.

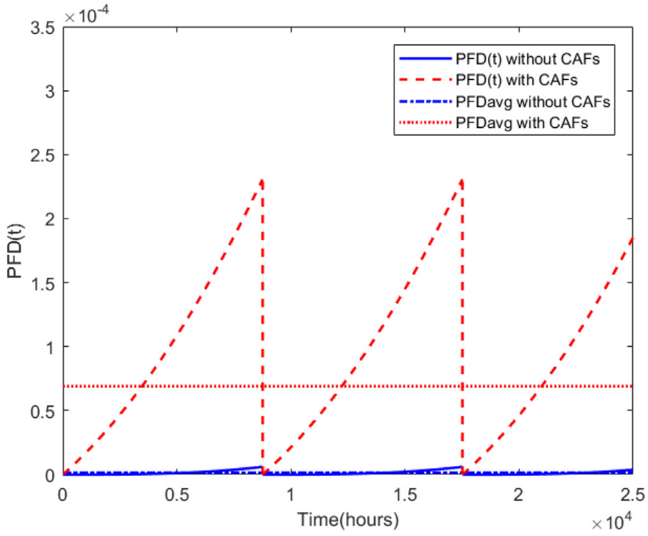

Fig. 7. PFD (t) without and with CAFs for 1oo3 system.

by CAFs is obviously bigger than that for *1oo3* configuration. It implies that the *2oo3* configuration is more sensitive to CAFs compared to the *1oo3* one. That is because only one cascade result in the failures within *2oo3* configuration. The implication to the SIS designer is to increase the number of N-K in the voting structure if the budget is allowed.

5.3. Effects of cascaded failure probability γ

To examine the effect of the cascading failure probability γ, the changes of PFD_{avg} and SILs are observed in different configurations when γ varying from 0 to 0.2. PFD_{avg} is calculated by the proposed formulas Eq. (15) for some selected typical configurations, such as *1oo2*, *1oo3*, *1oo4, 2oo3*, *3oo4* and *2oo4* configurations. Fig. 8 illustrates how γ affects PFD_{avg} in different system configurations. It is obvious that the PFD_{avg} increases along with γ and the values of PFD_{avg} for *3oo4* and *2oo3* configurations are more sensitive to CAFs. A conclusion can be reached that CAFs have more significant influence on the PFD_{avg} when the value of *N-K* decrease. Particularly, if *N-K* is equal to one, the configurations are the most vulnerable to CAFs. On the other hand, when the configuration is limited as N-K=1, the effectiveness of reducing γ in controlling PFD_{avg} is higher.

It is essential to ensure that SISs can achieve required SIL requirement in operational phase. $\text{Log}_{10}(\text{PFD}_{avg})$ is used to illustrate corresponding SILs for these configurations in Fig. 9. The variation of SILs with different γ dependents on configurations, namely the value of *N-K*. In this case, PFD_{avg} of the *1oo4* configuration is always within the range of SIL4. The values of PFD_{avg} for *2oo4* and *1oo3* configurations drop from the range of SIL4 to that of SIL3. The values of PFD_{avg} for *3oo4, 2oo3* and *1oo2* configurations change from SIL3 to SIL2.

The findings are helpful in determining SIL of SISs. When considering CAFs in SISs, their integrities are not only relying on the reliability of parallel components, but on the identified dependency of components and the system configurations. It shows that the impacts of CAFs on PFD_{avg} and SILs are unignorable regardless SIS configurations, especially when γ is not small. The results encourage the industry to put more efforts into analyzing and avoiding CAFs.

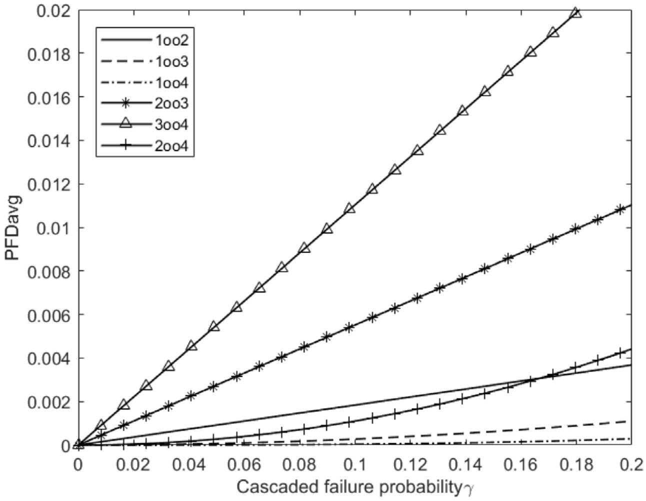

Fig. 8. PFD_{avg} of different configurations subject to CAFs.

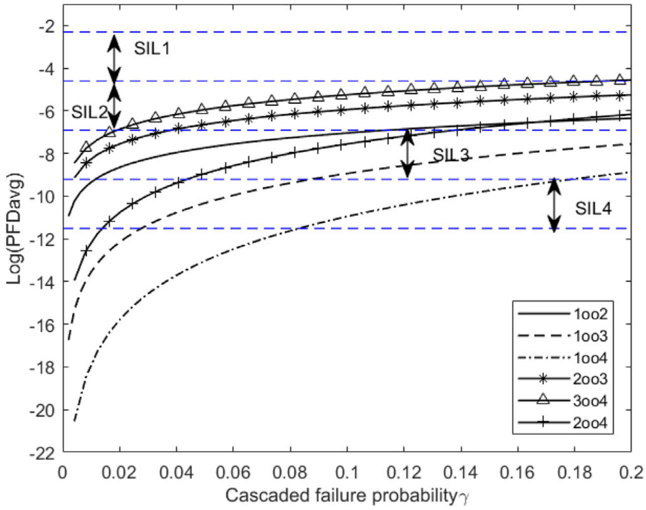

Fig. 9. $\text{Log}_{10}(\text{PFD}_{avg})$ of different configurations subject to CAFs.

5.4. The effects of CCFs and CAFs

To illustrate the need to consider the efforts of CAFs, we compare the effects of CCFs and CAFs on PFD_{avg} with different parameters, beta value β for CCFs and cascading intensity γ for CAFs. The configurations *2oo3* and *1oo3* are reconsidered in this subsection. According to Table 4, σ_{KooN} for *2oo3* and *1oo3* configurations are $3\gamma^2$ and 6. C_{KooN} for *2oo3* and *1oo3* configurations are 0.5 and 2. PFD_{avg} can be calculated by Eqs. (18) and (19), and the results are shown in Figs. 10 and 11. It is demonstrated that CAFs have comparable effects on PFD_{avg} and SIL as CCFs in this case.

The effects of CCFs and cascading failure on PFD_{avg} become more significant when the parameters increase. PFD_{avg} of the *2oo3* configuration considering CAFs is always higher than that of the same configuration considering CCFs. In a *1oo3* configuration, however, the effects of CCFs on PFD_{avg} are more significant than those from CAFs when the value of parameter is less than 0.17 approximately. Both two figures show that performance assessment of redundant SISs should be conservative since CAFs have comparable effects on PFD_{avg} and SIL as CCFs. It is noted that different configurations of SISs perform differently in terms of their vulnerabilities to CAFs and CCFs, even though the parameters of these two types of failures are set as equal.

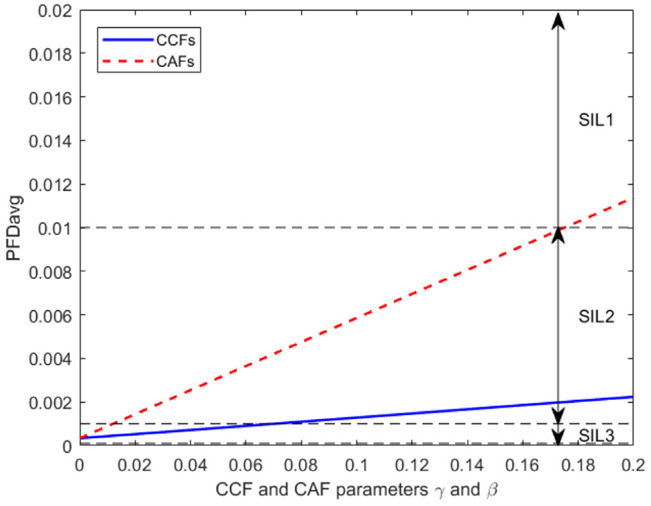

Fig. 10. The effects of CCFs and CAFs in 2oo3 systems.

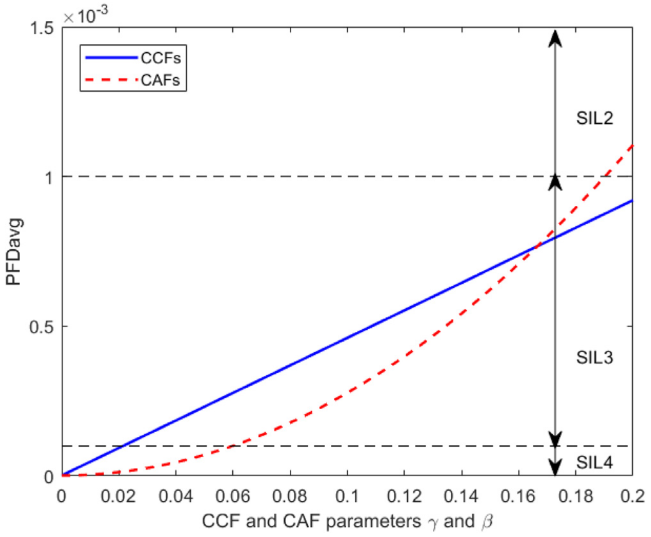

Fig. 11. The effects of CCFs and CAFs in 1oo3 systems.

The results of the case studies may increase the awareness to how CAFs can impact on the SIS performance and encourage that contribution of CAFs are considered in analyzes carried out design and in the operational phase. It is necessary to investigate the root causes and possible influence factors of CAFs. Possible solutions to decrease cascading intensities may include reducing functional dependence or sharing loads, enhancing absorptive ability and resistant capacity. In the operation phase, when determining proof test interval of SISs, the potential effects of CAFs should also be considered to ensure that the SISs can met SIL requirement.

6. Conclusions and future works

In this paper, a recursive aggregation-based approach has been developed for incorporating CAFs into reliability and availability analysis of SISs. General approximation formulas for $\mathrm{PFD}_{\mathrm{avg}}$ of *KooN* voted SISs have been proposed considering CAFs. The effects of cascading failures in the performance of SISs have been presented in comparison with those by CCFs. Numerical examples have shown that the contribution of CAFs towards $\mathrm{PFD}_{\mathrm{avg}}$ relies on not only the cascaded failure probability, but also the system configurations. Such analysis can help designers and operators better evaluate effects of dependent failures and estimate system performance of SISs. The proposed approach has been illustrated in the case study of SISs, but it must be highlighted that the analytical formulas can be more generally applied to other industrial *KooN* voted systems.

Independent/self-failures are assumed to be exponential distribution because the exponential distribution is the most used life distribution in applied reliability analysis. However, many other distributions, such as Weibull distribution for many mechanical systems, can also be considered by using the convolutions in the approach.

In this paper, we assume constant cascading probability, which is rather restrictive. It is worthy to consider statistical dependency, such as time-dependent cascading probability between CAFs. Further, the future work can involve performance assessment for the SISs in high/continuous mode, where average frequency of failure (PFH) are used as a measure. New approximation formulas for these SISs are needed.

Another topic to be explored is how to allocate SILs to reduce required amount of risk with consideration of dependent failures, like CCFs and CAFs. Traditionally, the allocation process often excludes dependent failures that may exist within and between SISs. It is thus of interest to perform further studies on the SIL allocation considering dependent failures.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] IEC61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission; 2010.

[2] IEC61511. Functional safety-safety instrumented systems for the process industry sector. Geneva: International Electrotechnical Commission; 2016.

[3] Xie L, Håbrekke S, Liu Y, Lundteigen MA. Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry. J Loss Prevent Process Ind 2019;60:96–105.

[4] Raus M. Reliability of safety-critical systems: Theory and applicationsed. Hoboken, New Jersey, USA: John Wiley & Sons; 2014.

[5] Hauge S, Kråkenes T, Hokstad P, Håbrekke S, Jin H. Reliability prediction method for safety instrumented systems–PDS method handbooked. Trondheim, Norway: SINTEF; 2013.

[6] Liu Y, Raus M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prevent Process Ind 2011;24(1):49–56.

[7] Summers AE, Raney G. Common cause and common sense, designing failure out of your safety instrumented systems (SIS). ISA Trans 1999;38(3):291–9.

[8] ISO/TR12489. Petroleum, petrochemical and natural gas industries—Reliability modelling and calculation of safety systems. 2013.

[9] Biswal GR, Maheshwari RP, Dewal M. System reliability and fault tree analysis of SeSHRS-based augmentation of hydrogen: Dedicated for combined cycle power plants. IEEE Syst J 2012;6(4):647–56.

[10] Levitin G, Xing L. Reliability and performance of multi-state systems with propagated failures having selective effect. Reliab Eng Syst Saf 2010;95(6):655–61.

[11] Xing L, Levitin G, Wang C, Dai Y. Reliability of systems subject to failures with dependent propagation effect. IEEE Trans Syst Man Cybern Syst 2013;43(2):277–90.

[12] Rausand M, Høyland A. System reliability theory: Models, statistical methods, and applications. 2nd ed. Hoboken, New Jersey, USA: John Wiley & Sons; 2004.

[13] Xie L, Lundteigen MA, Liu YL. Common cause failures and cascading failures in technical systems: similarities, differences and barriers. In: European safety and reliability conference (ESREL). Trondheim: NTNU; 2018.

[14] Levitin G. A universal generating function approach for the analysis of multi-state systems with dependent elements. Reliab Eng Syst Saf 2004;84(3):285–92.

[15] Motter AE, Lai Y-C. Cascade-based attacks on complex networks. Phys Rev 2002;66(6):065102.

[16] Albert R, Barabási A-L. Statistical mechanics of complex networks. Rev Modern Phys 2002;74(1):47–97.

[17] Zio E, Sansavini G. Component criticality in failure cascade processes of network systems. Risk Anal 2011;31(8):1196–210.

[18] Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks. Phys Rev E 2004;69(4):045104.

[19] Cozzani V, Gubinelli G, Antonioni G, Spadoni G, Zanelli S. The assessment of risk caused by domino effect in quantitative area risk analysis. J Hazard Mater 2005;127(1–3):14–30.

[20] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliab Eng Syst Saf 2001;71(3):249–60.

[21] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature 2010;464(7291):1025–8.

[22] Iyer SM, Nakayama MK, Gerbessiotis AV. Markovian dependability model with cascading failures. IEEE Trans Comput 2009;58(9):1238–49.

[23] Xie L, Lundteigen MA, Liu Y. Reliability and barrier assessment of series–parallel systems subject to cascading failures. Proc. Inst. Mech. Eng. O 2020;234(3):455–69.

[24] Zhao G, Xing L. Reliability analysis of IoT systems with competitions from cascading probabilistic function dependence. Reliab Eng Syst Saf 2020;198:106812.

[25] Murthy D, Nguyen D. Study of two-component system with failure interaction. Nav Res Logist 1985;32(2):239–47.

[26] Liu B, Wu J, Xie M. Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty. European J Oper Res 2015;243(3):874–82.

[27] Jin H, Lundteigen MA, Raus M. New PFH-formulas for k-out-of-n: F-systems. Reliab Eng Syst Saf 2013;111:112–8.

[28] Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi SA. A new method for assessing domino effect in chemical process industry. J Hard Mater 2010;182(1–3):416–26.